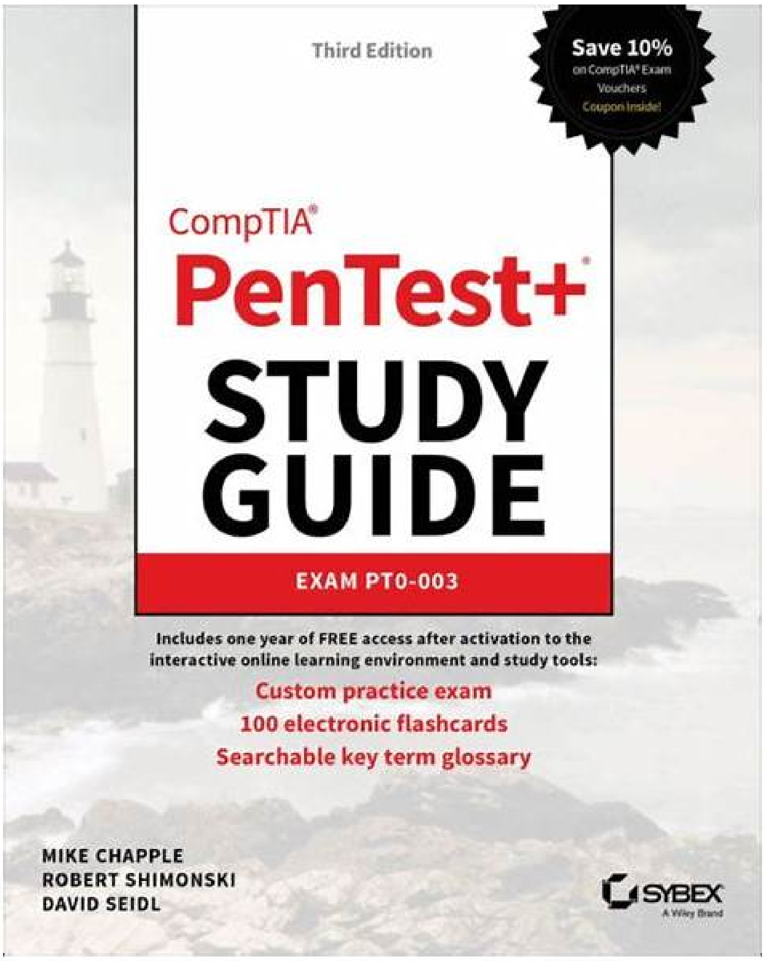
PT0-003 Associate Level Exam & PT0-003 Valid Exam Cost


Third Edition
Save 10% on CompTIA® Exam Vouchers Coupon inside!
CompTIA®
PenTest+®
STUDY GUIDE
EXAM PT0-003
Includes one year of FREE access after activation to the interactive online learning environment and study tools:
Custom practice exam
100 electronic flashcards
Searchable key term glossary
MIKE CHAPPLE
ROBERT SHIMONSKI
DAVID SEIDL
SYBEX
A Wiley Brand

BONUS!!! Download part of PassLeader PT0-003 dumps for free: https://drive.google.com/open?id=1yjq7HWTlqf8O7xNdCDqnoTFLABaJ8IFF

PassLeader website is fully equipped with resources and the questions of CompTIA PT0-003 exam, it also includes the CompTIA PT0-003 exam practice test. Which can help candidates prepare for the exam and pass the exam. You can download the part of the trial exam questions and answers as a try. PassLeader provide true and comprehensive exam questions and answers. With our exclusive online CompTIA PT0-003 Exam Training materials, you'll easily through CompTIA PT0-003 exam. Our site ensure 100% pass rate.

We have dedicated staff to update all the content of PT0-003 exam questions every day. So you don't need to worry about that you buy the materials so early that you can't learn the last updated content. And even if you failed to pass the exam for the first time, as long as you decide to continue to use PT0-003 torrent prep, we will also provide you with the benefits of free updates within one year and a half discount more than one year. PT0-003 Test Guide use a very easy-to-understand language. So even if you are a newcomer, you don't need to worry that you can't understand the contents. Industry experts hired by PT0-003 exam questions also explain all of the difficult professional vocabulary through examples, forms, etc. You can completely study alone without the help of others.

>> PT0-003 Associate Level Exam <<

PT0-003 Valid Exam Cost & New PT0-003 Exam Simulator

No matter where you are or what you are, PT0-003 practice questions promises to never use your information for commercial purposes. If you attach great importance to the protection of personal information and want to choose a very high security product, PT0-003 Real Exam is definitely your first choice. And we always have a very high hit rate on the PT0-003 study guide by our customers for our high pass rate is high as 98% to 100%.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	- 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 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	- 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	- 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.

