EDUSUM

#1 Online Certification Guide

COMPTIA PT0-003

CompTIA PenTest+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

PT0-003

CompTIA PenTest+

90 Questions Exam – 750 / 900 Cut Score – Duration of 165 minutes

Table of Contents:

Know Your PT0-003 Certification Well:

The PT0-003 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your PT0-003 preparation you may struggle to get all the crucial PenTest+ materials like PT0-003 syllabus, sample questions, study guide.

But don't worry the PT0-003 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the PT0-003 syllabus?
- How many questions are there in the PT0-003 exam?
- Which Practice test would help me to pass the PT0-003 exam at the first attempt?

Passing the PT0-003 exam makes you CompTIA PenTest+. Having the PenTest+ certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA PT0-003 PenTest+ Certification Details:

Exam Name	CompTIA PenTest+
Exam Code	PT0-003
Exam Price	$404 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	Pearson VUE
Sample Questions	CompTIA PenTest+ Sample Questions
Practice Exam	**CompTIA PT0-003 Certification Practice Exam**

PT0-003 Syllabus:

Topic	Details
Engagement Management - 13%	
Summarize pre-engagement activities.	- Scope definition • Regulations, frameworks, and standards - Privacy - Security • Rules of engagement - Exclusions - Test cases - Escalation process - Testing window • Agreement types - Non-disclosure agreement (NDA) - Master service agreement (MSA) - Statement of work (SoW) - Terms of service (ToS) • Target selection - Classless Inter-Domain Routing(CIDR) ranges - Domains - Internet Protocol (IP) addresses - Uniform Resource Locator (URL) • Assessment types - Web - Network - Mobile - Cloud - Application programming interface(API) - Application - Wireless - Shared responsibility model • Hosting provider responsibilities • Customer responsibilities • Penetration tester responsibilities • Third-party responsibilities - Legal and ethical considerations • Authorization letters • Mandatory reporting requirements • Risk to the penetration tester

Topic	Details
Explain collaboration and communication activities.	- Peer review - Stakeholder alignment - Root cause analysis - Escalation path - Secure distribution - Articulation of risk, severity, and impact - Goal reprioritization - Business impact analysis - Client acceptance
Compare and contrast testing frameworks and methodologies.	- Open Source Security Testing Methodology Manual (OSSTMM) - Council of Registered Ethical Security Testers (CREST) - Penetration Testing Execution Standard(PTES) - MITRE ATT&CK - Open Worldwide Application Security Project (OWASP) Top 10 - OWASP Mobile Application Security Verification Standard (MASVS) - Purdue model - Threat modeling frameworks • Damage potential, Reproducibility, Exploitability, Affected users, Discoverability (DREAD) • Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) • Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
Explain the components of a penetration test report.	- Format alignment - Documentation specifications - Risk scoring - Definitions - Report components • Executive summary • Methodology • Detailed findings • Attack narrative • Recommendations - Remediation guidance - Test limitations and assumptions - Reporting considerations

Topic	Details
	• Legal • Ethical • Quality control (QC) • Artificial intelligence (AI)
Given a scenario, analyze the findings and recommend the appropriate remediation within a report.	- Technical controls • System hardening • Sanitize user input/parameterize queries • Multifactor authentication • Encryption • Process-level remediation • Patch management • Key rotation • Certificate management • Secrets management solution • Network segmentation • Infrastructure security controls - Administrative controls • Role-based access control • Secure software development life cycle • Minimum password requirements • Policies and procedures - Operational controls • Job rotation • Time-of-day restrictions • Mandatory vacations • User training - Physical controls • Access control vestibule • Biometric controls • Video surveillance
Reconnaissance and Enumeration - 21%	
Given a scenario, apply information gathering techniques.	- Active and passive reconnaissance - Open-source intelligence (OSINT) • Social media • Job boards • Scan code repositories • Domain Name System (DNS) - DNS lookups - Reverse DNS lookups • Cached pages • Cryptographic flaws

