PT0-003 Trustworthy Dumps, Upgrade PT0-003 Dumps

BONUS!!! Download part of TrainingDump PT0-003 dumps for free: https://drive.google.com/open?id=1BAF8ViZhCzRXJIroRIDwTv_63oOeV63r

You will gain a clear idea of every CompTIA PT0-003 exam topic by practicing with Web-based and desktop CompTIA PT0-003 practice test software. You can take CompTIA PT0-003 Practice Exam many times to analyze and overcome your weaknesses before the final CompTIA PT0-003 exam.

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	• 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 3	• 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 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	• 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.

Upgrade PT0-003 Dumps, Reliable PT0-003 Exam Braindumps

Our passing rate is very high to reach 99% and our PT0-003 exam torrent also boost high hit rate. Our PT0-003 study questions are compiled by authorized experts and approved by professionals with years of experiences. They are compiled according to the latest development conditions in the theory and practice and the questions and answers are based on real exam. Our study materials can improves your confidence for real exam and will help you remember the exam questions and answers that you will take part in. You can choose the version which suits you mostly. Our CompTIA PenTest+ Exam exam torrents simplify the important information and seize the focus to make you master the PT0-003 Test Torrent in a short time.

CompTIA PenTest+ Exam Sample Questions (Q28-Q33):

NEW QUESTION # 28
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62 Which of the following commands can be used to further attack the website?

- A. /var/www/html/index.php;whoami
- B. ../../../../../../../../../../etc/passwd
- C. 1 UNION SELECT 1, DATABASE(),3--
- D. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>

Answer: C

NEW QUESTION # 29
A company hires a penetration tester to perform an external attack surface review as part of a security engagement. The company informs the tester that the main company domain to investigate is comptia.org.
Which of the following should the tester do to accomplish the assessment objective?

- A. Perform information-gathering techniques to review internet-facing assets for the company.
- B. Perform a phishing assessment to try to gain access to more resources and users' computers.
- C. Perform a physical security review to identify vulnerabilities that could affect the company.
- D. Perform a vulnerability assessment over the main domain address provided by the client.

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
An external attack surface review focuses on identifying publicly accessible assets that an attacker could exploit. The first step in this process is information gathering, which involves enumerating domains, subdomains, public IPs, DNS records, and other internet-facing resources. This is done using passive reconnaissance tools such as Whois, Shodan, Google Dorking, and OSINT techniques.
Option A is correct because it aligns with the assessment goal-finding public-facing systems and their vulnerabilities before an attacker does.
Option B (phishing assessment) is incorrect because it involves social engineering, which is not part of an external attack surface review.
Option C (physical security review) is incorrect as it pertains to physical penetration testing, not an external attack analysis.
Option D (vulnerability assessment) is incorrect because a vulnerability assessment is a later step after reconnaissance. The first step is identifying assets through information gathering.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Chapter 4 (Information Gathering and OSINT).

NEW QUESTION # 30
A penetration tester finishes a security scan and uncovers numerous vulnerabilities on several hosts. Based on the targets' EPSS (Exploit Prediction Scoring System) and CVSS (Common Vulnerability Scoring System) scores, which of the following targets is the most likely to get attacked?

- A. Target 3: EPSS Score = 0.6, CVSS Score = 1
- B. Target 1: EPSS Score = 0.6, CVSS Score = 4
- C. Target 2: EPSS Score = 0.3, CVSS Score = 2
- D. Target 4: EPSS Score = 0.4, CVSS Score = 4.5

Answer: B

Explanation:
The EPSS (Exploit Prediction Scoring System) estimates how likely a vulnerability is to be exploited. Higher EPSS scores indicate a higher likelihood of exploitation.
* Option A (Target 1) #:
* EPSS 0.6 (60% chance of exploitation)
* CVSS 4 (Medium severity)
* # Best candidate since it has the highest likelihood of exploitation.
* Option B (Target 2) #: EPSS 0.3 (30%) is lower, making it less likely to be attacked.
* Option C (Target 3) #: EPSS 0.6 is high, but CVSS 1 is very low, meaning the vulnerability is not critical.
* Option D (Target 4) #: CVSS 4.5 is higher, but EPSS 0.4 is lower, meaning attackers are less likely to exploit it.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Vulnerability Prioritization with EPSS & CVSS

NEW QUESTION # 31
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?

- A. Target 3: EPSS Score = 0.6 and CVSS Score = 1
- B. Target 4: EPSS Score = 0.4 and CVSS Score = 4.5
- C. Target 2: EPSS Score = 0.3 and CVSS Score = 2
- D. Target 1: EPSS Score = 0.6 and CVSS Score = 4

Answer: D

Explanation:
EPSS and CVSS Analysis:
EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.
CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.
Rationale:
Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.
Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.
CompTIA Pentest+ Reference:
Domain 2.0 (Information Gathering and Vulnerability Identification)

NEW QUESTION # 32
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

- A. XSS
- B. SSRF
- C. SQL injection
- D. Server-side template injection

Answer: A

Explanation:

Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users.
XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.

NEW QUESTION # 33
.....

With so many methods can boost individual competitiveness, people may be confused, which can really bring them a glamorous work or brighter future? We are here to tell you that a PT0-003 certification definitively has everything to gain and nothing to lose for everyone. You might have seen lots of advertisements about PT0-003 learning question, there are so many types of PT0-003 exam material in the market, why you should choose us? Our reasons are as follow. Our PT0-003 test guide is test-oriented, which makes the preparation become highly efficient.