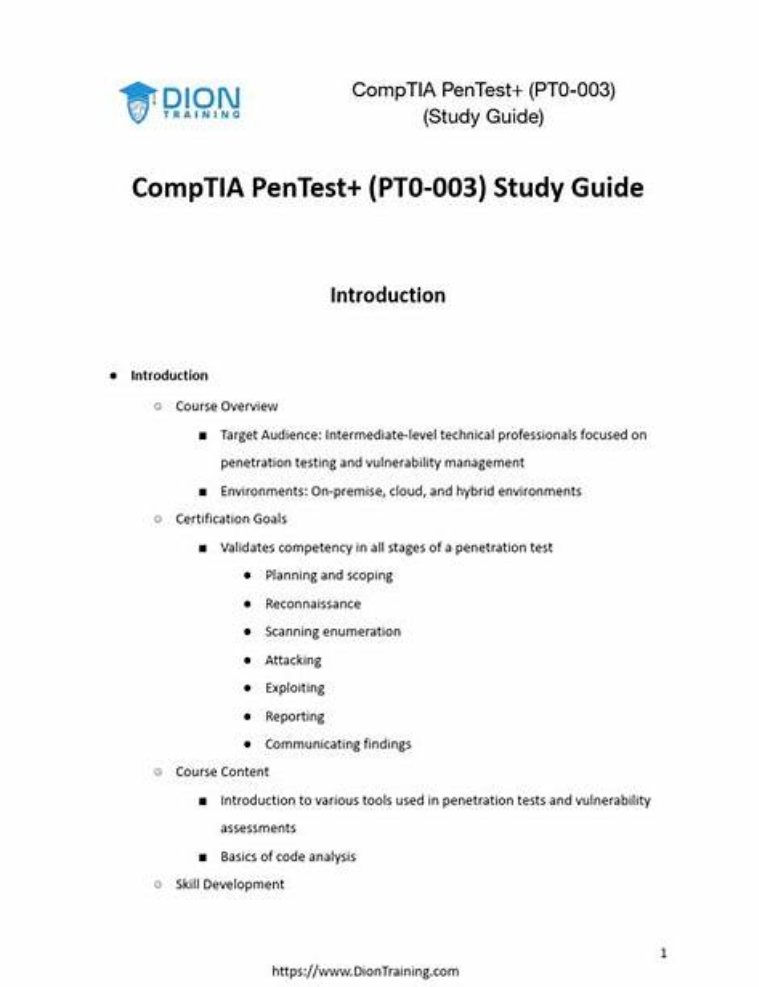
New PT0-003 Test Discount - PT0-003 Test Topics Pdf


CompTIA PenTest+ (PT0-003)
(Study Guide)

CompTIA PenTest+ (PT0-003) Study Guide

Introduction

- Introduction
  - Course Overview
    - Target Audience: Intermediate-level technical professionals focused on penetration testing and vulnerability management
    - Environments: On-premise, cloud, and hybrid environments
  - Certification Goals
    - Validates competency in all stages of a penetration test
      - Planning and scoping
      - Reconnaissance
      - Scanning enumeration
      - Attacking
      - Exploiting
      - Reporting
      - Communicating findings
  - Course Content
    - Introduction to various tools used in penetration tests and vulnerability assessments
    - Basics of code analysis
  - Skill Development

1

https://www.DionTraining.com

BTW, DOWNLOAD part of DumpsTorrent PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1C_HV3xVS_HXZZ_Ecrf6TnG9-sZUQ0XZJ

If you would like to use all kinds of electronic devices to prepare for the PT0-003 exam, with the online app version of our PT0-003 study materials, you can just feel free to practice the questions in our PT0-003 training materials no matter you are using your mobile phone, personal computer, or tablet PC. In addition, another strong point of the online app version is that it is convenient for you to use even though you are in offline environment. In other words, you can prepare for your PT0-003 Exam with under the guidance of our PT0-003 training materials anywhere at any time.

In this way, the CompTIA PT0-003 certified professionals can not only validate their skills and knowledge level but also put their careers on the right track. By doing this you can achieve your career objectives. To avail of all these benefits you need to pass the CompTIA PenTest+ Exam (PT0-003) exam which is a difficult exam that demands firm commitment and complete CompTIA PT0-003 exam questions preparation.

