Free Questions for PT0-002 by certscare

Shared by Simpson on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

During a penetration test of a server application, a security consultant found that the application randomly crashed or remained stable after opening several simultaneous connections to the application and always submitting the same packets of dat

a. Which of the following is the best sequence of steps the tester should use to understand and exploit the vulnerability?

Options:

A- Attach a remote profiler to the server application. Establish a random number of connections to the server application. Send fixed packets of data simultaneously using those connections.

B- Attach a remote debugger to the server application. Establish a large number of connections to the server application. Send fixed packets of data simultaneously using those connections.

C- Attach a local disassembler to the server application. Establish a single connection to the server application. Send fixed packets of data simultaneously using that connection.

D- Attach a remote disassembler to the server application. Establish a small number of connections to the server application. Send fixed packets of data simultaneously using those connections.

Answer:

B

Explanation:

To understand and exploit the vulnerability causing the server application to crash or remain stable after opening several simultaneous connections, the best approach is to attach a remote debugger to the application. This allows the penetration tester to monitor the application's behavior in real-time without affecting the stability of the testing environment. Establishing a large number of connections to the server and sending fixed packets of data simultaneously can help to reproduce the issue consistently, which is crucial for identifying the cause of the crashes. Analyzing the application's response and debugging data will provide insights into potential buffer overflow, race conditions, or other vulnerabilities.

Effective Debugging Techniques

Fuzz Testing and Debugging

Question 2

Question Type: MultipleChoice

A penetration tester exploits a vulnerable service to gain a shell on a target server. The tester receives the following:

Directory of C:\Users\Guest 05/13/2022 09:23 PM mimikatz.exe 05/18/2022 09:24 PM mimidrv.sys 05/18/2022 09:24 PM mimilib.dll

Which of the following best describes these findings?

Options:

A- Indicators of prior compromise

B- Password encryption tools

C- False positives

D- De-escalation attempts

Answer:

A

Explanation:

The presence of files such as mimikatz.exe, mimidrv.sys, and mimilib.dll on a target server indicates prior compromise. Mimikatz is a well-known post-exploitation tool used for extracting plaintext passwords, hash dumps, PIN codes, and Kerberos tickets from memory. These files suggest that an attacker has previously gained access to the system and used Mimikatz for credential harvesting. This is a strong indicator of a prior security breach rather than tools used for password encryption or false positives.

Mimikatz Usage and Detection

Understanding Indicators of Compromise

Question 3

Question Type: **MultipleChoice**

A penetration tester is conducting an assessment on a web application. Which of the following active reconnaissance techniques would be best for the tester to use to gather additional information about the application?

Options:

A- Using cURL with the verbose option

B- Crawling UR Is using an interception proxy

C- Using Scapy for crafted requests

D- Crawling URIs using a web browser

Answer:

B

Explanation:

Crawling URIs using an interception proxy is the best active reconnaissance technique for gathering additional information about a web application. An interception proxy, such as Burp Suite or OWASP ZAP, allows the penetration tester to see and manipulate the requests and responses between the client and the server, providing detailed insights into the application's behavior, structure, and vulnerabilities. This technique is more comprehensive and controlled compared to using cURL or a web browser.

OWASP Testing Guide: Web Application Security Testing

Burp Suite Documentation

OWASP ZAP User Guide

Question 4

Question Type: MultipleChoice

An organization is using Android mobile devices but does not use MDM services. Which of the following describes an existing risk present in this scenario?

Options:

A- Device log facility does not record actions.

B- End users have root access by default.

C- Unsigned applications can be installed.

D- Push notification services require internet.

Answer:

C

Explanation:

The risk present in an organization using Android mobile devices without Mobile Device Management (MDM) services is that unsigned applications can be installed. Without MDM, there are fewer controls over the installation of applications, which increases the risk of installing malicious or unauthorized applications. MDM services typically provide a way to enforce application signing policies, preventing the installation of unsigned apps.

OWASP Mobile Security Project

NIST Mobile Device Management Guide

Question 5

Question Type: **MultipleChoice**

A vulnerability assessor is looking to establish a baseline of all IPv4 network traffic on the local VLAN without a local IP address. Which of the following Nmap command sequences would best provide this information?

Options:

A- sudo nmap ---script=bro* -e ethO

B- sudo nmap -sF ---script=* -e ethO

C- sudo nmap -sV -sT -p 0-65535 -e ethO

D- sudo nmap -sV -p 0-65535 0.0.0.0/0

Answer:

A

Explanation:

The command sudo nmap ---script=bro* -e ethO is the best choice for establishing a baseline of all IPv4 network traffic on the local VLAN without a local IP address. The ---script=bro* specifies the use of scripts that can capture and analyze traffic, and -e ethO specifies the network interface to be used. This allows the vulnerability assessor to capture and analyze network traffic at a low level, which is essential for baseline analysis.

Nmap Scripting Engine (NSE)

Nmap Network Interface Specification

Question 6

Question Type: MultipleChoice

During a REST API security assessment, a penetration tester was able to sniff JSON content containing user credentials. The JSON structure was as follows:

transaction_id: "1234S6", content: [{

user_id: "mrcrowley", password: ["54321#"] b

user_id: "ozzy",

password: ["1112228"])]

Assuming that the variable json contains the parsed JSON data, which of the following Python code snippets correctly returns the password for the user ozzy?

Options:

A- json['content']['password'][1]

B- json['user_id']['password'][0][1]

C- json['content'][1]['password'][0]

D- json['content'][0]['password'][1]

Answer:

C

Explanation:

To correctly return the password for the user 'ozzy' from the given JSON structure, the Python code snippet should navigate the nested structure appropriately. The 'content' array contains objects with 'user_id' and 'password' fields. The correct password for 'ozzy' can be accessed using the code json['content'][1]['password'][0], which navigates to the second object in the 'content' array (index 1) and then accesses the first element (index 0) of the 'password' array for that user.