Topic	Details
	• Password dumps - Network reconnaissance - Protocol scanning • Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP) scanning - Certificate transparency logs - Information disclosure - Search engine analysis/ enumeration - Network sniffing • Internet of Things (IoT) and operational technology (OT) protocols - Banner grabbing - Hypertext Markup Language (HTML) scraping
Given a scenario, apply enumeration techniques.	- Operating system (OS) fingerprinting - Service discovery - Protocol enumeration - DNS enumeration - Directory enumeration - Host discovery - Share enumeration - Local user enumeration - Email account enumeration - Wireless enumeration - Permission enumeration - Secrets enumeration • Cloud access keys • Passwords • API keys • Session tokens - Attack path mapping - Web application firewall (WAF) enumeration • Origin address - Web crawling - Manual enumeration • Robots.txt • Sitemap • Platform plugins
Given a scenario, modify scripts for reconnaissance and enumeration.	- Information gathering - Data manipulation - Scripting languages • Bash

Topic	Details
	• Python • PowerShell - Logic constructs • Loops • Conditionals • Boolean operator • String operator • Arithmetic operator - Use of libraries, functions,and classes
Given a scenario, use the appropriate tools for reconnaissance and enumeration.	- Wayback Machine - Maltego - Recon-ng - Shodan - SpiderFoot - WHOIS - nslookup/dig - Censys.io - Hunter.io - DNSdumpster - Amass - Nmap • Nmap Scripting Engine (NSE) - theHarvester - WiGLE.net - InSSIDer - OSINTframework.com - Wireshark/tcpdump - Aircrack-ng
Vulnerability Discovery and Analysis - 17%	
Given a scenario, conduct vulnerability discovery using various techniques.	- Types of scans • Container scans - Sidecar scans • Application scans - Dynamic application security testing (DAST) - Interactive application security testing (IAST) - Software composition analysis (SCA) - Static application security testing (SAST) 1. Infrastructure as Code (IaC) 2. Source code analysis - Mobile scan

Topic	Details
	• Network scans - TCP/UDP scan - Stealth scans • Host-based scans • Authenticated vs. unauthenticated scans • Secrets scanning • Wireless - Service set identifier (SSID) scanning - Channel scanning - Signal strength scanning - Industrial control systems (ICS) vulnerability assessment • Manual assessment • Port mirroring - Tools • Nikto • Greenbone/Open Vulnerability Assessment Scanner (OpenVAS) • TruffleHog • BloodHound • Tenable Nessus • PowerSploit • Grype • Trivy • Kube-hunter
Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.	- Validate scan, reconnaissance, and enumeration results • False positives • False negatives • True positives • Scan completeness • Troubleshooting scan configurations - Public exploit selection - Use scripting to validate results
Explain physical security concepts.	- Tailgating - Site surveys - Universal Serial Bus (USB) drops - Badge cloning - Lock picking
Attacks and Exploits - 35%	

Topic	Details
Given a scenario, analyze output to prioritize and prepare attacks.	- Target prioritization • High-value asset identification • Descriptors and metrics - Common Vulnerability Scoring System (CVSS) base score - Common Vulnerabilities and Exposures (CVE) - Common Weakness Enumeration (CWE) - Exploit Prediction Scoring System (EPSS) • End-of-life software/systems • Default configurations • Running services • Vulnerable encryption methods • Defensive capabilities - Capability selection • Tool selection • Exploit selection and customization - Code analysis • Documentation - Attack path - Low-level diagram creation - Storyboard • Dependencies • Consideration of scope limitations Labeling sensitive systems
Given a scenario, perform network attacks using the appropriate tools.	- Attack types • Default credentials • On-path attack • Certificate services • Misconfigured services exploitation • Virtual local area network (VLAN) hopping • Multihomed hosts • Relay attack • Share enumeration • Packet crafting - Tools • Metasploit • Netcat • Nmap - NSE • Impacket • CrackMapExec (CME)

Topic	Details
	• Wireshark/tcpdump • msfvenom • Responder • Hydra
Given a scenario, perform authentication attacks using the appropriate tools.	- Attack types • Multifactor authentication (MFA) fatigue • Pass-the-hash attacks • Pass-the-ticket attacks • Pass-the-token attacks • Kerberos attacks • Lightweight Directory Access Protocol (LDAP) injection • Dictionary attacks • Brute-force attacks • Mask attacks • Password spraying • Credential stuffing • OpenID Connect (OIDC) attacks • Security Assertion Markup Language (SAML) attacks - Tools • CME • Responder • hashcat • John the Ripper • Hydra • BloodHound • Medusa • Burp Suite
Given a scenario, perform host-based attacks using the appropriate tools.	- Attack types • Privilege escalation • Credential dumping • Circumventing security tools • Misconfigured endpoints • Payload obfuscation • User-controlled access bypass • Shell escape • Kiosk escape • Library injection • Process hollowing and injection • Log tampering

