CompTIA Valid Test PT0-003 Test: CompTIA PenTest+ Exam - PassLeader 365 Days Free Updates

P.S. Free & New PT0-003 dumps are available on Google Drive shared by PassLeader: https://drive.google.com/open?id=16IgCikrBz_cJv2MMHiOUoq6tFpWSikyh

CompTIA PenTest+ Exam exam tests are a high-quality product recognized by hundreds of industry experts. Over the years, PT0-003 exam questions have helped tens of thousands of candidates successfully pass professional qualification exams, and help them reach the peak of their career. It can be said that PT0-003 test guide is the key to help you open your dream door. We have enough confidence in our products, so we can give a 100% refund guarantee to our customers. PT0-003 Exam Questions promise that if you fail to pass the exam successfully after purchasing our product, we are willing to provide you with a 100% full refund.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• Attacks and Exploits: This extensive topic trains cybersecurity analysts to analyze data and prioritize attacks. Analysts will learn how to conduct network, authentication, host-based, web application, cloud, wireless, and social engineering attacks using appropriate tools. Understanding specialized systems and automating attacks with scripting will also be emphasized.
Topic 2	• Post-exploitation and Lateral Movement: Cybersecurity analysts will gain skills in establishing and maintaining persistence within a system. This topic also covers lateral movement within an environment and introduces concepts of staging and exfiltration. Lastly, it highlights cleanup and restoration activities, ensuring analysts understand the post-exploitation phase's responsibilities.
Topic 3	• Engagement Management: In this topic, cybersecurity analysts learn about pre-engagement activities, collaboration, and communication in a penetration testing environment. The topic covers testing frameworks, methodologies, and penetration test reports. It also explains how to analyze findings and recommend remediation effectively within reports, crucial for real-world testing scenarios.
Topic 4	• Vulnerability Discovery and Analysis: In this section, cybersecurity analysts will learn various techniques to discover vulnerabilities. Analysts will also analyze data from reconnaissance, scanning, and enumeration phases to identify threats. Additionally, it covers physical security concepts, enabling analysts to understand security gaps beyond just the digital landscape.
Topic 5	• Reconnaissance and Enumeration: This topic focuses on applying information gathering and enumeration techniques. Cybersecurity analysts will learn how to modify scripts for reconnaissance and enumeration purposes. They will also understand which tools to use for these stages, essential for gathering crucial information before performing deeper penetration tests.

>> Valid Test PT0-003 Test <<

CompTIA Valid Test PT0-003 Test: CompTIA PenTest+ Exam - PassLeader Providers you Best Reliable Test Forum

We provide first-rate service on the PT0-003 learning prep to the clients and they include the service before and after the sale, 24-hours online customer service and long-distance assistance, the refund service and the update service. The client can try out our and download PT0-003 Guide materials freely before the sale and if the client have problems about our PT0-003 study braindumps after the sale they can contact our customer service at any time.

CompTIA PenTest+ Exam Sample Questions (Q273-Q278):

NEW QUESTION # 273
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

- A. External
- B. Segmentation
- C. Mobile
- D. Web

Answer: A

Explanation:
An external assessment focuses on testing the security of internet-facing services. Here's why option C is correct:
* External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.
* Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It's more relevant to internal network architecture.
* Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
* Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.
References from Pentest:
* Horizontall HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.
* Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.
Conclusion:
Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.

NEW QUESTION # 274
A penetration tester identifies the following open ports during a network enumeration scan:
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
443/tcp open https
27017/tcp open mongodb
50123/tcp open ms-rpc
Which of the following commands did the tester use to get this output?

- A. nmap -sV 10.10.10.10
- B. nmap -sV -Pn -p- 10.10.10.10
- C. nmap -Pn -w 10.10.10.10
- D. nmap -Pn -A 10.10.10.10

Answer: B

Explanation:
To detect all open ports and enumerate services, the tester needs to:
Use -sV (Service Version Detection)
Use -Pn (Disables ICMP ping to bypass firewalls)
Use -p- (Scans all 65,535 TCP ports)
nmap -sV -Pn -p- 10.10.10.10 (Option D):
This command performs full-port scanning, including high-numbered ports like 50123/tcp (ms-rpc).
Without -p-, high ports would be missed.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Nmap Scanning Techniques" Incorrect options:
Option A (-A): Includes OS detection but does not guarantee scanning all ports.
Option B (-sV without -p-): Scans default ports only, missing 50123/tcp.
Option C (-w): Invalid Nmap flag.

NEW QUESTION # 275
A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks. To avoid disrupting this user's work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

- A. Change the password of the root user and revert after the test.
- B. Add a web shell to the root of the website.
- C. Add a new user with ID 0 to the /etc/passwd file.
- D. Upgrade the reverse shell to a true TTY terminal.

Answer: C

Explanation:
The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won't disrupt the other user's work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

NEW QUESTION # 276
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?

- A. Remote access
- B. File sharing
- C. Database
- D. Email

Answer: B

NEW QUESTION # 277
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

- A. OSSTMM
- B. OWASP MASVS

- C. MITRE ATT&CK
- D. CREST

Answer: A

Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle.
OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.
OWASP MASVS: This is a framework for mobile application security verification and does not have a 14-component life cycle.
MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.
CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.

NEW QUESTION # 278
.....

Under the leadership of a professional team, we have created the most efficient learning PT0-003 training guide for our users. Our users use their achievements to prove that we can get the most practical knowledge in the shortest time. PT0-003 exam questions are tested by many users and you can rest assured. If you want to spend the least time to achieve your goals, PT0-003 Learning Materials are definitely your best choice. You can really try it we will never let you down!

What's more, part of that PassLeader PT0-003 dumps now are free: https://drive.google.com/open?id=16IgCikrBz_cJv2MMHiOUoq6tFpWSikyh