>> New PT0-003 Test Discount <<

CompTIA PT0-003 Online Practice Test Engine Recommendation

You don't need to worry about wasting your precious time but failing to get the PT0-003certification. With our PT0-003 practice guide, your success is 100% guaranteed. Tens of thousands of people have used our PT0-003 Study Materials and the pass rate of the exam is high as 98% to 100%. This means as long as you learn with our PT0-003 learning quiz, you will pass the exam without doubt.

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	• 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 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	• 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.

CompTIA PenTest+ Exam Sample Questions (Q243-Q248):

NEW QUESTION # 243
A penetration tester would like to crack a hash using a list of hashes and a predefined set of rules. The tester runs the following command:
hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule
Which of the following is the penetration tester using to crack the hash?

- A. Dictionary
- B. Brute-force method
- C. Rainbow table
- D. Hybrid attack

Answer: A

Explanation:
The command hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule indicates that the penetration tester is using a dictionary attack combined with rule-based modifications. The -a 0 option specifies a dictionary attack mode, where .\rockyou.txt is the dictionary file containing potential passwords, and -r .\rules\replace.rule applies predefined rules to mutate these passwords. This method leverages a known list of potential passwords and augments them with additional variations based on the rules provided.

NEW QUESTION # 244
A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives' accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

- A. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.
- B. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.

- C. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
- D. Configure an external domain using a typosquatting technique. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.

Answer: C

Explanation:
To bypass two-factor authentication (2FA) and gain access to the executives' accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.
* Phishing with Evilginx:
* Evilginx is designed to proxy legitimate login pages, capturing credentials and 2FA tokens in the process.
* It uses "phishlets" which are configurations that simulate real login portals.
* Typosquatting:
* Typosquatting involves registering domains that are misspelled versions of legitimate domains (e.
g., example.co instead of example.com).
* This technique tricks users into visiting the malicious domain, thinking it's legitimate.
* Steps:
* Configure an External Domain: Register a typosquatting domain similar to the company's domain.
* Set Up Evilginx: Install and configure Evilginx on a server. Use a phishlet that mimics the company's mail portal.
* Send Phishing Emails: Craft phishing emails targeting the executives, directing them to the typosquatting domain.
* Capture Credentials and 2FA Tokens: When executives log in, Evilginx captures their credentials and session tokens, effectively bypassing 2FA.
Pentest References:
* Phishing: Social engineering technique to deceive users into providing sensitive information.
* Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
* OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.

NEW QUESTION # 245
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. User hashes sent over SMB
- B. IP addresses
- C. Multiple handshakes
- D. Encrypted file transfers

Answer: B

NEW QUESTION # 246
A penetration tester obtains the following output during an Nmap scan:
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
1801/tcp open msmq
2103/tcp open msrpc
3389/tcp open ms-wbt-server
Which of the following should be the next step for the tester?

- A. Enumerate shares and search for vulnerabilities on the SMB service.
- B. Execute a new Nmap command to search for another port.
- C. Execute a brute-force attack against the Remote Desktop Services.
- D. Search for vulnerabilities on msrpc.

Answer: A

Explanation:
The presence of SMB (port 445) and MSRPC (port 135) indicates potential Windows network services that could be vulnerable to misconfigurations or exploits.
Enumerate shares and search for vulnerabilities on SMB (Option B):
SMB (Server Message Block) allows file and printer sharing. Misconfigured or open shares could contain sensitive data.
Tools like enum4linux or smbclient can be used to list available shares and check for anonymous access.
SMB vulnerabilities (e.g., EternalBlue - CVE-2017-0144) can be exploited for remote code execution.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "SMB Enumeration and Exploitation" Incorrect options:
Option A (Search vulnerabilities on msrpc): MSRPC (Microsoft Remote Procedure Call) is not commonly exploited directly unless an SMB or RDP vulnerability is found.
Option C (Brute-force RDP): Brute-force attacks generate excessive failed login attempts, triggering security alerts.
Option D (Search for another port): The open ports already provide sufficient attack vectors.

NEW QUESTION # 247
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

- A. Run KARMA to break the password.
- B. Enable monitoring mode using Aircrack-ng.
- C. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
- D. Research WiGLE.net for potential nearby client access points.

