PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester executes multiple enumeration commands to find a path to escalate privileges. Given the following command:

find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null

Which of the following is the penetration tester attempting to enumerate?

A. Attack path mapping

B. API keys

C. Passwords

D. Permission

Correct Answer: D

The command find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null is used to find files with the SUID bit set. SUID (Set User ID) permissions allow a file to be executed with the permissions of the file owner (root), rather than the

permissions of the user running the file.

Understanding the Command:

Purpose:

Why Enumerate Permissions:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 2

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

Correct Answer: A

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.

QUESTION 3

A penetration tester has gained access to the Chief Executive Officer\\'s (CEO\\'s) internal, corporate email. The next objective is to gain access to the network.

Which of the following methods will MOST likely work?

A. Try to obtain the private key used for S/MIME from the CEO\\'s account.

B. Send an email from the CEO\\'s account, requesting a new account.

C. Move laterally from the mail server to the domain controller.

D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D

QUESTION 4

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company\\'s web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

A. IP addresses and subdomains

B. Zone transfers

C. DNS forward and reverse lookups

D. Internet search engines

E. Externally facing open ports

F. Shodan results

Correct Answer: AD

A. IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company\\'s web presence. IP addresses can reveal the location, network, and service provider of the company\\'s web servers, while subdomains can indicate the different functions and features of the company\\'s website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company\\'s domain name.

D. Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company\\'s web presence. Search engines can provide a wealth of information, such as the company\\'s profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results by the title of the web pages.

QUESTION 5

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.

B. Verify the client has granted network access to the hot site.

C. Determine if the failover environment relies on resources not owned by the client.

D. Establish communication and escalation procedures with the client.

Correct Answer: A

The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.