EDUSUM

#1 Online Certification Guide

Excel at PT0-002 PenTest+ Exam: Proven Study Methods for Triumph

CompTIA PenTest+ CERTIFICATION QUESTIONS & ANSWERS

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

Table of Contents

Getting Ready for the PT0-002 Exam:

Use proven study tips and techniques to prepare for the PT0-002 exam confidently. Boost your readiness, improve your understanding regarding the Cybersecurity, and increase your chances of success in the CompTIA CompTIA PenTest+ with our comprehensive guide. Start your journey towards exam excellence today.

CompTIA PenTest+ Certification Details:

Exam Name	CompTIA PenTest+
Exam Code	PT0-002
Exam Price	$404 (USD)
Duration	165 mins
Number of Questions	85
Passing Score	750 / 900
Books / Training	CompTIA PenTest+ Certification Training CertMaster Learn for PenTest+
Schedule Exam	Pearson VUE
Sample Questions	CompTIA PenTest+ Sample Questions
Practice Exam	CompTIA PT0-002 Certification Practice Exam

Explore PT0-002 Syllabus:

Topic	Details
	Planning and Scoping - 14%
Compare and contrast governance, risk, and compliance concepts.	- Regulatory compliance considerations • Payment Card Industry Data Security Standard (PCI DSS) • General Data Protection Regulation (GDPR) - Location restrictions • Country limitations • Tool restrictions • Local laws • Local government requirements - Privacy requirements - Legal concepts

Topic	Details
	• Service-level agreement (SLA) • Confidentiality • Statement of work • Non-disclosure agreement (NDA) • Master service agreement - Permission to attack
Explain the importance of scoping and organizational/customer requirements.	- Standards and methodologies • MITRE ATT&CK • Open Web Application Security Project (OWASP) • National Institute of Standards and Technology (NIST) • Open-source Security Testing Methodology Manual (OSSTMM) • Penetration Testing Execution Standard (PTES) • Information Systems Security Assessment Framework (ISSAF) - Rules of engagement • Time of day • Types of allowed/disallowed tests • Other restrictions - Environmental considerations • Network • Application • Cloud - Target list/in-scope assets • Wireless networks • Internet Protocol (IP) ranges • Domains • Application programming interfaces (APIs) • Physical locations • Domain name system (DNS) • External vs. internal targets • First-party vs. third-party hosted

Topic	Details
	- Validate scope of engagement • Question the client/review contracts • Time management • Strategy - Unknown-environment vs. known-environment testing
Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.	- Background checks of penetration testing team - Adhere to specific scope of engagement - Identify criminal activity - Immediately report breaches/criminal activity - Limit the use of tools to a particular engagement - Limit invasiveness based on scope - Maintain confidentiality of data/information - Risks to the professional • Fees/fines • Criminal charges
Information Gathering and Vulnerability Scanning - 22%	
Given a scenario, perform passive reconnaissance.	- DNS lookups - Identify technical contacts - Administrator contacts - Cloud vs. self-hosted - Social media scraping • Key contacts/job responsibilities • Job listing/technology stack - Cryptographic flaws • Secure Sockets Layer (SSL) certificates • Revocation - Company reputation/security posture - Data • Password dumps • File metadata • Strategic search engine analysis/enumeration • Website archive/caching • Public source-code repositories - Open-source intelligence (OSINT)

Topic	Details
	• Tools - Shodan - Recon-ng • Sources - Common weakness enumeration (CWE) - Common vulnerabilities and exposures (CVE)
Given a scenario, perform active reconnaissance.	- Enumeration • Hosts • Services • Domains • Users • Uniform resource locators (URLs) - Website reconnaissance • Crawling websites • Scraping websites • Manual inspection of web links - robots.txt - Packet crafting • Scapy - Defense detection • Load balancer detection • Web application firewall (WAF) detection • Antivirus • Firewall - Tokens • Scoping • Issuing • Revocation - Wardriving - Network traffic • Capture API requests and responses • Sniffing - Cloud asset discovery

