Quiz CompTIA - High Hit-Rate PT0-003 - CompTIA PenTest+ Exam Latest Exam Pass4sure

2025 Latest Itexamguide PT0-003 PDF Dumps and PT0-003 Exam Engine Free Share: https://drive.google.com/open?id=1Atm-80xYRtNoLmTrSH1x--PqwQW8Dzsi

Through years of persistent efforts and centering on the innovation and the clients-based concept, our company has grown into the flagship among the industry. Our company struggles hard to improve the quality of our PT0-003 study materials and invests a lot of efforts and money into the research and innovation of our PT0-003 Study Materials. Our brand fame in the industry is like the Microsoft in the computer industry, Google in the internet industry and Apple in the cellphone industry. High quality, considerate service, constant innovation and the concept of customer first are the four pillars of our company.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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	• 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.

>> PT0-003 Latest Exam Pass4sure <<

CompTIA PT0-003 Latest Exam Pass4sure: CompTIA PenTest+ Exam - Itexamguide Official Pass Certify

Facing the incoming CompTIA PT0-003 Exam, you may feel stained and anxious, suspicious whether you could pass the exam smoothly and successfully. Actually, you must not impoverish your ambition. Our suggestions are never boggle at difficulties. It is your right time to make your mark. Preparation of exam without effective materials is just like a soldier without gun.

CompTIA PenTest+ Exam Sample Questions (Q210-Q215):

NEW QUESTION # 210
A company developed a new web application to allow its customers to submit loan applications. A penetration tester is reviewing the application and discovers that the application was developed in ASP and used MSSQL for its back-end database. Using the application's search form, the penetration tester inputs the following code in the search input field:
IMG SRC=vbscript:msgbox ("Vulnerable_to_Attack") ;
>originalAttribute="SRC"originalPath="vbscript;msgbox ("Vulnerable_to_Attack ") ;>" When the tester checks the submit button on the search form, the web browser returns a pop-up windows that displays "Vulnerable_to_Attack." Which of the following vulnerabilities did the tester discover in the web application?

- A. Cross-site request forgery
- B. Cross-site scripting
- C. Command injection
- D. SQL injection

Answer: B

NEW QUESTION # 211
During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

- A. Rootkit
- B. On-path
- C. Logic bomb
- D. Buffer overflow

Answer: A

Explanation:
A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host's operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.
* Definition and Purpose:
* Rootkits are primarily used to gain and maintain root access (administrative privileges) on a system.
* They disguise themselves as legitimate software or integrate deeply into the operating system to avoid detection.
* Mechanisms of Action:
* Kernel Mode Rootkits: These operate at the kernel level, which is the core of the operating system, making them very powerful and hard to detect.
* User Mode Rootkits: These run in the same space as user applications, intercepting and altering standard system API calls to hide their presence.
* Bootkits: These infect the Master Boot Record (MBR) or Volume Boot Record (VBR) and load before the operating system, making them extremely difficult to detect and remove.
* Detection and Prevention:
* Detection Tools: Tools like RootkitRevealer, Chkrootkit, and rkhunter can help in identifying rootkits.
* Prevention: Regular system updates, use of strong antivirus and anti-malware solutions, and integrity checking tools like Tripwire can help in preventing rootkit infections.
* Real-World Examples:
* Sony BMG Rootkit: In 2005, Sony BMG included a rootkit in their digital rights management (DRM) software on music CDs. The rootkit hid files and processes, leading to a major scandal when it was discovered.
* Stuxnet: This sophisticated worm included a rootkit component to hide its presence on infected systems, making it one of the most

infamous examples of rootkit use in a cyber attack.
* References from Pentesting Literature:
* In "Penetration Testing - A Hands-on Introduction to Hacking" by Georgia Weidman, rootkits are discussed in the context of post-exploitation, where maintaining access to the compromised system is crucial.
* Various HTB write-ups, such as the analysis of complex attacks involving multiple stages of exploitation, often highlight the use of rootkits in maintaining persistent access.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups on sophisticated attacks

NEW QUESTION # 212
A penetration tester completes a scan and sees the following Nmap output on a host:
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open snmp
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp0
The tester wants to obtain shell access. Which of the following related exploits should the tester try first?

- A. auxiliary/scanner/snmp/snmp_login
- B. exploit/windows/smb/ms17_010_eternalblue
- C. exploit/windows/smb/ms08_067_netapi
- D. exploit/windows/smb/psexec

Answer: B

NEW QUESTION # 213
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

- A. Netcat
- B. Wireshark
- C. Nmap
- D. Dnsenum

Answer: D

Explanation:
Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses.
Here's why option A is correct:
* Dnsenum: This tool is used for DNS enumeration and can gather information about a domain's DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network's domain structure.
* Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
* Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
* Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
* Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target's domain structure.
* Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.

NEW QUESTION # 214
A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to

capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

- A. Replay
- B. Evil twin
- C. Key reinstallation
- D. Deauthentication

Answer: D

Explanation:
Deauth will make the client connect again

NEW QUESTION # 215
.....

There is no doubt that advanced technologies are playing an important role in boosting the growth of CompTIA companies. This is the reason why the employees have now started upgrading their skillset with the CompTIA PenTest+ Exam (PT0-003) certification exam because they want to work with those latest applications and save their jobs. They attempt the CompTIA PenTest+ Exam (PT0-003) exam to validate their skills and try to get their dream job.

P.S. Free 2025 CompTIA PT0-003 dumps are available on Google Drive shared by Itexamguide: https://drive.google.com/open?id=1Atm-80xYRtNoLmTrSH1x--PqwQW8Dzsi