Free Questions for PT0-002 by braindumpscollection

Shared by Mccarty on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After successfully compromising a remote host, a security consultant notices an endpoint protection software is running on the host. Which of the following commands would be

best for the consultant to use to terminate the protection software and its child processes?

Options:

A- taskkill /PID <PID> /T /F

B- taskkill /PID <PID> /IM /F

C- taskkill /PID <PID> /S /U

D- taskkill /PID <PID> /F /P

Answer:

A

Explanation:

The taskkill command is used in Windows to terminate tasks by process ID (PID) or image name (IM). The correct command to terminate a specified process and any child processes which were started by it uses the /T flag, and the /F flag is used to force terminate the process. Therefore, taskkill /PID <PID> /T /F is the correct syntax to terminate the endpoint protection software and its child processes.

The other options listed are either incorrect syntax or do not accomplish the task of terminating the child processes:

* /IM specifies the image name but is not necessary when using /PID.

* /S specifies the remote system to connect to and /U specifies the user context under which the command should execute, neither of which are relevant to terminating processes.

* There is no /P flag in the taskkill command.

Question 2

Question Type: **MultipleChoice**

A penetration tester uses Hashcat to crack hashes discovered during a penetration test and obtains the following output:

ad09cd16529b5f5a40a3e15344e57649f4a43a267a97f008af01af803603c4c8 : Summer2023 !!

7945bb2bb08731fc8d57680ffa4aefec91c784d231de029c610b778eda5ef48b:p@ssWord123

ea88ceab69cb2fb8bdcf9ef4df884af219fffbffab473ec13f20326dc6f84d13: Love-You999

Which of the following is the best way to remediate the penetration tester's discovery?

Options:

A- Requiring passwords to follow complexity rules

B- Implementing a blocklist of known bad passwords

C- Setting the minimum password length to ten characters

D- Encrypting the passwords with a stronger algorithm

Answer:

B

Explanation:

The penetration tester's discovery of passwords vulnerable to hash cracking suggests a lack of robust password policies within the organization. Among the options provided, implementing a blocklist of known bad passwords is the most effective immediate remediation. This measure would prevent users from setting passwords that are easily guessable or commonly used, which are susceptible to hash cracking tools like Hashcat.

Requiring passwords to follow complexity rules (Option A) can be helpful, but attackers can still crack complex passwords if they are common or have been exposed in previous breaches. Setting a minimum password length (Option C) is a good practice, but length alone does not ensure a password's strength against hash cracking techniques. Encrypting passwords with a stronger algorithm (Option D) is a valid long-term strategy but would not prevent users from choosing weak passwords that could be easily guessed before hash cracking is even necessary.

Therefore, a blocklist addresses the specific vulnerability exposed by the penetration tester---users setting weak passwords that can be easily cracked. It's also worth noting that the best practice is a combination of strong, enforced password policies, user education, and the use of multi-factor authentication to enhance security further.

Question 3

Question Type: **MultipleChoice**

A penetration testing firm wants to hire three additional consultants to support a newly signed long-term contract with a major customer. The following is a summary of candidate

background checks:

Candidate number	Criminal charges
Candidate 1	Public intoxication
Candidate 2	Unauthorized system access
Candidate 3	None
Candidate 4	Speeding in a construction area

Which of the following candidates should most likely be excluded from consideration?

Options:

A- Candidate 1

B- Candidate 2

C- Candidate 3

D- Candidate 4

Answer:

B

Explanation:

In the context of penetration testing or cybersecurity, hiring a consultant with a background in unauthorized system access could present both risks and benefits. From a risk management perspective, Candidate 2's history of unauthorized system access is a significant red flag. Such past behavior indicates a willingness to operate outside of legal and ethical boundaries, which could pose a risk to the firm and its clients, especially in a role that requires trust and adherence to legal guidelines.

However, the very skills that enabled unauthorized access might also provide the firm with deep insights into hacker methodologies, potentially enhancing the firm's capability to secure systems against such intrusions. It is a common practice in the cybersecurity industry to employ individuals with a history of hacking in roles where they can contribute positively, known as 'ethical hacking' or 'white hat' roles.