Topic	Details
	- Third-party hosted services - Detection avoidance
Given a scenario, analyze the results of a reconnaissance exercise.	- Fingerprinting • Operating systems (OSs) • Networks • Network devices • Software - Analyze output from: • DNS lookups • Crawling websites • Network traffic • Address Resolution Protocol (ARP) traffic • Nmap scans • Web logs
Given a scenario, perform vulnerability scanning.	- Considerations of vulnerability scanning • Time to run scans • Protocols • Network topology • Bandwidth limitations • Query throttling • Fragile systems • Non-traditional assets - Scan identified targets for vulnerabilities - Set scan settings to avoid detection - Scanning methods • Stealth scan • Transmission Control Protocol (TCP) connect scan • Credentialed vs. non-credentialed - Nmap • Nmap Scripting Engine (NSE) scripts • Common options - A - sV

Topic	Details
	- sT - Pn - O - sU - sS - T 1-5 - script=vuln - p - Vulnerability testing tools that facilitate automation
Attacks and Exploits - 30%	
Given a scenario, research attack vectors and perform network attacks.	- Stress testing for availability - Exploit resources • Exploit database (DB) • Packet storm - Attacks • ARP poisoning • Exploit chaining • Password attacks - Password spraying - Hash cracking - Brute force - Dictionary • On-path (previously known as man-in-the-middle) • Kerberoasting • DNS cache poisoning • Virtual local area network (VLAN) hopping • Network access control (NAC) bypass • Media access control (MAC) spoofing • Link-Local Multicast Name Resolution (LLMNR)/NetBIOS Name Service (NBT-NS) poisoning • New Technology LAN Manager (NTLM) relay attacks - Tools • Metasploit

Topic	Details
	• Netcat • Nmap
Given a scenario, research attack vectors and perform wireless attacks.	- Attack methods • Eavesdropping • Data modification • Data corruption • Relay attacks • Spoofing • Deauthentication • Jamming • Capture handshakes • On-path - Attacks • Evil twin • Captive portal • Bluejacking • Bluesnarfing • Radio-frequency identification (RFID) cloning • Bluetooth Low Energy (BLE) attack • Amplification attacks [Near-field communication (NFC)] • WiFi protected setup (WPS) PIN attack - Tools • Aircrack-ng suite • Amplified antenna
Given a scenario, research attack vectors and perform application-based attacks.	- OWASP Top 10 - Server-side request forgery - Business logic flaws - Injection attacks • Structured Query Language (SQL) injection - Blind SQL - Boolean SQL - Stacked queries • Command injection • Cross-site scripting

Topic	Details
	- Persistent - Reflected • Lightweight Directory Access Protocol (LDAP) injection - Application vulnerabilities • Race conditions • Lack of error handling • Lack of code signing • Insecure data transmission • Session attacks - Session hijacking - Cross-site request forgery (CSRF) - Privilege escalation - Session replay - Session fixation - API attacks • Restful • Extensible Markup Language-Remote Procedure Call (XML-RPC) • Soap - Directory traversal - Tools • Web proxies - OWASP Zed Attack Proxy (ZAP) - Burp Suite community edition • SQLmap • DirBuster - Resources • Word lists
Given a scenario, research attack vectors and perform attacks on cloud technologies.	- Attacks • Credential harvesting • Privilege escalation • Account takeover • Metadata service attack • Misconfigured cloud assets

Topic	Details
	- Identity and accessmanagement (IAM) - Federation misconfigurations - Object storage - Containerization technologies • Resource exhaustion • Cloud malware injection attacks • Denial-of-service attacks • Side-channel attacks • Direct-to-origin attacks - Tools • Software development kit (SDK)
Explain common attacks and vulnerabilities against specialized systems.	- Mobile • Attacks - Reverse engineering - Sandbox analysis - Spamming • Vulnerabilities - Insecure storage - Passcode vulnerabilities - Certificate pinning - Using known vulnerable components (i) Dependency vulnerabilities (ii) Patching fragmentation - Execution of activities using root - Over-reach of permissions - Biometrics integrations - Business logic vulnerabilities • Tools - Burp Suite - Drozer - Mobile Security Framework (MobSF) - Postman - Ettercap - Frida - Objection - Android SDK tools - ApkX - APK Studio

