PT0-003 PDF Questions | Test PT0-003 Price

BONUS!!! Download part of FreeCram PT0-003 dumps for free: https://drive.google.com/open?id=1BukaZ7vml3Ua4fsizro9kDjDgLlSHb_Q

There are no threshold limits to attend the PT0-003 test such as the age, sexuality, education background and your job conditions, and anybody who wishes to improve their volume of knowledge and actual abilities can attend the test. Our PT0-003 study materials contain a lot of useful and helpful knowledge which can help you find a good job and be promoted quickly. Our PT0-003 Study Materials are compiled by the senior experts elaborately and we update them frequently to follow the trend of the times.

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	• 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	• 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	• 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.

>> PT0-003 PDF Questions <<

Test PT0-003 Price, Vce PT0-003 File

These practice exams are solely designed to help you achieve PT0-003 certification on the first attempt. The mock exam simulator helps you get through every topic inside out and you get overall better grades. This is because you have hands-on the most updated and most reliable CompTIA PT0-003 Questions created under the supervision of 90,000 CompTIA professionals.

CompTIA PenTest+ Exam Sample Questions (Q150-Q155):

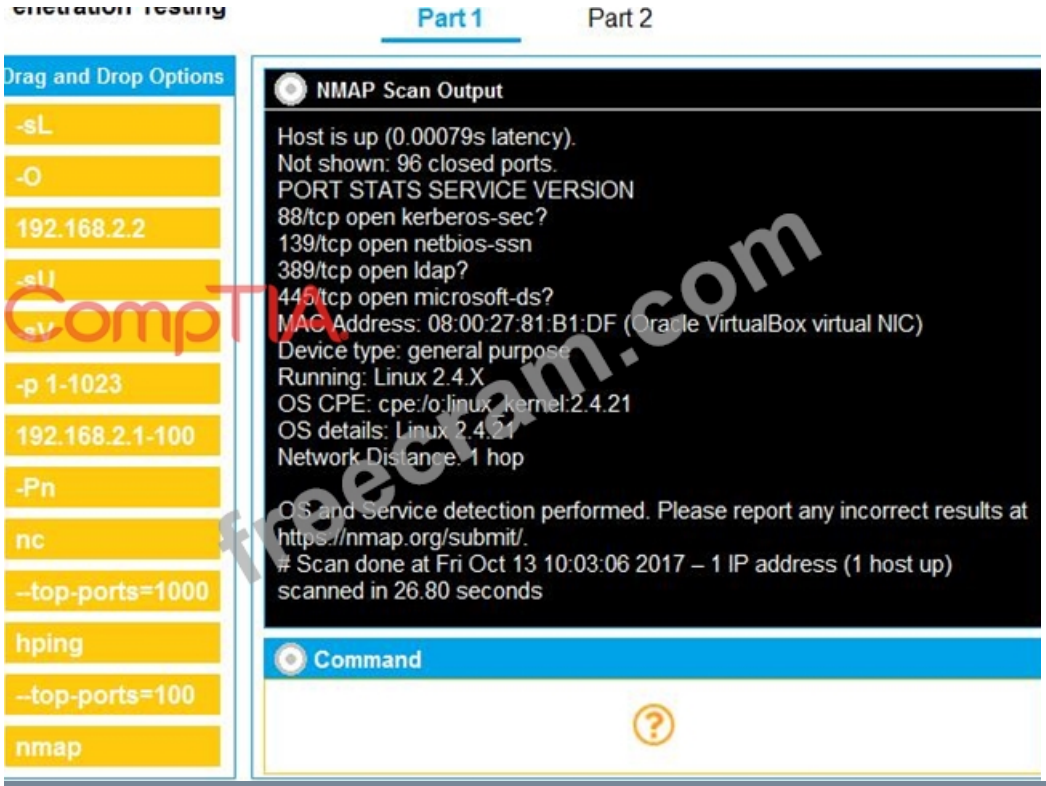
NEW QUESTION # 150
Which of the following explains the reason a tester would opt to use DREAD over PTES during the planning phase of a penetration test?