Nonetheless, given the legal and ethical responsibilities inherent in cybersecurity work, Candidate 2's past criminal charge of unauthorized system access is the most pertinent to the role and poses the most direct risk to the firm's operations and reputation. It would be crucial for the firm to conduct a thorough risk assessment, including the nature of the unauthorized access, the candidate's subsequent actions, rehabilitation, and current capabilities, before making a hiring decision.

From the provided information, it appears that Candidate 2 should most likely be excluded from consideration due to the direct relevance of their criminal charges to the position in question. Without evidence of rehabilitation and a clear demonstration of ethical standards, the liability risks might outweigh the potential benefits to the firm.

Question 4

Question Type: **MultipleChoice**

An organization's Chief Information Security Officer debates the validity of a critical finding from a penetration assessment that was completed six months ago. Which of the following post-report delivery activities would have most likely prevented this scenario?

Options:

A- Client acceptance

B- Data destruction process

C- Attestation of findings

D- Lessons learned

Answer:

A

Explanation:

Client acceptance (A) is a critical post-report delivery activity that involves the client formally accepting the findings and conclusions of a penetration assessment report. This process usually includes a review of the findings by the client, discussions about the impact, and agreement on the accuracy and relevance of the reported vulnerabilities and issues. Ensuring client acceptance soon after the delivery of the report can prevent scenarios where the validity of findings is debated long after the assessment, as in the case described.

Data destruction process (B), attestation of findings (C), and lessons learned (D) are also important aspects of a penetration testing engagement, but they do not directly address the issue of the client disputing the findings well after the report has been delivered. Client

acceptance ensures both parties are in agreement on the outcomes of the assessment, minimizing disputes about the findings later on.

Question 5

Question Type: MultipleChoice

A penetration tester noticed that an employee was using a wireless headset with a smartphone. Which of the following methods would be best to use to intercept the communications?

Options:

A- Multiplexing

B- Bluejacking

C- Zero-day attack

D- Smurf attack

Answer:

B

Explanation:

To intercept the communications between an employee's wireless headset and smartphone, the penetration tester would likely use 'Bluejacking' (B). Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices, but in the context of penetration testing and security, it can also encompass techniques for intercepting or hijacking Bluetooth connections. This could allow the tester to eavesdrop on communications or even take control of the headset.

Question 6

Question Type: MultipleChoice

A penetration tester approaches a company employee in the smoking area and starts a conversation about the company's recent social event. After a few minutes, the employee holds the badge-protected door open for the penetration tester and both enter the company's building. Which of the following attacks did the penetration tester perform?

Options:

A- Dumpster diving

B- Phishing

C- Badge cloning

D- Tailgating

Answer:

D

Explanation:

In this scenario, the penetration tester performed a 'Tailgating' attack (D), where the tester follows closely behind a legitimate employee to gain unauthorized access to a secure area without being noticed. This social engineering technique relies on exploiting human tendencies to be polite or avoid confrontation, rather than using technical hacking methods. The tester engaged the employee in casual conversation to appear less suspicious and took advantage of the situation when the employee, perhaps distracted or feeling socially obliged, held the door open for them.

Question 7

Question Type: MultipleChoice

During a security assessment of a web application, a penetration tester was able to generate the following application response:

Unclosed quotation mark after the character string Incorrect syntax near ''.

Which of the following is the most probable finding?

Options:

A- SQL injection

B- Cross-site scripting

C- Business logic flaw

D- Race condition

Answer:

A

Explanation:

The error message 'Unclosed quotation mark after the character string Incorrect syntax near '.' suggests that the application is vulnerable to SQL Injection (A). This type of vulnerability occurs when an attacker is able to inject malicious SQL queries into an application's database query. The error message indicates that the application's input handling allows for the manipulation of the underlying SQL queries, which can lead to unauthorized data access, data modification, and other database-related attacks.

Question 8

Question Type: MultipleChoice

A penetration tester captures SMB network traffic and discovers that users are mistyping the name of a fileshare server. This causes the workstations to send out requests attempting to resolve the fileshare server's name. Which of the following is the best way for a penetration tester to exploit this situation?