Topic	Details
	- Internet of Things (IoT) devices • BLE attacks • Special considerations - Fragile environment - Availability concerns - Data corruption - Data exfiltration • Vulnerabilities - Insecure defaults - Cleartext communication - Hard-coded configurations - Outdated firmware/hardware - Data leakage - Use of insecure or outdated components - Data storage system vulnerabilities • Misconfigurations—on-premises and cloud-based - Default/blank username/password - Network exposure • Lack of user input sanitization • Underlying software vulnerabilities • Error messages and debug handling • Injection vulnerabilities - Single quote method - Management interface vulnerabilities • Intelligent platform management interface (IPMI) - Vulnerabilities related to supervisory control and data acquisition (SCADA)/Industrial Internet of Things (IIoT)/industrial control system (ICS) - Vulnerabilities related to virtual environments • Virtual machine (VM) escape • Hypervisor vulnerabilities • VM repository vulnerabilities - Vulnerabilities related to containerized workloads
Given a scenario, perform a social	- Pretext for an approach - Social engineering attacks

Topic	Details
engineering or physical attack.	• Email phishing - Whaling - Spear phishing • Vishing • Short message service (SMS) phishing • Universal Serial Bus (USB) drop key • Watering hole attack - Physical attacks • Tailgating • Dumpster diving • Shoulder surfing • Badge cloning - Impersonation - Tools • Browser exploitation framework (BeEF) • Social engineering toolkit • Call spoofing tools - Methods of influence • Authority • Scarcity • Social proof • Urgency • Likeness • Fear
Given a scenario, perform post-exploitation techniques.	- Post-exploitation tools • Empire • Mimikatz • BloodHound - Lateral movement • Pass the hash - Network segmentation testing - Privilege escalation

Topic	Details
	• Horizontal • Vertical - Upgrading a restrictive shell - Creating a foothold/persistence • Trojan • Backdoor - Bind shell - Reverse shell • Daemons • Scheduled tasks - Detection avoidance • Living-off-the-land techniques/fileless malware - PsExec - Windows Management Instrumentation (WMI) - PowerShell (PS) remoting/Windows Remote Management (WinRM) • Data exfiltration • Covering your tracks • Steganography • Establishing a covert channel - Enumeration • Users • Groups • Forests • Sensitive data • Unencrypted files
Reporting and Communication - 18%	
Compare and contrast important components of written reports.	- Report audience • C-suite • Third-party stakeholders • Technical staff • Developers - Report contents (** not in a particular order)

Topic	Details
	• Executive summary • Scope details • Methodology - Attack narrative • Findings - Risk rating (reference framework) - Risk prioritization - Business impact analysis • Metrics and measures • Remediation • Conclusion • Appendix - Storage time for report - Secure distribution - Note taking • Ongoing documentation during test • Screenshots - Common themes/root causes • Vulnerabilities • Observations • Lack of best practices
Given a scenario, analyze the findings and recommend the appropriate remediation within a report.	- Technical controls • System hardening • Sanitize user input/parameterize queries • Implemented multifactor authentication • Encrypt passwords • Process-level remediation • Patch management • Key rotation • Certificate management • Secrets management solution • Network segmentation - Administrative controls • Role-based access control

Topic	Details
	• 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
Explain the importance of communication during the penetration testing process.	- Communication path • Primary contact • Technical contact • Emergency contact - Communication triggers • Critical findings • Status reports • Indicators of prior compromise - Reasons for communication • Situational awareness • De-escalation • Deconfliction • Identifying false positives • Criminal activity - Goal reprioritization - Presentation of findings
Explain post-report delivery activities.	- Post-engagement cleanup • Removing shells • Removing tester-created credentials • Removing tools

Topic	Details
	- Client acceptance - Lessons learned - Follow-up actions/retest - Attestation of findings - Data destruction process
Tools and Code Analysis - 16%	
Explain the basic concepts of scripting and software development.	- Logic constructs • Loops • Conditionals • Boolean operator • String operator • Arithmetic operator - Data structures • JavaScript Object Notation (JSON) • Key value • Arrays • Dictionaries • Comma-separated values (CSV) • Lists • Trees - Libraries - Classes - Procedures - Functions
Given a scenario, analyze a script or code sample for use in a penetration test.	- Shells • Bash • PS - Programming languages • Python • Ruby • Perl • JavaScript - Analyze exploit code to:

Topic	Details
	• Download files • Launch remote access • Enumerate users • Enumerate assets - Opportunities for automation • Automate penetration testing process - Perform port scan and then automate next steps based on results - Check configurations and produce a report • Scripting to modify IP addresses during a test • Nmap scripting to enumerate ciphers and produce reports
Explain use cases of the following tools during the phases of a penetration test. (**The intent of this objective is NOT to test specific vendor feature sets.)	- Scanners • Nikto • Open vulnerability assessment scanner (Open VAS) • SQLmap • Nessus • Open Security Content Automation Protocol (SCAP) • Wapiti • WPScan • Brakeman • Scout Suite - Credential testing tools • Hashcat • Medusa • Hydra • CeWL • John the Ripper • Cain • Mimikatz • Patator • DirBuster - Debuggers