Topic	Details
	• Unquoted service path injection - Tools • Mimikatz • Rubeus • Certify • Seatbelt • PowerShell/PowerShell Integrated Scripting Environment (ISE) • PsExecEvil-WinRM • Living off the land binaries (LOLbins)
Given a scenario, perform web application attacks using the appropriate tools.	- Attack types • Brute-force attack • Collision attack • Directory traversal • Server-side request forgery (SSRF) • Cross-site request forgery (CSRF) • Deserialization attack • Injection attacks - Structured Query Language (SQL) injection - Command injection - Cross-site scripting (XSS) - Server-side template injection • Insecure direct object reference • Session hijacking • Arbitrary code execution • File inclusions - Remote file inclusion (RFI) - Local file inclusion (LFI) - Web shell • API abuse • JSON Web Token (JWT) manipulation - Tools • TruffleHog • Burp Suite • Zed Attack Proxy (ZAP) • Postman • sqlmap • Gobuster/DirBuster • Wfuzz • WPScan

Topic	Details
Given a scenario, perform cloud-based attacks using the appropriate tools.	- Attack types • Metadata service attacks • Identity and access management misconfigurations • Third-party integrations • Resource misconfiguration - Network segmentation - Network controls - Identity and access management (IAM) credentials - Exposed storage buckets - Public access to services • Logging information exposure • Image and artifact tampering • Supply chain attacks • Workload runtime attacks • Container escape • Trust relationship abuse - Tools • Pacu • Docker Bench • Kube-hunter • Prowler • ScoutSuite • Cloud-native vendor tools
Given a scenario, perform wireless attacks using the appropriate tools.	- Attacks • Wardriving • Evil twin attack • Signal jamming • Protocol fuzzing • Packet crafting • Deauthentication • Captive portal • Wi-Fi Protected Setup (WPS) personal identification number (PIN) attack - Tools • WPAD • WiFi-Pumpkin • Aircrack-ng • WiGLE.net • InSSIDer

Topic	Details
	• Kismet
Given a scenario, perform social engineering attacks using the appropriate tools.	- Attack types • Phishing • Vishing • Whaling • Spearphishing • Smishing • Dumpster diving • Surveillance • Shoulder surfing • Tailgating • Eavesdropping • Watering hole • Impersonation • Credential harvesting - Tools • Social Engineering Toolkit (SET) • Gophish • Evilginx • theHarvester • Maltego • Recon-ng • Browser Exploitation Framework (BeEF)
Explain common attacks against specialized systems.	- Attack types • Mobile attacks - Information disclosure - Jailbreak/rooting - Permission abuse • AI attacks - Prompt injection - Model manipulation • OT - Register manipulation - CAN bus attack - Modbus attack - Plaintext attack - Replay attack • Near-field communication (NFC) • Bluejacking • Radio-frequency identification (RFID) • Bluetooth spamming

Topic	Details
	- Tools • Scapy • tcprelay • Wireshark/tcpdump • MobSF • Frida • Drozer • Android Debug Bridge (ADB) • Bluestrike
Given a scenario, use scripting to automate attacks.	- PowerShell • PowerSploit • PowerView • PowerUpSQL • AD search - Bash • Input/output management • Data manipulation - Python • Impacket • Scapy - Breach and attack simulation (BAS) • Caldera • Infection Monkey • Atomic Red Team
Post-exploitation and Lateral Movement - 14%	
Given a scenario, perform tasks to establish and maintain persistence.	- Scheduled tasks/cron jobs - Service creation - Reverse shell - Bind shell - Add new accounts - Obtain valid account credentials - Registry keys - Command and control (C2) frameworks - Backdoor • Web shell • Trojan - Rootkit - Browser extensions - Tampering security controls

Topic	Details
Given a scenario, perform tasks to move laterally throughout the environment.	- Pivoting - Relay creation - Enumeration • Service discovery • Network traffic discovery • Additional credential capture • Credential dumping • String searches - Service discovery • Server Message Block (SMB)/ fileshares • Remote Desktop Protocol (RDP)/ Virtual Network Computing (VNC) • Secure Shell (SSH) • Cleartext • LDAP • Remote Procedure Call (RPC) • File Transfer Protocol (FTP) • Telnet • Hypertext Transfer Protocol (HTTP)/ Hypertext Transfer Protocol Secure (HTTPS) - Web interfaces • Line Printer Daemon (LPD) • JetDirect • RPC/Distributed Component Object Model (DCOM) • Process IDs - Window Management Instrumentation(WMI) - Window Remote Management (WinRM) - Tools • LOLBins - Netstat - Net commands - cmd.exe - explorer.exe - ftp.exe - mmc.exe - rundll32 - msbuild - route - strings/findstr.exe • Covenant