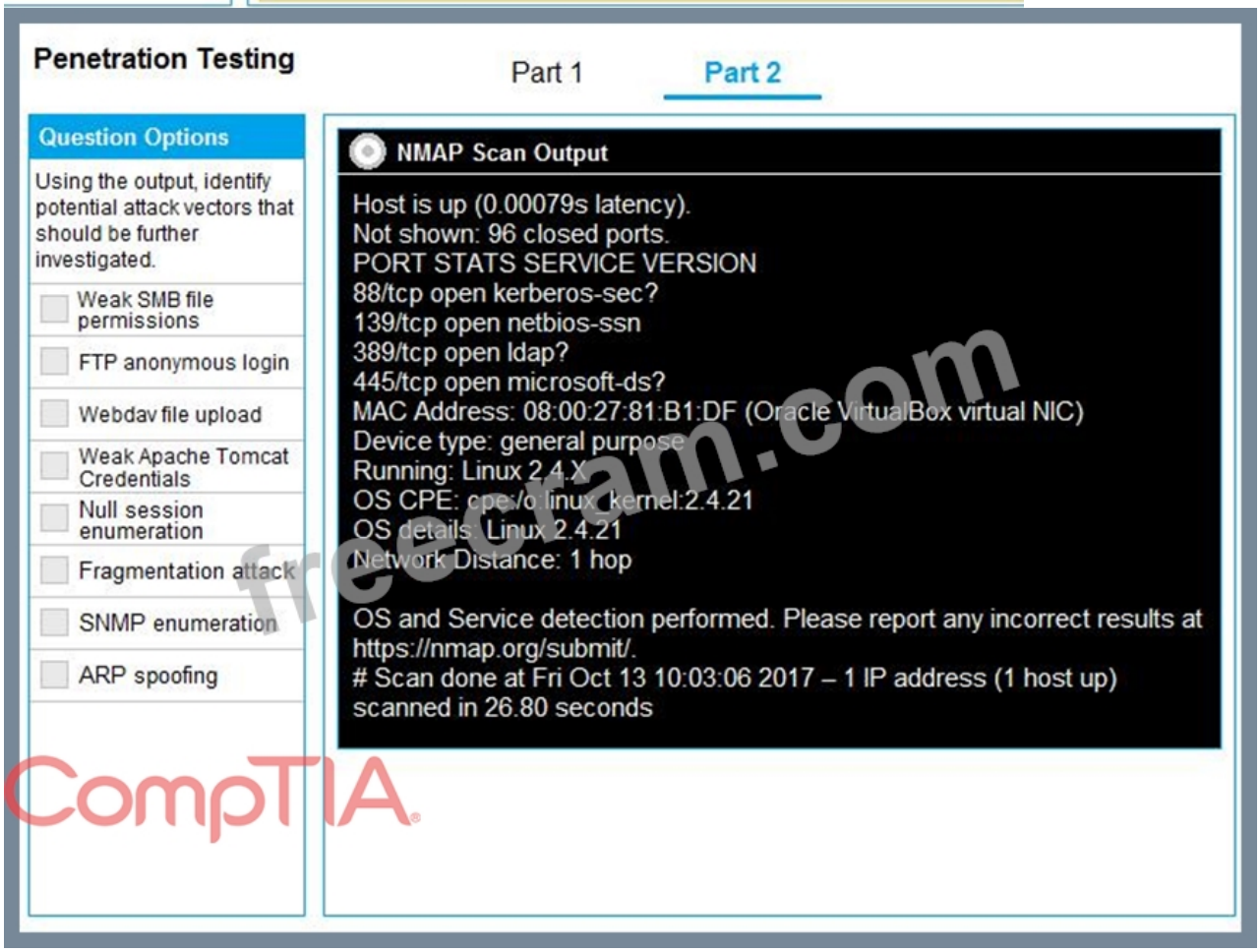
- A. The tester is evaluating a thick client application.
- B. The tester is creating a threat model.
- C. The tester is conducting a web application test.
- D. The tester is assessing a mobile application.

