Quiz Pass-Sure PT0-003 - Relevant CompTIA PenTest+ Exam Answers


Buy here:
http://theperfecthomework.com/cmit-321-quiz-3/

Question 1 (5 points)

By default, where are the IIS logs recorded?

Question 1 options:

	Inetpub/logs
	%systemroot%\logfiles
	%systemroot%\system32\logfiles
	Inetpub\www\logs

Save

Question 2 (5 points)

Which steps should be taken to increase web server security? (Select all that apply.)

Question 2 options:

	Remove unused application mappings.
	Enable remote administration.

What's more, part of that ActualVCE PT0-003 dumps now are free: https://drive.google.com/open?id=1fzqFqb1BAFHeh2nqQB2nNqUj78ef5HZU

Originating the PT0-003 exam questions of our company from tenets of offering the most reliable backup for customers, and outstanding results have captured exam candidates' heart for their functions. Our PT0-003 practice materials can be subdivided into three versions. All those versions of usage has been well-accepted by them. They are the PDF, Software and APP online versions of our PT0-003 Study Guide.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.

Pass Guaranteed Quiz 2026 CompTIA High-quality PT0-003: Relevant CompTIA PenTest+ Exam Answers

In order to gain more competitive advantages when you are going for a job interview, more and more people have been longing to get a PT0-003 certification. They think the certification is the embodiment of their ability; they are already convinced that getting a PT0-003 certification can help them look for a better job. There is no doubt that it is very difficult for most people to pass the exam and have the certification easily. If you are also weighted with the trouble about a PT0-003 Certification, we are willing to soothe your trouble and comfort you.

CompTIA PenTest+ Exam Sample Questions (Q154-Q159):

NEW QUESTION # 154
A penetration tester cannot complete a full vulnerability scan because the client's WAF is blocking communications. During which of the following activities should the penetration tester discuss this issue with the client?

- A. Client acceptance
- B. Stakeholder alignment
- C. Peer review
- D. Goal reprioritization

Answer: B

Explanation:
Stakeholder Alignment:
During stakeholder alignment, the penetration tester and client discuss challenges, constraints, and objectives.
Addressing WAF interference ensures the scope and goals are adjusted or mitigated to accommodate the issue.
Why Not Other Options?
A: Goal reprioritization focuses on internal team adjustments, not client collaboration.
B: Peer review evaluates findings and methodologies but doesn't involve clients.
C: Client acceptance occurs post-assessment, not during active engagement.
CompTIA Pentest+ Reference:
Domain 1.0 (Planning and Scoping)

NEW QUESTION # 155
A client warns the assessment team that an ICS application is maintained by the manufacturer. Any tampering of the host could void the enterprise support terms of use.
Which of the following techniques would be most effective to validate whether the application encrypts communications in transit?

- A. Utilizing port mirroring on a firewall appliance

- B. Reconfiguring the application to use a proxy
- C. Installing packet capture software on the server
- D. Requesting that certificate pinning be disabled

Answer: A

Explanation:
Since direct interaction with the ICS application is restricted, the best way to analyze network traffic without modifying the system is to use port mirroring on a firewall or network switch.
* Option A (Port mirroring) #:
* Correct. Port mirroring (SPAN) copies network traffic without modifying the host system.
* Allows passive analysis of whether encryption is used.
* Option B (Packet capture on the server) #:
* Requires modifying the host, which is prohibited by the client.
* Option C (Reconfiguring the app to use a proxy) #:
* Modifies application settings, which violates the client's terms.
* Option D (Disabling certificate pinning) #:
* Requires changes to security settings, which is not allowed in this scenario.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Passive Traffic Analysis for ICS Systems

NEW QUESTION # 156
A penetration tester must identify vulnerabilities within an ICS that is not connected to the internet or enterprise network. Which of the following should the tester utilize to conduct the testing?

- A. Manual assessment
- B. Stealth scans
- C. Source code analysis
- D. Channel scanning

Answer: A

Explanation:
In an Isolated Industrial Control System (ICS) environment that is not connected to external networks, the safest and most effective approach is a manual assessment. This involves carefully reviewing configurations, firmware versions, and system behavior without using automated or intrusive tools that might disrupt fragile ICS components.

NEW QUESTION # 157
A Chief Information Security Officer wants to automate adversarial activities from penetration tests that are relevant to the organization. Which of the following should a penetration tester do first to accomplish this task?

- A. Use Python 3 with added testing libraries and script the relevant action to test.
- B. Utilize the PowerShell PowerView tool with custom scripting additions based on test results.
- C. Deploy a command-and-control server with custom profiles to facilitate execution.
- D. Implement Atomic Red Team to chain critical TTPs and perform the test.

Answer: D

Explanation:
Atomic Red Team is the best first step because it is specifically designed to automate and emulate adversary techniques in a structured, repeatable, and organization-relevant way. It maps tests to known ATT & CK techniques and allows security teams to validate detections, logging, and defensive controls using small, controlled units of adversary behavior called "atomics." Since the goal is to automate adversarial activities from prior penetration tests that matter to the organization, using a framework built for repeatable TTP emulation is more appropriate than immediately deploying a command-and-control server or writing custom scripts from scratch. PowerView is useful for specific PowerShell-based enumeration and post-exploitation tasks, but it is not the best starting point for broad, reusable adversary emulation. Therefore, implementing Atomic Red Team is the most suitable first action.

