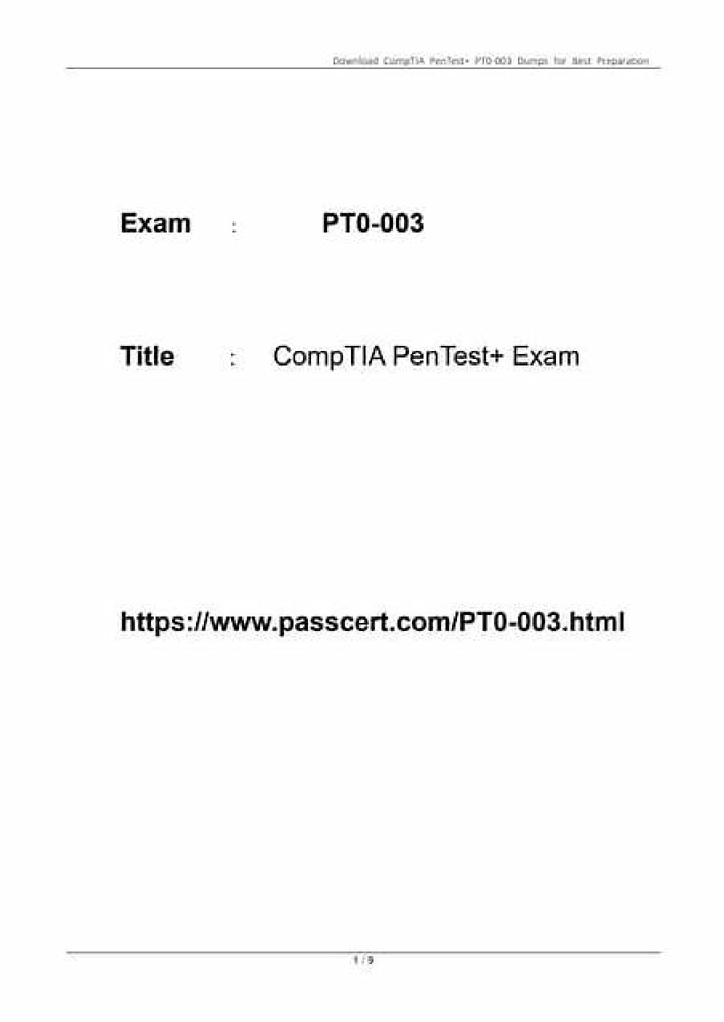
Exam Dumps CompTIA PT0-003 Zip - Reliable PT0-003 Exam Questions



Download CompTIA PenTest+ PT0-003 Dumps for Best Preparation

Exam : PT0-003

Title : CompTIA PenTest+ Exam

https://www.passcert.com/PT0-003.html

1 / 9

The world is changing rapidly and the requirements to the employees are higher than ever before. If you want to find an ideal job and earn a high income you must boost good working abilities and profound major knowledge. Passing PT0-003 certification can help you realize your dreams. If you buy our product, we will provide you with the best PT0-003 Study Materials and it can help you obtain PT0-003 certification. Our product is of high quality and our service is perfect.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	- 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 4	- 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 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.

Reliable PT0-003 Exam Questions - New PT0-003 Exam Cram

We offer free demo PT0-003 questions answers and trial services at ActualTestsIT. You can always check out our PT0-003 certification exam dumps questions that will help you pass the PT0-003 exams. With our well-researched and well-curated exam PT0-003 dumps, you can surely pass the exam in the best marks. We continuously update our products by adding latest questions in our PT0-003 Pdf Files. After the date of purchase, you will receive free updates for one year. You will also be able to get discounts for PT0-003 on complete packages.

CompTIA PenTest+ Exam Sample Questions (Q60-Q65):

NEW QUESTION # 60
During the reconnaissance phase, a penetration tester collected the following information from the DNS records:
A-----> www
A-----> host
TXT --> vpn.comptia.org
SPF---> ip =2.2.2.2
Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

- A. DMARC
- B. CNAME
- C. MX
- D. SOA

Answer: A

Explanation:
DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.
Step-by-Step Explanation
Understanding DMARC:
SPF: Defines which IP addresses are allowed to send emails on behalf of a domain.
DKIM: Provides a way to check that an email claiming to come from a specific domain was indeed authorized by the owner of that domain.
DMARC: Uses SPF and DKIM to determine the authenticity of an email and specifies what action to take if the email fails the authentication checks.
Implementing DMARC:
Create a DMARC policy in your DNS records. This policy can specify to reject, quarantine, or take no action on emails that fail SPF or DKIM checks.
Example DMARC record: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com; Benefits of DMARC:
Helps to prevent email spoofing and phishing attacks.

Provides visibility into email sources through reports.
Enhances domain reputation by ensuring only legitimate emails are sent from the domain.
DMARC Record Components:
v: Version of DMARC.
p: Policy for handling emails that fail the DMARC check (none, quarantine, reject).
rua: Reporting URI of aggregate reports.
ruf: Reporting URI of forensic reports.
pct: Percentage of messages subjected to filtering.
Real-World Example:
A company sets up a DMARC policy with p=reject to ensure that any emails failing SPF or DKIM checks are rejected outright, significantly reducing the risk of phishing attacks using their domain.
Reference from Pentesting Literature:
In "Penetration Testing - A Hands-on Introduction to Hacking," DMARC is mentioned as part of email security protocols to prevent phishing.
HTB write-ups often highlight the importance of DMARC in securing email communications and preventing spoofing attacks.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION # 61
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