Answer: B

Explanation:
DREAD for Threat Modeling:
DREAD is a risk assessment framework used in threat modeling to prioritize vulnerabilities based on their impact, reproducibility, exploitability, affected users, and discoverability.
It is specifically designed for creating and analyzing threat models.
Why Not Other Options?
A, B, C: While DREAD can be applied in various contexts (web, mobile, thick client applications), its primary purpose is threat modeling, not specific testing methodologies like PTES.
CompTIA Pentest+ Reference:
Domain 1.0 (Planning and Scoping)

NEW QUESTION # 151
SIMULATION
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

Explanation:
See explanation below
Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

NEW QUESTION # 152
After detecting a web shell on a compromised server, what is the best course of action to prevent the attacker from regaining access?

- A. Remove the persistence mechanisms.
- B. Preserve artifacts.
- C. Perform secure data destruction.
- D. Spin down the infrastructure.

Answer: A

Explanation:
Web shells provide remote access and persistence for attackers. The best mitigation is to remove persistence mechanisms.
* Remove the persistence mechanisms (Option A):
* Attackers often modify startup scripts, cron jobs, or registry keys to maintain access.
* If persistence is not removed, even after the web shell is deleted, attackers can reinstall or reaccess it.

NEW QUESTION # 153
Which of the following OT protocols sends information in cleartext?

- A. PROFINET
- B. Modbus
- C. DNP3
- D. TTEthernet

Answer: B

Explanation:
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here's an analysis of each protocol regarding whether it sends information in cleartext:
* TTEthernet (Option A):
* Explanation: TTEthernet (Time-Triggered Ethernet) is designed for real-time communication and safety-critical systems.
* Security: It includes mechanisms for reliable and deterministic data transfer, not typically sending information in cleartext.
* DNP3 (Option B):
* Explanation: DNP3 (Distributed Network Protocol) is used in electric and water utilities for SCADA (Supervisory Control and Data Acquisition) systems.
* Security: While the original DNP3 protocol transmits data in cleartext, the DNP3 Secure Authentication extensions provide cryptographic security features.
* Modbus
* Explanation: Modbus is a communication protocol used in industrial environments for transmitting data between electronic devices.
* Security: Modbus transmits data in cleartext, which makes it susceptible to interception and unauthorized access.
* References: The lack of security features in Modbus, such as encryption, is well-documented and a known vulnerability in ICS environments.
* PROFINET (Option D):
* Explanation: PROFINET is a standard for industrial networking in automation.
* Security: PROFINET includes several security features, including support for encryption, which means it doesn't necessarily send information in cleartext.
Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

NEW QUESTION # 154
During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge's information to create a duplicate for unauthorized entry. Which of the following best describes this action?

- A. Smurfing
- B. Credential stuffing
- C. RFID cloning
- D. Card skimming

Answer: C

Explanation:
RFID Cloning:
RFID (Radio-Frequency Identification) cloning involves copying the data from an access badge and creating a duplicate that can be used for unauthorized entry.
Tools like Proxmark or RFID duplicators are commonly used for this purpose.
Why Not Other Options?
A (Smurfing): A network-based denial-of-service attack, unrelated to physical access.
B (Credential stuffing): Involves using stolen credentials in bulk for authentication attempts, unrelated to badge cloning.
D (Card skimming): Relates to stealing credit card information, not access badges.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)

NEW QUESTION # 155
......

It takes a lot of effort and hard work to get the results. The first step is to download real CompTIA PenTest+ Exam (PT0-003) Exam Questions of FreeCram. These CompTIA PenTest+ Exam (PT0-003) exam questions are available in PDF, desktop practice test software, and web-based practice exam. If you are already an employee or busy in your routine, you can prepare PT0-003 Exam quickly with FreeCram pdf questions. PT0-003 pdf exam questions help applicants study for the CompTIA PenTest+ Exam (PT0-003) exam at any time from any location. With the pdf questions, it will be easy for you to complete the CompTIA PenTest+ Exam (PT0-003) exam preparation in a short time.

Test PT0-003 Price: https://www.freecram.com/CompTIA-certification/PT0-003-exam-dumps.html

myportal.utt.edu.tt, esellingsupport.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, theislamicacademy.net, 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, 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

P.S. Free & New PT0-003 dumps are available on Google Drive shared by FreeCram: https://drive.google.com/open?id=1BukaZ7vml3Ua4fsizro9kDjDgLlSHb_Q