Topic	Details
	• OllyDbg • Immunity Debugger • GNU Debugger (GDB) • WinDbg • Interactive Disassembler (IDA) • Covenant • SearchSploit - OSINT • WHOIS • Nslookup • Fingerprinting Organization with Collected Archives (FOCA) • theHarvester • Shodan • Maltego • Recon-ng • Censys - Wireless • Aircrack-ng suite • Kismet • Wifite2 • Rogue access point • EAPHammer • mdk4 • Spooftooph • Reaver • Wireless Geographic Logging Engine (WiGLE) • Fern - Web application tools • OWASP ZAP • Burp Suite • Gobuster • w3af - Social engineering tools

Topic	Details
	• Social Engineering Toolkit (SET) • BeEF - Remote access tools • Secure Shell (SSH) • Ncat • Netcat • ProxyChains - Networking tools • Wireshark • Hping - Misc. • SearchSploit • Responder • Impacket tools • Empire • Metasploit • mitm6 • CrackMapExec • TruffleHog • Censys - Steganography tools • Openstego • Steghide • Snow • Coagula • Sonic Visualiser • TinEye - Cloud tools • Scout Suite • CloudBrute • Pacu • Cloud Custodian

Prepare with PT0-002 Sample Questions:

Question: 1

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site.

Which of the following recommendations would BEST address this situation?

a) Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
b) Implement a recurring cybersecurity awareness education program for all users.
c) Implement multifactor authentication on all corporate applications.
d) Implement an email security gateway to block spam and malware from email communications.

Answer: b

Question: 2

During which phase of a penetration testing engagement does a penetration tester clearly define the scope of the engagement?

a) Master penetration rules agreement
b) Service level agreement
c) Planning and preparation phase
d) Pre-setup phase

Answer: c

Question: 3

Which of the following is the process of distributing, installing, and applying software updates?

a) Patch management
b) Key rotation
c) Encryption of passwords
d) Process-level remediation

Answer: a

Question: 4

Cyber war and cyber espionage are both related to which type of threat actors?

a) Hacktivists
b) State-sponsored attackers
c) Organized crime
d) Insider threats

Answer: b

Question: 5

How can an attacker maintain persistence of a compromised system?

a) Send phishing email links
b) Create a bind or reverse shell
c) Use an evil twin
d) Ping the core processor

Answer: b

Question: 6

What type of attack uses a password hash collected from a compromised system and then uses the same hash to log in to another client or server system?

a) Brute force
b) Evil twin
c) Pass-the-hash attack
d) Pass-the-password attack

Answer: c

Question: 7

Job rotation, mandatory vacations, and user training are examples of which types of controls?

a) Operational controls
b) Administrative controls
c) Physical controls
d) None of these answers are correct.

Answer: a

Question: 8

When was the Security Standards for the Protection of Electronic Protected Health Information, known as the HIPAA Security Rule, published?

a) March 1963
b) July 2021
c) February 2003
d) September 1970

Answer: c

Question: 9

Organizations sometimes require which of the following to feel comfortable with the penetration testing team that they are giving access to their environment and information?

a) Fingerprints
b) Polygraphs
c) Down payment
d) Background checks

Answer: d

Question: 10

Bash is a command shell and language interpreter that is available for operating systems such as Linux, macOS, and even Windows. The name Bash is an acronym for Bourne-Again shell. What does a shell do?

a) It deletes temporary files.
b) It deletes application logs.
c) It suppresses Syslog messages.
d) It allows for interactive or non-interactive command execution.

Answer: d

Study Tips to Pass the CompTIA PenTest+ Exam:

Understand the PT0-002 Exam Format:

Before diving into your study routine, it's essential to familiarize yourself with the PT0-002 exam format. Take the time to review the **exam syllabus**, understand the test structure, and identify the key areas of focus. Prior knowledge of what to expect on exam day will help you tailor your study plan.

Make A Study Schedule for the PT0-002 Exam:

To effectively prepare for the PT0-002 exam, make a study schedule that fits your lifestyle and learning style. Set specific time slots for studying each day and focus on the topics based on their importance and your proficiency level. Consistency is a must, so stick to your schedule and avoid procrastination.

