# PT0-003 Zertifizierungsfragen, CompTIA PT0-003 PrüfungFragen


Wenn Sie ein Pendler sind, wenn Sie die CompTIA PT0-003 Prüfung so schnell wie möglich bestehen möchten, dass ist ExamFragen Ihre beste Wahl. Unser ExamFragen bietet Ihnen die Testfragen und Antworten von CompTIA PT0-003, die von den IT-Experten durch Experimente und Praxis erhalten werden und über IT-Zertifizierungserfahrungen über 10 Jahre verfügt. Mit ExamFragen können Sie nicht nur Zeit sparen, sondern auch die CompTIA PT0-003 Zertifizierungsprüfung leicht und züglich bestehen.

ExamFragen hat riesieges Expertenteam. Sie untersucht ständig nach ihren Kenntnissen und Erfahrungen die CompTIA PT0-003 (CompTIA PenTest+ Exam) IT-Zertifizierungsprüfung in den letzten Jahren. Ihre Forschungsergebnisse sind nämlich die Produkte von ExamFragen. Die Fragen und Antworten zur CompTIA PT0-003 Zertifizierungsprüfung von ExamFragen sind den realen Fragen und Antworten sehr ähnlich. Sie können vielen helfen, ihren Traum zu verwirklichen. ExamFragen verspricht, dass Sie die CompTIA PT0-003 (CompTIA PenTest+ Exam) Prüfung erfolgreich zu bestehen. Sie können beruhigt ExamFragen in Ihren Warenkorb schicken. Mit ExamFragen könen Sie Ihren Wunsch sofort erfüllen.

**>> PT0-003 Online Praxisprüfung <<**

## PT0-003 Lernhilfe, PT0-003 Kostenlos Downloden

ExamFragen ist eine erstklassige Website für die CompTIA PT0-003 Zertifzierungsprüfung. Im ExamFragen können Sie Tipps und Prüfungsmaterialien finden. Sie können auch die Examensfragen-und antworten teilweise als Probe kostenlos herunterladen. ExamFragen kann Ihnen umsonst die Updaets der Prüfungsmaterialien für die CompTIA PT0-003 Prüfung bieten. Alle unseren Zertifizierungsprüfungen enthalten Antworten. Unser Eliteteam von IT-Fachleuten wird die neuesten und richtigen Examensübungen nach ihren fachlichen Erfahrungen bearbeiten, um Ihnen bei der Prüfung zu helfen. Alles in allem, wir werden Ihnen alle einschlägigen Materialien in Bezug auf die CompTIA PT0-003 Zertifizierungsprüfung bieten.

## CompTIA PT0-003 Prüfungsplan:

| Thema | Einzelheiten |
|---|---|
| Thema 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. |
| Thema 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. |

| | |
|---|---|
| Thema 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. |
| Thema 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. |
| Thema 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. |

## CompTIA PenTest+ Exam PT0-003 Prüfungsfragen mit Lösungen (Q179-Q184):

**179. Frage**
A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

- A. Sniffing
- B. Banner grabbing
- C. Ping sweeps
- D. TCP/UDP scanning

**Antwort: A**

Begründung:
To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.
Sniffing:
Definition: Sniffing involves capturing and analyzing network traffic passing through the network.
It is a passive reconnaissance technique that does not generate detectable traffic on the network.
Tools: Tools like Wireshark and tcpdump are commonly used for sniffing. They capture packets and provide insights into network communications, protocols in use, devices, and potential vulnerabilities.
Advantages:
Stealthy: Since sniffing is passive, it does not generate additional traffic that could be detected by intrusion detection systems (IDS) or other monitoring tools.
Information Gathered: Sniffing can reveal IP addresses, MAC addresses, open ports, running services, and potentially sensitive information transmitted in plaintext.

**180. Frage**
A penetration tester is configuring a vulnerability management solution to perform credentialed scans of an Active Directory server. Which of the following account types should the tester provide to the scanner?

- A. Domain administrator
- B. Root
- C. Read-only
- D. Local user

**Antwort: A**

Begründung:
To perform credentialed scans on an Active Directory (AD) server, the scanner requires high-level access to retrieve system configuration, patch levels, and user rights. A Domain Administrator account ensures full visibility into domain resources and permissions, which is essential for a complete vulnerability assessment.

From the CompTIA PenTest+ PT0-003 Objectives - Domain 2.0: Information Gathering and Vulnerability Identification: "Credentialed scans require administrative-level access on target systems to provide detailed insights into software versions, missing patches, and security settings." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 6

**181. Frage**
Given the following Nmap scan command:
[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101

Which of the following is the total number of servers that Nmap will attempt to scan?

- A. 0
- B. 1
- C. 2
- D. 3

**Antwort: A**

Begründung:
The Nmap scan command given will scan all the hosts in the 192.168.0.0/24 subnet, except for the one with the IP address 192.168.0.101. The subnet has 256 possible hosts, but one of them is excluded, so the total number of servers that Nmap will attempt to scan is 255. References:
Nmap Commands - 17 Basic Commands for Linux Network, Section: Scan Multiple Hosts, Subsection: Excluding Hosts from Search Nmap Cheat Sheet 2023: All the Commands and More, Section: Target Specification, Subsection:
-exclude

**182. Frage**
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack.
During the engagement, the tester is able to obtain an internal foothold on the target network.
Which of the following is the next task the tester should complete to accomplish the objective?

- A. Initiate a social engineering campaign.
- B. Compromise an endpoint.
- C. Share enumeration.
- D. Perform credential dumping.

**Antwort: D**

Begründung:
Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping.
Purpose: Credential dumping involves extracting password hashes and plaintext passwords from compromised systems. These credentials can be used to gain further access to sensitive data and critical systems within the network.
Tools: Common tools used for credential dumping include Mimikatz, Windows Credential Editor, and ProcDump.
Impact: With these credentials, the tester can move laterally across the network, escalate privileges, and access confidential information.

**183. Frage**
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

- A. XSS
- B. Server-side template injection
- C. SQL injection
- D. SSRF

**Antwort: A**

Begründung:
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here's why option C is correct:
XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.
Reference from Pentest:
Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.
Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

**184. Frage**
.....