Answer: B

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes.
Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
* Preparation:
* Wireless USB Dongle: Ensure the wireless USB dongle is compatible with monitoring mode and packet injection.
* Aircrack-ng Suite: Use the Aircrack-ng suite, a popular set of tools for wireless network auditing.
* Enable Monitoring Mode:
* Command: Use the airmon-ng tool to enable monitoring mode on the wireless interface.
Step-by-Step Explanationairmon-ng start wlan0
* Verify: Check if the interface is in monitoring mode.
iwconfig
* Capture WPA2 Handshakes:
* Airodump-ng: Use airodump-ng to start capturing traffic and handshakes.
airodump-ng wlan0mon
* References from Pentesting Literature:
* Enabling monitoring mode is a fundamental step in wireless penetration testing, discussed in guides like "Penetration Testing - A Hands-on Introduction to Hacking".
* HTB write-ups often start with enabling monitoring mode before proceeding with capturing WPA2 handshakes.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION # 248
.....

Our PT0-003 learning questions are famous for that they are undeniable excellent products full of benefits, so our exam materials can spruce up our own company image. Besides, our PT0-003 study quiz is priced reasonably, so we do not overcharge you at all. Not only the office staff can buy it, the students can also afford it. Meanwhile, our PT0-003 Exam Materials are demonstrably high effective to help you get the essence of the knowledge which was convoluted. You will get more than you can imagine by our PT0-003 learning guide.

Study Materials

- Valid Braindumps PT0-003 Ebook □ PT0-003 Valid Exam Preparation □ PT0-003 Pass Guaranteed □ ☀ www.pdfvce.com □☀□ is best website to obtain □ PT0-003 □ for free download □PT0-003 Training Kit
- Reliable PT0-003 Guide Dumps: CompTIA PenTest+ Exam - PT0-003 Test Prep Materials - www.vce4dumps.com □ The page for free download of 【 PT0-003 】 on ➤ www.vce4dumps.com □ will open immediately □Free PT0-003 Pdf Guide
- PT0-003 Valid Exam Camp □ PT0-003 Training Kit □ PT0-003 Sample Questions Answers □ Search on ➠ www.pdfvce.com □ for [PT0-003] to obtain exam materials for free download ◂PT0-003 Training Kit
- Three CompTIA PT0-003 Exam Practice Questions Formats □ Search for ➤ PT0-003 □ on { www.torrentvce.com } immediately to obtain a free download □Valid Braindumps PT0-003 Ppt
- PT0-003 Exam Question □ PT0-003 Valid Exam Camp □ PT0-003 Exam Question □ Open □ www.pdfvce.com □ and search for □ PT0-003 □ to download exam materials for free □Latest PT0-003 Test Pdf
- First-grade New PT0-003 Test Discount - Trustable Source of PT0-003 Exam □ The page for free download of ➽ PT0-003 □ on □ www.vce4dumps.com □ will open immediately □Free PT0-003 Pdf Guide
- Valid Braindumps PT0-003 Ppt □ PT0-003 Pass4sure Exam Prep □ PT0-003 Sample Questions Answers □ Go to website ➽ www.pdfvce.com □ open and search for □ PT0-003 □ to download for free □PT0-003 Pass Guaranteed
- New PT0-003 Test Discount - Realistic CompTIA PenTest+ Exam Test Topics Pdf Pass Guaranteed Quiz □ Search for ☀ PT0-003 □☀□ and obtain a free download on ➽ www.torrentvce.com □ □PT0-003 Exam Tests
- PT0-003 Exam Tests □ Latest PT0-003 Test Pdf □ Valid Braindumps PT0-003 Ppt ～ Search on □ www.pdfvce.com □ for （ PT0-003 ） to obtain exam materials for free download □PT0-003 Pass Guaranteed
- High-efficient PT0-003 Training materials are helpful Exam Questions - www.practicevce.com □ Search for ▹ PT0-003 ◃ and download exam materials for free through □ www.practicevce.com □ □PT0-003 Exam Practice
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.notebook.ai, futds.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of DumpsTorrent PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1C_HV3xVS_HXZZ_Ecrf6TnG9-sZUQ0XZJ