Study from Different Resources:

Make sure to expand beyond one source of study material. Utilize multiple resources such as textbooks, online courses, practice exams, and study guides to understand the PT0-002 exam topics comprehensively. Each resource offers unique insights and explanations that can enhance your learning experience.

Practice Regularly for the PT0-002 Exam:

Practice makes you perfect for the PT0-002 exam preparation as well. Regular practice allows you to reinforce your knowledge of key concepts, enhance your problem-solving skills, and familiarize yourself with the exam format. Dedicate time to solving practice questions and **sample tests** to gauge your progress.

Take Breaks and Rest:

While it's essential to study, taking breaks and allowing yourself to rest is equally important. Overloading your brain with information without adequate rest can lead to burnout and decreased productivity. Set short breaks during your study sessions to recharge and maintain focus.

Stay Organized During the PT0-002 Exam Preparation:

Stay organized throughout your PT0-002 study journey by keeping track of your progress and materials. Maintain a tidy study space, use folders or digital

tools to organize your notes and resources, and create a checklist of topics to cover. An organized approach helps you stay on track and minimize stress.

Seek Clarification from Mentors:

Feel free to seek clarification if you encounter any confusing or challenging concepts during your study sessions. Reach out to peers, instructors, or online forums for assistance. Clarifying doubts early on will prevent misunderstandings and ensure you have a solid grasp of the material.

Regular Revision Plays A vital Role for the PT0-002 Exam:

Consistent revision is essential for the long-term retention of information. Review previously covered topics to reinforce your understanding and identify any areas requiring additional attention. Reviewing regularly will help solidify your knowledge and boost your confidence.

Practice Time Management for the PT0-002 Exam:

Effective time management is crucial on exam day to ensure you complete all sections within the allocated time frame. During your practice sessions, simulate PT0-002 exam conditions and practice pacing yourself accordingly. Develop strategies for tackling each section efficiently to maximize your score.

Stay Positive and Confident:

Lastly, always have a positive mindset and believe in your abilities. Stay confident in your preparation efforts and trust that you have adequately equipped yourself to tackle the PT0-002 exam. Visualize success, stay focused, and approach the exam calmly and confidently.

Benefits of Earning the PT0-002 Exam:

- Achieving the PT0-002 certification opens doors to new career opportunities and advancement within your field.
- The rigorous preparation required for the PT0-002 exam equips you with in-depth knowledge and practical skills relevant to your profession.
- Holding the PT0-002 certification demonstrates your expertise and commitment to excellence, earning recognition from peers and employers.
- Certified professionals often grab higher salaries and enjoy greater earning potential than their non-certified counterparts.
- Obtaining the PT0-002 certification validates your proficiency and credibility, instilling confidence in clients, employers, and colleagues.

Discover the Reliable Practice Test for the PT0-002 Certification:

EduSum.com brings you comprehensive information about the PT0-002 exam. We offer genuine practice tests tailored for the PT0-002 certification. What benefits do these practice tests offer? You'll encounter authentic exam-like questions crafted by industry experts, providing an opportunity to enhance your performance in the actual exam. Count on EduSum.com for rigorous, unlimited access to PT0-002 practice tests over two months, enabling you to bolster your confidence steadily. Through dedicated practice, many candidates have succeeded in streamlining their journey towards obtaining the CompTIA PenTest+.

Concluding Thoughts:

Preparing for the PT0-002 exam requires dedication, strategy, and effective study techniques. These study tips can enhance your preparation, boost your confidence, and improve your chances of passing the exam with flying colors. Remember to stay focused, stay organized, and believe in yourself. Good luck!

Here is the Trusted Practice Test for the PT0-002 Certification

EduSum.com offers comprehensive details about the PT0-002 exam. Our platform provides authentic practice tests designed for the PT0-002 exam. What benefits do these practice tests offer? By accessing our practice tests, you will encounter questions closely resembling those crafted by industry experts in the exam. This allows you to enhance your performance and readiness for the real exam. Count on EduSum.com to provide rigorous practice opportunities, offering unlimited attempts over two months for the PT0-002 practice tests. Through consistent practice, many candidates have found success and simplified their journey towards attaining the CompTIA PenTest+.

Start Online Practice of PT0-002 Exam by Visiting URL

https://www.edusum.com/comptia/pt0-002-comptia-pentest