Pass Guaranteed Quiz Marvelous CompTIA PT0-003 - CompTIA PenTest+ Exam Actual Test

P.S. Free & New PT0-003 dumps are available on Google Drive shared by Pass4guide: https://drive.google.com/open?id=1pXx3D0IVDSJimbtflE-6eIE7CSsw2g0X

Pass4guide CompTIA PenTest+ Exam (PT0-003) exam questions are consistently updated to make sure they are according to the CompTIA latest exam syllabus. If you choose Pass4guide, you can be sure that you'll always get the updated and real PT0-003 exam questions, which are essential to go through the PT0-003 test in one go. In addition, we also offer up to 1 year of free CompTIA PT0-003 certification exam question updates. These free updates ensure that candidates get access to the latest CompTIA exam questions even after they have made their initial purchase.

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	• 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.
Topic 3	• 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 4	• 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 5	• 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.

Certification PT0-003 Dumps | Online PT0-003 Tests

You have to upgrade your skills and knowledge then you will be in a position to compete in the modern world. The CompTIA PT0-003 certification offers a great way to learn new in-demand skills and upgrade your knowledge level. To do this you just need to enroll in the PT0-003 Exam and put in your efforts to pass this career booster PT0-003 certification exam.

CompTIA PenTest+ Exam Sample Questions (Q85-Q90):

NEW QUESTION # 85
During a security assessment, a penetration tester wants to compromise user accounts without triggering IDS /IPS detection rules. Which of the following is the most effective way for the tester to accomplish this task?

- A. Crack user accounts using compromised hashes.
- B. Bypass authentication using SQL injection.
- C. Brute force accounts using a dictionary attack.
- D. Compromise user accounts using an XSS attack.

Answer: A

Explanation:
To avoid triggering IDS/IPS alerts, the attacker should use offline cracking on compromised hashes rather than direct brute-force attempts.
Crack user accounts using compromised hashes (Option A):
Hashes can be cracked offline using tools like Hashcat or John the Ripper.
No direct login attempts, avoiding detection by security systems.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Password Cracking Techniques and Evasion" Incorrect options:
Option B (Brute force): Generates excessive failed logins, triggering IDS/IPS alerts.
Option C (SQL injection): Exploits database vulnerabilities, not direct account compromise.
Option D (XSS attack): Can steal cookies but does not directly compromise accounts.

NEW QUESTION # 86
A penetration tester is required to perform a vulnerability scan that reduces the likelihood of false positives and increases the true positives of the results. Which of the following would MOST likely accomplish this goal?

- A. Using Nmap as the root user
- B. Using Nessus with credentials
- C. Using OpenVAS in default mode
- D. Using OWASP ZAP

Answer: B

Explanation:
Using credentials during a vulnerability scan allows the scanner to gather more detailed information about the target system, including installed software, patch levels, and configuration settings. This helps to reduce the likelihood of false positives and increase the true positives of the results. Nessus is a popular vulnerability scanner that supports credential-based scanning and can be used to accomplish this goal. OpenVAS and Nmap are also popular scanning tools, but using default mode or running as the root user alone may not provide the necessary level of detail for accurate vulnerability identification. OWASP ZAP is a web application scanner and may not be applicable for non-web-based targets.

NEW QUESTION # 87
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

- A. Library injection
- B. Kiosk escape
- C. Arbitrary code execution
- D. Process hollowing

Answer: B

Explanation:
A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system.
Kiosk Escape: This attack targets environments where user access is intentionally limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.
Arbitrary Code Execution: This involves running unauthorized code on the system, but the scenario described is more about escaping a restricted environment.
Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.
Library Injection: This involves injecting malicious code into a running process by loading a malicious library, which is not the focus in this scenario.

NEW QUESTION # 88
A company's incident response team determines that a breach occurred because a penetration tester left a web shell. Which of the following should the penetration tester have done after the engagement?

- A. Turn off command-and-control infrastructure
- B. Enable a host-based firewall on the machine
- C. Remove utilized persistence mechanisms on client systems
- D. Revert configuration changes made during the engagement

Answer: C

Explanation:
Comprehensive and Detailed
The immediate and mandatory post-engagement action after completing an authorized penetration test is to remove any accounts, implants, backdoors, web shells, scheduled tasks, or other persistence mechanisms that were created or used during the test. Leaving persistence (a web shell in this case) is exactly what caused the breach and is an unacceptable post-test lapse.
Why B is correct:
Persistence mechanisms provide continued unauthorized access and are a direct security risk if not removed. Removing them returns the environment to its pre-test security posture and prevents later compromise by third parties.
Removal of persistence is a standard requirement in rules of engagement and in post-test cleanup checklists.
Why the other answers are incomplete or secondary:
A . Enable a host-based firewall on the machine - a reasonable defensive step if missing, but it does not replace removing the persistence that was the cause of the breach.
C . Revert configuration changes made during the engagement - also important and should be done, but the highest priority is removing active persistence that gives access. (Both B and C are valid cleanup activities; B is the single best answer given the question.) D . Turn off command-and-control infrastructure - this is appropriate for the tester's own infrastructure, but the critical action on the client side is removing client-side persistence. Also, turning off C2 after the test is expected, but will not remediate the remaining web shell on the client.
CompTIA PT0-003 Mapping:
Domain 5.0 Reporting and Communication - post-engagement cleanup and handoff (remediation actions, removal of test artifacts, maintaining chain of custody and evidence, and returning environment to agreed baseline).

NEW QUESTION # 89
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?

- A. ..nmap -sX -sC target.company.com
- B. ..nmap -sS -sV -F target.company.com
- C. ..nmap -sU -sV -T4 -F target.company.com
- D. ..nmap -sT -v -T5 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.

NEW QUESTION # 90
.....

□ Search for □ PT0-003 □ and download it for free immediately on ➽ www.practicevce.com □ □Latest PT0-003 Test Testking

- CompTIA PenTest+ Exam study questions torrent - PT0-003 training study guide - CompTIA PenTest+ Exam practice pdf dumps □ Search for ➥ PT0-003 □ and download it for free on □ www.pdfvce.com □ website □Certification PT0-003 Dump
- 2026 CompTIA PT0-003: CompTIA PenTest+ Exam Perfect Actual Test □ Immediately open [www.pdfdumps.com] and search for □ PT0-003 □ to obtain a free download □PT0-003 Book Free
- mekkawyacademy.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PT0-003 dumps are available on Google Drive shared by Pass4guide: https://drive.google.com/open?id=1pXx3D0IVDSJimbtflE-6eIE7CSsw2g0X