- A. Responder
- B. CrackMapExec
- C. Hydra
- D. BloodHound

Answer: B

Explanation:
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:
Option A: Responder
Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
Option B: Hydra
Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
Option C: BloodHound
BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
Option D: CrackMapExec
CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes.
Reference from Pentest:
Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

NEW QUESTION # 62
A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. CentralOps
- B. FOCA

- C. Responder
- D. Netcraft

Answer: B

Explanation:
https://kalilinuxtutorials.com/foca-metadata-hidden-documents/
FOCA (Fingerprinting Organizations with Collected Archives) is a tool that is used to find hidden information in documents available on the web. It can be used to extract metadata from documents such as PDF, Microsoft Office, OpenOffice, and others. The metadata can include information such as the author, creation date, and software used to create the document. FOCA can also extract information from the document's properties such as the title, keywords, and comments. This tool can also identify specific keywords and patterns in the document and can be useful in identifying sensitive information that may have been inadvertently left in the document.

NEW QUESTION # 63
A penetration tester conducted an assessment on a web server. The logs from this session show the following: http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ; DROP TABLE SERVICES; -- Which of the following attacks is being attempted?

- A. Parameter pollution
- B. Cookie hijacking
- C. Session hijacking
- D. Cross-site scripting
- E. Clickjacking

Answer: A

NEW QUESTION # 64
A penetration tester is preparing a credential stuffing attack against a company's website. Which of the following can be used to passively get the most relevant information?

- A. Shodan
- B. HaveIBeenPwned
- C. BeEF
- D. Maltego

Answer: B

Explanation:
HaveIBeenPwned is a website that allows users to check if their personal data has been compromised by data breaches. For a penetration tester preparing a credential stuffing attack, HaveIBeenPwned can provide valuable information about which accounts and passwords have been exposed, making them more likely targets for successful credential stuffing. This passive information gathering tool can help in identifying the most relevant credentials without actively probing the target's systems. The other tools listed (Shodan, BeEF, Maltego) serve different purposes, such as device and service enumeration, client-side exploitation, and information gathering through different means, respectively.

NEW QUESTION # 65
......

Our web-based practice exam software is an online version of the CompTIA PT0-003 practice test. It is also quite useful for instances when you have internet access and spare time for study. To study and pass the CompTIA PT0-003 Exam on the first attempt, our web-based CompTIA PT0-003 practice test software is your best option. You will go through CompTIA PenTest+ Exam mock exams and will see for yourself the difference in your preparation.

Reliable PT0-003 Exam Questions: https://www.actualtestsit.com/CompTIA/PT0-003-exam-prep-dumps.html

- PT0-003 Download Fee □ Latest PT0-003 Exam Pdf □ PT0-003 Valid Dumps Questions □ ➽ www.verifieddumps.com □ is best website to obtain 《 PT0-003 》 for free download □Valid PT0-003 Exam Notes

- PT0-003 Latest Practice Questions □ Exam Dumps PT0-003 Provider □ Latest PT0-003 Exam Pdf □ Search for ☀ PT0-003 □☀□ on （ www.pdfvce.com ） immediately to obtain a free download □Exam PT0-003 Questions Answers
- Exam PT0-003 Questions □ Exam PT0-003 Questions □ Valid PT0-003 Exam Notes □ ▶ www.practicevce.com ◀ is best website to obtain □ PT0-003 □ for free download □PT0-003 Reliable Braindumps Ebook
- Latest PT0-003 Exam Pdf □ Valid PT0-003 Test Camp □ Test PT0-003 Vce Free □ Immediately open ➤ www.pdfvce.com □ and search for ☀ PT0-003 □☀□ to obtain a free download □PT0-003 Best Vce
- Latest updated Exam Dumps PT0-003 Zip | Amazing Pass Rate For PT0-003 Exam | Top PT0-003: CompTIA PenTest+ Exam □ Go to website ➥ www.pdfdumps.com □ open and search for 【 PT0-003 】 to download for free □Test PT0-003 Vce Free
- New PT0-003 Real Test □ PT0-003 Latest Practice Questions □ Valid PT0-003 Exam Notes □ Search for " PT0-003 " and obtain a free download on [www.pdfvce.com] □New PT0-003 Exam Pattern
- Pass Guaranteed Unparalleled CompTIA - PT0-003 - Exam Dumps CompTIA PenTest+ Exam Zip □ Search for ➡ PT0-003 □□□ and easily obtain a free download on □ www.troytecdumps.com □ □Exam PT0-003 Questions Answers
- Valid PT0-003 Exam Notes ↘ Valid PT0-003 Test Camp □ Exam Dumps PT0-003 Provider □ Copy URL { www.pdfvce.com } open and search for 《 PT0-003 》 to download for free □Valid PT0-003 Exam Notes
- Real and Updated CompTIA PT0-003 Exam Questions □ Download ➤ PT0-003 □ for free by simply searching on ⇛ www.examdiscuss.com ⇚ □Latest PT0-003 Exam Pdf
- Exam PT0-003 Questions □ Latest PT0-003 Exam Pdf □ New PT0-003 Exam Pattern □ Search for ➽ PT0-003 □ □ and obtain a free download on □ www.pdfvce.com □ □Latest PT0-003 Exam Pdf
- PT0-003 Valid Dumps Questions □ Exam Dumps PT0-003 Provider □ Exam PT0-003 Questions □ Search on ⇛ www.examcollectionpass.com ⇚ for 《 PT0-003 》 to obtain exam materials for free download □PT0-003 Test Objectives Pdf
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.baliacg.com, 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, www.stes.tyc.edu.tw, motionentrance.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes