Free Questions for PT0-002 by go4braindumps

Shared by Haynes on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

ion tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the.. :tive way for the tester to achieve this objective?

Options:

A- Dropping USB flash drives around the company campus with the file on it

B- Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts

C- Sending a pretext email from the IT department before sending the download instructions later

D- Saving the file in a common folder with a name that encourages people to click it

Answer:

C

Explanation:

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a

legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

Question 2

Question Type: **MultipleChoice**

During an assessment, a penetration tester inspected a log and found a series of thousands of requests coming from a single IP address to the same URL. A few of the requests are listed below.

```
.myprofile.com/servicestatus.php?serviceID=1
.myprofile.com/servicestatus.php?serviceID=2
.myprofile.com/servicestatus.php?serviceID=3
.myprofile.com/servicestatus.php?serviceID=4
.myprofile.com/servicestatus.php?serviceID=5
.myprofile.com/servicestatus.php?serviceID=6
```

Which of the following vulnerabilities was the attacker trying to exploit?

Options:

A- ..Session hijacking

B- ..URL manipulation

C- ..SQL injection

D- ..Insecure direct object reference

Answer:

C

Explanation:

The vulnerability that the attacker was trying to exploit is SQL injection, which is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. SQL injection can allow an attacker to perform various actions on the database, such as reading, modifying, deleting, or creating data, or executing commands on the underlying OS. The log shows that the attacker was sending thousands of requests to the same URL with different parameters, such as id=1' OR 1=1;--, id=1' AND 1=2;--, or id=1' UNION SELECT * FROM users;--. These parameters are examples of SQL injection payloads, which are crafted SQL statements that are designed to manipulate or bypass the intended SQL query. For example, id=1' OR 1=1;-- is a payload that terminates the original query with a single quote and a semicolon, appends an OR condition that is always true (1=1), and comments out the rest of the query with two dashes (--). This payload can cause the web application to return all records from

the database table instead of just one record with id=1. The other options are not vulnerabilities that match the log entries. Session hijacking is a type of attack that exploits a vulnerability in a web application that allows an attacker to take over an active session of another user by stealing or guessing their session identifier or cookie. URL manipulation is a type of attack that exploits a vulnerability in a web application that allows an attacker to modify parameters or values in the URL to access unauthorized resources or functions. Insecure direct object reference is a type of attack that exploits a vulnerability in a web application that allows an attacker to access objects or resources directly by modifying their identifiers or references in the URL or request.

Question 3

Question Type: MultipleChoice

Which of the following OSSTM testing methodologies should be used to test under the worst conditions?

Options:

A- Tandem

B- Reversal

C- Semi-authorized

D- Known environment

Answer:

D

Explanation:

The OSSTM testing methodology that should be used to test under the worst conditions is known environment, which is a testing approach that assumes that the tester has full knowledge of the target system or network, such as its architecture, configuration, vulnerabilities, or defenses. A known environment testing can simulate a worst-case scenario, where an attacker has gained access to sensitive information or insider knowledge about the target, and can exploit it to launch more sophisticated or targeted attacks. A known environment testing can also help identify the most critical or high-risk areas of the target, and provide recommendations for improving its security posture. The other options are not OSSTM testing methodologies that should be used to test under the worst conditions. Tandem is a testing approach that involves two testers working together on the same target, one as an attacker and one as a defender, to simulate a realistic attack scenario and evaluate the effectiveness of the defense mechanisms. Reversal is a testing approach that involves switching roles between the tester and the client, where the tester acts as a defender and the client acts as an attacker, to assess the security awareness and skills of the client. Semi-authorized is a testing approach that involves giving partial or limited authorization or access to the tester, such as a user account or a network segment, to simulate an attack scenario where an attacker has compromised a legitimate user or device.

Question 4

Question Type: MultipleChoice

A penetration tester is conducting an Nmap scan and wants to scan for ports without establishing a connection. The tester also wants to find version data information for services running on Projects. Which of the following Nmap commands should the tester use?

Options:

A- ..nmap -sU -sV -T4 -F target.company.com

B- ..nmap -sS -sV -F target.company.com

C- ..nmap -sT -v -T5 target.company.com

D- ..nmap -sX -sC target.company.com

Answer:

B

Explanation:

The Nmap command that the tester should use to scan for ports without establishing a connection and to find version data information for services running on open ports is nmap -sS -sV -F target.company.com. This command has the following options:

-sS performs a TCP SYN scan, which is a scan technique that sends TCP packets with the SYN flag set to the target ports and analyzes the responses. A TCP SYN scan does not establish a full TCP connection, as it only completes the first step of the three-way handshake. A TCP SYN scan can stealthily scan for open ports without alerting the target system or application.

-sV performs version detection, which is a feature that probes open ports to determine the service and version information of the applications running on them. Version detection can provide useful information for identifying vulnerabilities or exploits that affect specific versions of services or applications.

-F performs a fast scan, which is a scan option that only scans the 100 most common ports according to the nmap-services file. A fast scan can speed up the scan process by avoiding scanning less likely or less interesting ports.

target.company.com specifies the domain name of the target system or network to be scanned.

The other options are not valid Nmap commands that meet the requirements of the question. Option A performs a UDP scan (-sU), which is a scan technique that sends UDP packets to the target ports and analyzes the responses. A UDP scan can scan for open ports that use UDP protocol, such as DNS, SNMP, or DHCP. However, a UDP scan does establish a connection with the target system or application, unlike a TCP SYN scan. Option C performs a TCP connect scan (-sT), which is a scan technique that sends TCP packets with the SYN flag set to the target ports and completes the three-way handshake with an ACK packet if a SYN/ACK packet is received. A TCP connect scan can scan for open ports that use TCP protocol, such as HTTP, FTP, or SSH. However, a TCP connect scan does establish a full TCP connection with the target system or application, unlike a TCP SYN scan. Option D performs an Xmas scan (-sX), which is a scan technique that sends TCP packets with the FIN, PSH, and URG flags set to the target ports and analyzes the responses. An Xmas scan can stealthily scan for open ports without alerting the target system or application, similar to a TCP SYN scan. However, option D does not perform version detection (-sV), which is one of the requirements of the question.

Question 5

Question Type: **MultipleChoice**

While performing the scanning phase of a penetration test, the penetration tester runs the following command:

.....v -sV -p- 10.10.10.23-28

....ip scan is finished, the penetration tester notices all hosts seem to be down. Which of the following options should the penetration tester try next?

Options:

A- -su

B- -pn

C- -sn

D- -ss

Answer:

B

Explanation:

The command nmap -v -sV -p- 10.10.10.23-28 is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The command has the following

options:

-v enables verbose mode, which increases the amount of information displayed by nmap

-sV enables version detection, which attempts to determine the version and service of the open ports

-p- specifies that all ports from 1 to 65535 should be scanned

10.10.10.23-28 specifies the range of IP addresses to be scanned The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not respond. However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error. The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

Question 6

Question Type: **MultipleChoice**

During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ----------company systems?

Options:

A- Aside-channel attack

B- A command injection attack

C- A watering-hole attack

D- A cross-site scripting attack

Answer:

C

Explanation:

The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website.A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server

frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

Question 7

Question Type: MultipleChoice

During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?

Options:

A- Federation misconfiguration of the container

B- Key mismanagement between the environments

C- laaS failure at the provider

D- Container listed in the public domain

Answer:

A

Explanation:

The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

Question 8

Question Type: MultipleChoice

A penetration tester runs the following command:

l.comptia.local axfr comptia.local

which of the following types of information would be provided?

Options:

A- The DNSSEC certificate and CA

B- The DHCP scopes and ranges used on the network

C- The hostnames and IP addresses of internal systems

D- The OS and version of the DNS server

Answer:

C

Explanation:

The command dig @ns1.comptia.local axfr comptia.local is a command that performs a DNS zone transfer, which is a process of copying the entire DNS database or zone file from a primary DNS server to a secondary DNS server. A DNS zone file contains records

that map domain names to IP addresses and other information, such as mail servers, name servers, or aliases. A DNS zone transfer can provide useful information for enumeration, such as the hostnames and IP addresses of internal systems, which can help identify potential targets or vulnerabilities.A DNS zone transfer can be performed by using tools such as dig, which is a tool that can query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records1. The other options are not types of information that would be provided by a DNS zone transfer. The DNSSEC certificate and CA are not part of the DNS zone file, but rather part of the DNSSEC protocol, which is an extension of the DNS protocol that provides authentication and integrity for DNS data. The DHCP scopes and ranges used on the network are not part of the DNS zone file, but rather part of the DHCP protocol, which is a protocol that assigns dynamic IP addresses and other configuration parameters to devices on a network. The OS and version of the DNS server are not part of the DNS zone file, but rather part of the OS fingerprinting technique, which is a technique that identifies the OS and version of a remote system by analyzing its responses to network probes.

Question 9

Question Type: MultipleChoice

An organization wants to identify whether a less secure protocol is being utilized on a wireless network. Which of the following types of attacks will achieve this goal?

Options:

A- Protocol negotiation

B- Packet sniffing

C- Four-way handshake

D- Downgrade attack

Answer:

D

Explanation:

A downgrade attack is a type of attack that exploits a vulnerability in the protocol negotiation process between a client and a server to force them to use a less secure protocol than they originally intended. A downgrade attack can be used to identify whether a less secure protocol is being utilized on a wireless network by intercepting and modifying the messages exchanged during the protocol negotiation phase, such as the association request and response frames, and making the client and the server agree on a weaker protocol, such as WEP or WPA, instead of a stronger one, such as WPA2 or WPA3. A downgrade attack can also enable the attacker to perform other attacks, such as cracking the encryption keys or capturing the network traffic, more easily by taking advantage of the weaknesses of the less secure protocol.A downgrade attack can be performed by using tools such as Airgeddon, which is a multi-use bash script for Linux systems to audit wireless networks1.

Question 10

Question Type: MultipleChoice

A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user ...ch of the following should be included in the recommendations for remediation?

Options:

A- training program on proper access to the web server

B- patch-management program for the web server.

C- the web server in a screened subnet

D- Implement endpoint protection on the workstations

Answer:

D

Explanation:

The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have

gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.