CompTIA PenTest+ Exam Sample Questions (Q216-Q221):

NEW QUESTION # 216
A penetration tester writes the following script:
Which of the following is the tester performing?

- A. Scanning a network for specific open ports
- B. Searching for service vulnerabilities
- C. Trying to recover a lost bind shell
- D. Building a reverse shell listening on specified ports

Answer: A

Explanation:
-z zero-I/O mode [used for scanning]
-v verbose
example output of script:
10.0.0.1: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.0.1] 22 (ssh) open
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out
https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for

NEW QUESTION # 217
A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

Part 1:
. Analyze the output and select the command to exploit the vulnerable service.
Part 2:
. Analyze the output from each command.
Select the appropriate set of commands to escalate privileges.
Identify which remediation steps should be taken.

Answer:

Explanation:
See the Explanation below for complete solution.
Explanation:
The command that would most likely exploit the services is:
hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
The appropriate set of commands to escalate privileges is:
echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
The remediations that should be taken after the successful privilege escalation are:
* Remove the SUID bit from cp.
* Make backup script not world-writable.
Comprehensive Step-by-Step Explanation of the Simulation
Part 1: Exploiting Vulnerable Service
* Nmap Scan Analysis
* Command: nmap -sC -T4 192.168.10.2
* Purpose: This command runs a default script scan with timing template 4 (aggressive).
* Output:
bash
Copy code

```
Port State Service
22/tcp open ssh
23/tcp closed telnet
80/tcp open http
111/tcp closed rpcbind
445/tcp open samba
3389/tcp closed rdp
```

Ports open are SSH (22), HTTP (80), and Samba (445).
* Enumerating Samba Shares
* Command: enum4linux -S 192.168.10.2
* Purpose: To enumerate Samba shares and users.
* Output:
makefile
Copy code

```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x42]
user:[syslog] rid:[0x4ba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
```

We identify a user lowpriv.
* Selecting Exploit Command
* Hydra Command: hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
* Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.
* Explanation:
* -l lowpriv: Specifies the username.
* -P 500-worst-passwords.txt: Specifies the password list.
* -t 4: Uses 4 tasks/threads for the attack.
* ssh://192.168.10.2:22: Specifies the SSH service and port.
* Executing the Hydra Command
* Result: Successful login as lowpriv user if a match is found.

Part 2: Privilege Escalation and Remediation
* Finding SUID Binaries and Configuration Files
* Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l
* Purpose: To find world-writable files.
* Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l
* Purpose: To find files with SUID permission.
* Command: grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
* Purpose: To identify users with bash shell access.
* Selecting Privilege Escalation Command
* Command: echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
* Purpose: To create a new root user entry in the passwd file.
* Explanation:
* root2: Username.
* 5ZOYXRFHVZ7OY: Password hash.
* ::0:0: User and group ID (root).
* /root: Home directory.
* /bin/bash: Default shell.
* Executing the Privilege Escalation Command
* Result: Creation of a new root user root2 with a specified password.
* Remediation Steps Post-Exploitation
* Remove SUID Bit from cp:
* Command: chmod u-s /bin/cp
* Purpose: Removing the SUID bit from cp to prevent misuse.
* Make Backup Script Not World-Writable:
* Command: chmod o-w /path/to/backup/script
* Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.
Execution and Verification
* Verifying Hydra Attack:
* Run the Hydra command and monitor for successful login attempts.
* Verifying Privilege Escalation:
* After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.
* Implementing Remediation:
* Apply the remediation commands to secure the system and verify the changes have been implemented.
By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION # 218

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

Answer: D

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 # 219

How does Responder work for LLMNR/NBT-NS poisoning, and how does it assist in capturing network credentials?

- A. responder.py -I eth0 -wP
- B. nc -tulpn 1234 192.168.1.2
- C. crackmapexec smb 192.168.1.0/24 -u "user" -p "pass123"
- D. ntlmrelayx.py -t 192.168.1.0/24 -1 1234

Answer: A

Explanation:
The goal is collecting information transmitted over the network during an internal assessment.
* C. responder.py -I eth0 -wP
* Responder is a widely used tool for LLMNR/NBT-NS poisoning and network credential capture.
* By listening on the network interface (-I eth0), it can intercept authentication requests, capture hashes, and perform MITM attacks.
* This directly aligns with network information gathering and interception.
Why not the others?
* A. ntlmrelayx.py: Used for relaying captured NTLM hashes to another target, but it doesn't collect the data directly. Typically used after Responder has captured credentials.
* B. nc -tulpn: Netcat with -tulpn is for listening/port binding, not for capturing network authentication broadcasts.
* D. crackmapexec smb: SMB enumeration/exploitation tool, useful once credentials are known, but not for collecting transmitted data.
CompTIA PT0-003 Objective Mapping:
* Domain 2.0: Information Gathering and Vulnerability Scanning
* 2.3: Given a scenario, gather information by leveraging tools (e.g., Responder for network-based credential capture).