Options:

A- Relay the traffic to the real file server and steal documents as they pass through.

B- Host a malicious file to compromise the workstation.

C- Reply to the broadcasts with a fake IP address to deny access to the real file server.

D- Respond to the requests with the tester's IP address and steal authentication credentials.

Answer:

D

Explanation:

In the scenario where users are mistyping the name of a fileshare server, leading to broadcast requests, the most effective exploitation strategy would be for the penetration tester to respond to these requests with their own IP address (D) and set up a service to capture

authentication credentials. This technique is known as a 'Man-in-the-Middle' (MitM) attack, where the attacker intercepts communication between two parties. In this case, the tester can exploit the misdirected requests to potentially capture sensitive information such as usernames and passwords.

Question 9

Question Type: MultipleChoice

After performing a web penetration test, a security consultant is ranking the findings by criticality. Which of the following standards or methodologies would be best for the consultant to use for reference?

Options:

A- OWASP

B- MITRE ATT&CK

C- PTES

D- NIST

Answer:

A

Explanation:

After performing a web penetration test, using the OWASP (Open Web Application Security Project) standards or methodologies would be the best choice for ranking the findings by criticality. OWASP is renowned for its comprehensive documentation and guidelines on web application security, including the well-known OWASP Top 10 list, which outlines the ten most critical web application security risks. This makes it an ideal reference for categorizing and prioritizing vulnerabilities discovered during a web penetration test.

While MITRE ATT&CK, PTES (Penetration Testing Execution Standard), and NIST (National Institute of Standards and Technology) provide valuable frameworks and methodologies for cybersecurity, OWASP's focus on web applications specifically makes it the most suitable for this context.

Question 10

Question Type: MultipleChoice

Which of the following documents should be consulted if a client has an issue accepting a penetration test report that was provided?

Options:

A- Rules of engagement

B- Signed authorization letter

C- Statement of work

D- Non-disclosure agreement

Answer:

A

Explanation:

The Rules of Engagement (RoE) document is crucial when there's a dispute or issue with accepting a penetration test report. The RoE outlines the scope, methods, timing, legal considerations, and objectives of a penetration test. It serves as a guideline for both the client and the testing team on what is expected and permissible during the assessment. If there are issues with the report, referring back to the agreed-upon RoE can clarify whether the test was conducted within the agreed parameters and help resolve any disputes.

The signed authorization letter, statement of work, and non-disclosure agreement are also important documents but are more related to the permission, scope of work, and confidentiality aspects of the engagement, respectively, rather than the specifics of how the test was to be conducted, which is what the RoE covers.

Question 11

Question Type: MultipleChoice

During a security assessment, a penetration tester decides to write the following Python script: import requests

x= ['OPTIONS', 'TRACE', 'TEST'l

for y in x;

z - requests.request(y, 'http://server.net')

print(y, z.status_code, z.reason)

Which of the following is the penetration tester trying to accomplish? (Select two).

Options:

A- Web server denial of service

B- HTTP methods availability

C- 'Web application firewall detection

D- 'Web server fingerprinting

E- Web server error handling

F- Web server banner grabbing

Answer:

B, D

Explanation:

The Python script mentioned in the question is designed to send HTTP requests using different methods ('OPTIONS', 'TRACE', 'TEST') to a specified URL ('http://server.net') and print out the method used along with the status code and reason for each response. The key objectives of this script are:

HTTP Methods Availability (B): By cycling through different HTTP methods, the script checks which methods are supported by the web server. This can reveal potential vulnerabilities, as certain methods like 'TRACE' can be exploited in certain situations (e.g., Cross Site Tracing (XST) attacks).

Web Server Fingerprinting (D): The response to different HTTP methods can provide clues about the web server's software and configuration, contributing to server fingerprinting. This information can be used to tailor further attacks or understand the security posture of the server.

This script is not designed for causing a denial of service, detecting web application firewalls, examining error handling, or performing banner grabbing directly, which excludes options A, C, E, and F.