NEW QUESTION # 158
A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the

network with the appropriate tools. Which of the following should the consultant engage first?

- A. OS fingerprinting
- B. Host discovery
- C. Service discovery
- D. DNS enumeration

Answer: B

Explanation:
In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:
Host Discovery (answer: C):
Objective: Identify live hosts on the network.
Tools & Techniques:
Ping Sweep: Using tools like nmap with the -sn option (ping scan) to check for live hosts by sending ICMP Echo requests.
ARP Scan: Useful in local networks, arp-scan can help identify all devices on the local subnet by broadcasting ARP requests.
nmap -sn 192.168.1.0/24
* Reference:
The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.
The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.
* Service Discovery (Option A):
Objective: After identifying live hosts, determine the services running on them.
Tools & Techniques:
Nmap: Often used with options like -sV for version detection to identify services.
nmap -sV 192.168.1.100
* Reference:
As seen in multiple write-ups (e.g., Anubis HTB and Bolt HTB), service discovery follows host identification to understand the services available for potential exploitation.
* OS Fingerprinting (Option B):
Objective: Determine the operating system of the identified hosts.
Tools & Techniques:
Nmap: With the -O option for OS detection.
nmap -O 192.168.1.100
* Reference:
Accurate OS fingerprinting helps tailor subsequent attacks and is often performed after host and service discovery, as highlighted in the write-ups.
* DNS Enumeration (Option D):
Objective: Identify DNS records and gather subdomains related to the target domain.
Tools & Techniques:
dnsenum, dnsrecon, and dig.
dnsenum example.com
Reference:
DNS enumeration is crucial for identifying additional attack surfaces, such as subdomains and related services. This step is typically part of the reconnaissance phase but follows host discovery and sometimes service identification.
Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration. This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

NEW QUESTION # 159
.....

- Quiz CompTIA - PT0-003 - CompTIA PenTest+ Exam –Professional Relevant Answers □ Easily obtain free download of ▸ PT0-003 ◂ by searching on （ www.troytecdumps.com ） □PT0-003 Training Courses
- Exam PT0-003 Demo □ PT0-003 Hottest Certification □ PT0-003 Exam Quick Prep □ Search for ➤ PT0-003 □ and download it for free on 「 www.pdfvce.com 」 website □Exam Sample PT0-003 Questions
- 2026 Professional PT0-003 – 100% Free Relevant Answers | CompTIA PenTest+ Exam Reliable Exam Pattern □ Search for ➠ PT0-003 □ and obtain a free download on { www.practicevce.com } □PT0-003 Reliable Exam Prep
- PT0-003 Brain Dumps □ PT0-003 Reliable Test Labs □ New PT0-003 Mock Test □ Enter ✔ www.pdfvce.com □✔□ and search for □ PT0-003 □ to download for free □PT0-003 Exam Guide Materials
- PT0-003 Hottest Certification □ Latest PT0-003 Demo □ PT0-003 Test Guide □ Search for " PT0-003 " and download it for free on ✔ www.examdiscuss.com □✔□ website □PT0-003 Training Courses
- Confirm Your Success With Free CompTIA PT0-003 Exam Questions Updates - Demo □ Simply search for ☀ PT0-003 □☀□ for free download on ▸ www.pdfvce.com ◂ □PT0-003 Free Dumps
- Excellect PT0-003 Pass Rate □ PT0-003 Brain Dumps □ PT0-003 Hottest Certification ✔□ Easily obtain ⇛ PT0-003 ⇚ for free download through □ www.vceengine.com □ □PT0-003 Free Dumps
- 2026 Professional PT0-003 – 100% Free Relevant Answers | CompTIA PenTest+ Exam Reliable Exam Pattern □ Open 「 www.pdfvce.com 」 enter ☀ PT0-003 □☀□ and obtain a free download □PT0-003 Training Courses
- Quiz 2026 CompTIA Pass-Sure PT0-003: Relevant CompTIA PenTest+ Exam Answers □ Download （ PT0-003 ） for free by simply entering ➠ www.prep4away.com □ website □PT0-003 Reliable Exam Prep
- PT0-003 Exam Quick Prep □ Download PT0-003 Fee □ Exam Sample PT0-003 Questions □ Open ☀ www.pdfvce.com □☀□ enter ➡ PT0-003 □□□ and obtain a free download □PT0-003 Exam Quick Prep
- 2026 Relevant PT0-003 Answers | Professional PT0-003 Reliable Exam Pattern: CompTIA PenTest+ Exam □ Simply search for ▸ PT0-003 ◂ for free download on ☀ www.practicevce.com □☀□ □PT0-003 Exam Quick Prep
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 CompTIA PT0-003 dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=1fzqFqb1BAFHeh2nqQB2nNqUj78ef5HZU