Topic	Details
	• CrackMapExec • Impacket • Netcat • sshuttle • Proxychains • PowerShell ISE • Batch files • Metasploit • PsExec • Mimikatz
Summarize concepts related to staging and exfiltration.	- File encryption and compression - Covert channe • Steganography • DNS • Internet Control Message Protocol (ICMP) • HTTPS - Email - Cross-account resources - Cloud storage - Alternate data streams - Text storage sites - Virtual drive mounting
Explain cleanup and restoration activities.	- Remove persistence mechanisms - Revert configuration changes - Remove tester-created credentials - Remove tools - Spin down infrastructure - Preserve artifacts - Secure data destruction

CompTIA PT0-003 Sample Questions:

Question: 1

You identify a server hosting sensitive financial data. Which factor makes this server a high-priority target?

a) End-of-life software/systems
b) High-value asset identification
c) Exploit Prediction Scoring System (EPSS)
d) Default configurations

Answer: b

Question: 2

During cleanup, you restore altered firewall rules and system settings to their original state. Which activity does this describe?

a) Remove persistence mechanisms
b) Revert configuration changes
c) Spin down infrastructure
d) Preserve artifacts

Answer: b

Question: 3

While simulating an attack, you write a Bash script to parse log files for failed login attempts and automate brute-force attacks. Which scripting functionality are you utilizing?

a) Breach and attack simulation (BAS)
b) Data manipulation
c) Input/output management
d) PowerShell enumeration

Answer: c

Question: 4

Which prioritization metric evaluates the technical characteristics and impact of a vulnerability?

a) Common Vulnerabilities and Exposures (CVE)
b) Exploit Prediction Scoring System (EPSS)
c) Common Weakness Enumeration (CWE)
d) Common Vulnerability Scoring System (CVSS) base score

Answer: d

Question: 5

A penetration tester discovers a system with weak default configurations. Which of the following best describes why this is a significant target?

a) Such systems are often easier to exploit due to predictable settings.
b) These systems are automatically high-value assets.
c) They always use outdated software.
d) They are typically immune to privilege escalation attacks.

Answer: a

Question: 6

You have identified a vulnerability in a system and want to confirm its validity. Which method could you use to validate the results using an exploit?

a) False negative analysis
b) Public exploit selection
c) Troubleshooting scan configurations
d) Scan completeness

Answer: b

Question: 7

After concluding a penetration test, you securely wipe all sensitive test data and logs to prevent recovery. What activity are you performing?

a) Secure data destruction
b) Remove tools
c) Remove tester-created credentials
d) Revert configuration changes

Answer: a

Question: 8

Which tool is best suited for mapping attack paths and enumerating privileges within an Active Directory environment?

a) Grype
b) Tenable Nessus
c) Nikto
d) BloodHound

Answer: d

Question: 9

During a wireless network vulnerability assessment, you need to measure the power levels of access points to determine their coverage and signal range. Which scanning method is most appropriate?

a) Service set identifier (SSID) scanning
b) Channel scanning
c) Signal strength scanning
d) Stealth scans

Answer: c

Question: 10

A pentester assigned to a bank must ensure that sensitive information is kept confidential throughout the engagement; which contractual document enforces this requirement?

a) Non-disclosure Agreement (NDA)
b) Master Service Agreement (MSA)
c) Statement of Work (SoW)
d) Service Level Agreement (SLA**)**

Answer: a

Study Guide to Crack CompTIA PenTest+ PT0-003 Exam:

- Getting details of the PT0-003 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the PT0-003 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for PT0-003 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the PT0-003 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on PT0-003 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for PT0-003 Certification

Make EduSum.com your best friend during your CompTIA PenTest+ exam preparation. We provide authentic practice tests for the PT0-003 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual PT0-003 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the PT0-003 exam.

Start Online practice of PT0-003 Exam by visiting URL
https://www.edusum.com/comptia/pt0-003-comptia-pentest