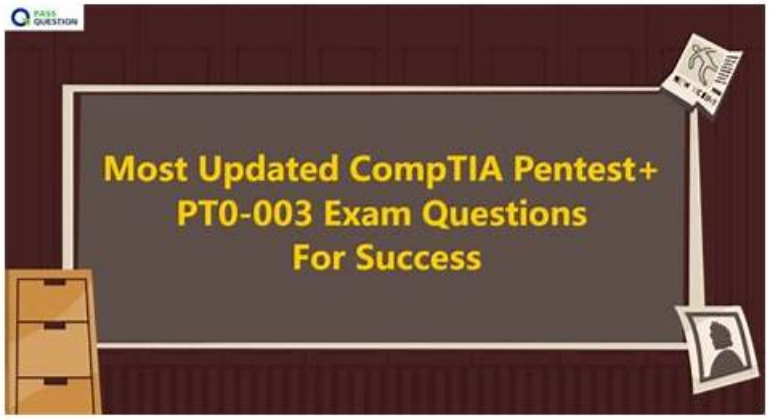
Updated CompTIA PT0-003 Exam Questions - Fast Track To Get Success



BONUS!!! Download part of PDFTorrent PT0-003 dumps for free: https://drive.google.com/open?id=1S36PMGQ64X0Esz4t_NdsB6YNg8l3gSt8

PDFTorrent provides CompTIA PT0-003 desktop-based practice software for you to test your knowledge and abilities. The PT0-003 desktop-based practice software has an easy-to-use interface. You will become accustomed to and familiar with the free demo for CompTIA PT0-003 Exam Questions. Exam self-evaluation techniques in our PT0-003 desktop-based software include randomized questions and timed tests. These tools assist you in assessing your ability and identifying areas for improvement to pass the CompTIA certification exam.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 5	• 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.

Free 1 year CompTIA PT0-003 Dumps Updates: a Full Refund Guarantee By PDFTorrent

Our website is considered to be the top test seller of PT0-003 practice materials, and gives you the best knowledge of the content of the syllabus of PT0-003 preparation materials. They provide you with the best possible learning prospects by using minimal effort to satisfy the results beyond your expectations. Despite the intricacies of the nominal concept, the questions of PT0-003 Exam Questions have been made suitable whatever level you are.

CompTIA PenTest+ Exam Sample Questions (Q214-Q219):

NEW QUESTION # 214
During host discovery, a security analyst wants to obtain GeoIP information and a comprehensive summary of exposed services. Which of the following tools is best for this task?

- A. Censys.io
- B. theHarvester
- C. WiGLE.net
- D. WHOIS

Answer: A

Explanation:
* Censys.io:
* Censys.io is a search engine for Internet-connected devices. It provides information about IP addresses, domains, GeoIP data, and exposed services.
* Why Not Other Options?
* A (WiGLE.net): Focuses on mapping Wi-Fi networks, not providing detailed information about IP addresses or services.
* B (WHOIS): Provides domain registration and ownership details but lacks GeoIP and service summaries.
* C (theHarvester): Primarily gathers OSINT like email addresses, subdomains, and names but not service information or GeoIP data.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)

NEW QUESTION # 215
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

- A. Shared responsibilities
- B. Authorization letter
- C. Testing window
- D. Terms of service

Answer: C

Explanation:
The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here's why option A is correct:
* Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.
* Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.
* Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.
* Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.
References from Pentest:
* Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

* Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.

NEW QUESTION # 216
A penetration tester conducts reconnaissance for a client's network and identifies the following system of interest:
$ nmap -A AppServer1.compita.org
Starting Nmap 7.80 (2023-01-14) on localhost (127.0.0.1) at 2023-08-04 15:32:27 Nmap scan report for AppServer1.compita.org (192.168.1.100) Host is up (0.001s latency).
Not shown: 999 closed ports
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
873/tcp open rsync
8080/tcp open http-proxy
8443/tcp open https-alt
9090/tcp open zeus-admin
10000/tcp open snet-sensor-mgmt
The tester notices numerous open ports on the system of interest. Which of the following best describes this system?

- A. An already-compromised system
- B. A Windows endpoint
- C. A Linux server
- D. A honeypot

Answer: D

Explanation:
A honeypot is a decoy system designed to attract attackers by exposing multiple services and vulnerabilities.
Indicators of a honeypot (Option A):
The system has an unusual combination of Windows (SMB, MSRPC) and Linux (Rsync, SSH) services.
It exposes a large number of open ports, which is uncommon for a production server.
Presence of "zeus-admin" (port 9090) suggests intentionally vulnerable services.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Honeypots and Decoys in Reconnaissance" Incorrect options:
Option B (Windows endpoint): Windows would not normally run Rsync (873/tcp) or SSH (22/tcp).
Option C (Linux server): Linux servers typically don't have NetBIOS (139/tcp) or MSRPC (135/tcp).
Option D (Already-compromised system): Although possible, honeypots mimic compromised systems to lure attackers.

NEW QUESTION # 217
Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

- A. Executing a process injection
- B. Installing a bind shell
- C. Creating registry keys
- D. Setting up a reverse SSH connection

Answer: C

Explanation:
Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here's an explanation of each option and why creating registry keys is the preferred method:
* Creating registry keys
* Explanation: Modifying or adding specific registry keys can ensure that malicious code or backdoors are executed every time the system starts, thus maintaining persistence.

* Advantages: This method is stealthy and can be effective in maintaining access over long periods, especially on Windows systems.
* Example: Adding a new entry to the HKLM\Software\Microsoft\Windows\CurrentVersion\Run registry key to execute a malicious script upon system boot.

NEW QUESTION # 218
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

- A. Performed a discovery scan.
- B. Rechecked the scanner configuration.
- C. Used a different scan engine.
- D. Configured all the TCP ports on the scan.

Answer: A

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:
Performing a Discovery Scan:
Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.
Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.
Comparison with Other Actions:
Rechecking the Scanner Configuration (A): Useful but not as comprehensive as ensuring all hosts are discovered.
Using a Different Scan Engine (C): Not necessary if the issue is with host discovery rather than the scanner's capability.
Configuring All TCP Ports on the Scan (D): Helps in detailed scanning but does not address missing hosts.
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.

NEW QUESTION # 219
.....

www.examcollectionpass.com] and search for ➽ PT0-003 □ to obtain a free download □Test PT0-003 Pdf

- PT0-003 Latest Guide Files □ PT0-003 Latest Guide Files □ Updated PT0-003 Test Cram ☀ Search on { www.pdfvce.com } for 「 PT0-003 」 to obtain exam materials for free download □PT0-003 Latest Guide Files
- Study PT0-003 Reference ✈ Test PT0-003 Pdf ☀ Pass PT0-003 Test Guide □ The page for free download of 「 PT0-003 」 on " www.exam4labs.com " will open immediately □PT0-003 Exam Questions Vce
- 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.posteezy.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, zenwriting.net, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PT0-003 dumps are available on Google Drive shared by PDFTorrent: https://drive.google.com/open?id=1S36PMGQ64X0Esz4t_NdsB6YNg8l3gSt8