Python JSON Handling

Python JSON Path Navigation

Question 7

Question Type: **MultipleChoice**

A penetration tester would like to crack a hash using a list of hashes and a predefined set of rules. The tester runs the following command: hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule

Which of the following is the penetration tester using to crack the hash?

Options:

A- Hybrid attack

B- Dictionary

C- Rainbow table

D- Brute-force method

Answer:

B

Explanation:

The command hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule indicates that the penetration tester is using a dictionary attack combined with rule-based modifications. The -a 0 option specifies a dictionary attack mode, where .\rockyou.txt is the dictionary file containing potential passwords, and -r .\rules\replace.rule applies predefined rules to mutate these passwords. This method leverages a known list of potential passwords and augments them with additional variations based on the rules provided.

Hashcat Dictionary Attack

Hashcat Rule-based Attack

Question 8

Question Type: **MultipleChoice**

A penetration testing team has gained access to an organization's data center, but the team requires more time to test the attack strategy. Which of the following wireless attack techniques would be the most successful in preventing unintended interruptions?

Options:

A- Captive portal

B- Evil twin

C- Bluejacking

D- Jamming

Answer:

B

Explanation:

An evil twin attack involves setting up a rogue wireless access point that mimics a legitimate one. This type of attack can be highly effective in a penetration testing scenario because it can intercept and capture data transmitted over the network without causing noticeable interruptions to the normal operation of the wireless network. Users are tricked into connecting to the evil twin instead of the legitimate access point, allowing the penetration testers to capture sensitive information. Unlike jamming, which disrupts the network, or bluejacking, which is limited to sending unsolicited messages, the evil twin can facilitate man-in-the-middle attacks seamlessly.

OWASP Wireless Evil Twin Attack

Kali Linux Evil Twin Tutorial

Question 9

Question Type: **MultipleChoice**

Which of the following components should a penetration tester most likely include in a report at the end of an assessment?

Options:

A- Metrics and measures

B- Client interviews

C- Compliance information

D- Business policies

Answer:

A

Explanation:

A penetration tester should most likely include metrics and measures in a report at the end of an assessment. Metrics and measures provide quantitative data that helps in understanding the extent and impact of vulnerabilities found during the assessment. They offer a clear and objective way to convey the results and the effectiveness of the security controls in place. This data-driven approach aids in prioritizing remediation efforts, benchmarking against industry standards, and demonstrating improvements over time.

OWASP Penetration Testing Methodologies

Question 10

Question Type: **MultipleChoice**

A penetration tester is performing an assessment against a customer's web application that is hosted in a major cloud provider's environment. The penetration tester observes that the majority of the attacks attempted are being blocked by the organization's WAF. Which of the following attacks would be most likely to succeed?

Options:

A- Reflected XSS

B- Brute-force

C- DDoS

D- Direct-to-origin

Answer:

D

Explanation:

When a web application firewall (WAF) is blocking most of the attacks, a direct-to-origin attack is likely to succeed. A direct-to-origin attack targets the backend servers directly, bypassing the WAF. This type of attack exploits any functionality that allows direct access to the origin servers (backend servers) without passing through the WAF. Techniques such as manipulating DNS, exploiting misconfigurations, or using direct IP access can be employed to bypass the WAF, making direct-to-origin attacks effective under these circumstances.

OWASP WAF Bypass Techniques

Imperva - What is a WAF? Web Application Firewall

Question 11

Question Type: **MultipleChoice**

A penetration tester runs a reconnaissance script and would like the output in a standardized machine-readable format in order to pass the data to another application. Which of the following is the best for the tester to use?

Options:

A- JSON

B- Lists

C- XLS

D- Trees

Answer:

A

Explanation:

JSON (JavaScript Object Notation) is the best format for a penetration tester to use when they need the output of a reconnaissance script in a standardized machine-readable format to pass data to another application. JSON is widely supported across different programming languages and platforms, making it an ideal choice for data interchange. It allows for the hierarchical organization of data, is easy to read and write, and can be parsed and generated by numerous tools and libraries. This makes JSON a versatile and practical choice for a variety of applications in penetration testing and beyond.

RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format

OWASP - JSON Security

Question 12

Question Type: MultipleChoice

A penetration tester runs an Nmap scan and obtains the following output:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-12 18:53 GMT

Nmap scan report for 10.22.2.2

Host is up (0.0011s latency).

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2019

1433/tcp open ms-sql-s Microsoft SQL Server 2019

3389/tcp open ms-wbt-server Microsoft Terminal Services

8080/tcp open http Microsoft IIS 9.0
```

Which of the following commands should the penetration tester try next to explore this server?

Options:

A- nikto -host http://10.22.2-2

B- hydra -1 administrator -P passwords.txt ftp://10.22.2.2

C- nmap -p 3389 ---script vnc-info.nse 10.22.2.2

D- medusa -h 10.22.2.2 -n 1433 -u sa -P passwords.txt-Mmssql

Answer:

A

Explanation:

Given the Nmap scan results showing an open HTTP service on port 8080 running Microsoft IIS 9.0, the next logical step for the penetration tester would be to further explore the web server. Nikto is a web server scanner that can identify known vulnerabilities, configuration issues, and other security problems.

Using the command nikto -host http://10.22.2.2 will initiate a scan against the HTTP service on the target server, helping the tester to identify potential weaknesses that could be exploited.

Nikto official documentation: Nikto Documentation

Examples of web server vulnerability scanning in penetration testing: Writeup.

20%
DISCOUNT