NEW QUESTION # 220

During a security assessment, a penetration tester captures plaintext login credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access.
Which of the following tools is the tester using?

- A. Zed Attack Proxy (ZAP)
- B. Metasploit
- C. Burp Suite
- D. Wireshark

Answer: D

Explanation:
Capturing plaintext credentials in network traffic is done using packet sniffing. Wireshark is the best tool for this task.
* Option A (Burp Suite) #: Used for web application testing and intercepting HTTPS traffic, but not general network sniffing.
* Option B (Wireshark) #: Correct.
* Wireshark is a packet analysis tool that captures unencrypted network traffic, including plaintext credentials.
* Option C (ZAP - Zed Attack Proxy) #: Similar to Burp Suite, but focused on web application security, not network packet capture.
* Option D (Metasploit) #: Metasploit is used for exploitation rather than capturing traffic.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Packet Sniffing & Network Traffic Analysis

NEW QUESTION # 221

......

time immediately. The learning costs you little time and energy and you can commit yourself mainly to your jobs or other important things.

PT0-003 Valid Exam Cost: https://www.passleader.top/CompTIA/PT0-003-exam-braindumps.html

- Braindump PT0-003 Free □ PT0-003 Exam Success □ Test PT0-003 Preparation □ Open website □ www.easy4engine.com □ and search for ➠ PT0-003 □ for free download □Braindump PT0-003 Free
- Marvelous PT0-003 Associate Level Exam - Leader in Qualification Exams - Hot PT0-003 Valid Exam Cost □ Immediately open （ www.pdfvce.com ） and search for 「 PT0-003 」 to obtain a free download □Reliable PT0-003 Exam Pattern
- Top CompTIA PT0-003 Associate Level Exam - Authoritative www.prepawaypdf.com - Leading Offer in Qualification Exams □ Search for □ PT0-003 □ on ✔ www.prepawaypdf.com □✔□ immediately to obtain a free download □Test PT0-003 Preparation
- PT0-003 Test Vce Free □ Test PT0-003 Preparation □ Exam PT0-003 Simulator Free □ [www.pdfvce.com] is best website to obtain □ PT0-003 □ for free download □Real PT0-003 Exam Questions
- Free PT0-003 Practice □ Learning PT0-003 Mode □ PT0-003 Reasonable Exam Price □ The page for free download of ▶ PT0-003 ◀ on □ www.verifieddumps.com □ will open immediately ❈PT0-003 Exam Discount
- Top CompTIA PT0-003 Associate Level Exam - Authoritative Pdfvce - Leading Offer in Qualification Exams □ Search for { PT0-003 } on 【 www.pdfvce.com 】 immediately to obtain a free download □Reliable PT0-003 Exam Pattern
- Evaluate Your Exam Preparation with Online CompTIA PT0-003 Practice Test Engine □ The page for free download of ➠ PT0-003 □ on " www.testkingpass.com " will open immediately □PT0-003 Practice Mock
- Learning PT0-003 Mode □ Reliable PT0-003 Exam Pattern □ Exam PT0-003 Discount □ Easily obtain ➠ PT0-003 □ for free download through （ www.pdfvce.com ） □PT0-003 Reliable Test Vce
- Braindump PT0-003 Free □ PT0-003 Reasonable Exam Price □ PT0-003 Practice Mock □ Search for 「 PT0-003 」 and download exam materials for free through □ www.practicevce.com □ □PT0-003 Exam Success
- Evaluate Your Exam Preparation with Online CompTIA PT0-003 Practice Test Engine □ Open □ www.pdfvce.com □ and search for ▶ PT0-003 ◀ to download exam materials for free □Reliable PT0-003 Test Review
- PT0-003 Exam Success □ PT0-003 Test Vce Free □ Exam PT0-003 Discount □ Go to website □ www.verifieddumps.com □ open and search for □ PT0-003 □ to download for free □Learning PT0-003 Mode
- www.stes.tyc.edu.tw, bbs.t-firefly.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, 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.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.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of PassLeader PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1yjq7HWTlqf8O7xNdCDqnoTFLABaJ8IFF