EDUSUM

#1 Online Certification Guide

# COMPTIA PT0-001

**CompTIA PenTest+ Certification Questions & Answers**

## Exam Summary – Syllabus –Questions

**PT0-001**

**CompTIA PenTest+**

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

## Table of Contents:

# Know Your PT0-001 Certification Well:

The PT0-001 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your PT0-001 preparation you may struggle to get all the crucial PenTest+ materials like PT0-001 syllabus, sample questions, study guide.

But don't worry the PT0-001 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 PT0-001 syllabus?
- How many questions are there in the PT0-001 exam?
- Which Practice test would help me to pass the PT0-001 exam at the first attempt?

Passing the PT0-001 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 PT0-001 PenTest+ Certification Details:

| | |
|---|---|
| Exam Name | CompTIA PenTest+ |
| Exam Code | PT0-001 |
| Exam Price | $370 (USD) |
| Duration | 165 mins |
| Number of Questions | 85 |
| Passing Score | 750 / 900 |
| Books / Training | **CompTIA PenTest+ Certification Training** |
| Schedule Exam | **Pearson VUE** |
| Sample Questions | **CompTIA PenTest+ Sample Questions** |
| Practice Exam | **CompTIA PT0-001 Certification Practice Exam** |

# PT0-001 Syllabus:

| Topic | Details |
|---|---|
| Planning and Scoping - 15% | |
| Explain the importance of planning for an engagement. | 1. Understanding the target audience<br>2. Rules of engagement<br>3. Communication escalation path<br>4. Resources and requirements<br>• Confidentiality of findings<br>• Known vs. unknown<br>5. Budget<br>6. Impact analysis and remediation timelines<br>7. Disclaimers<br>• Point-in-time assessment<br>• Comprehensiveness<br>8. Technical constraints<br>9. Support resources<br>• WSDL/WADL<br>• SOAP project file<br>• SDK documentation<br>• Swagger document<br>• XSD<br>• Sample application requests<br>• Architectural diagrams |
| Explain key legal concepts. | 1. Contracts<br>• SOW<br>• MSA<br>• NDA<br>2. Environmental differences<br>• Export restrictions<br>• Local and national government restrictions<br>• Corporate policies<br>3. Written authorization |

| Topic | Details |
|---|---|
|  | • Obtain signature from proper signing authority<br>• Third-party provider authorization when necessary |
| Explain the importance of scoping an engagement properly. | 1. Types of assessment<br>• Goals-based/objectives-based<br>• Compliance-based<br>• Red team<br>2. Special scoping considerations<br>• Premerger<br>• Supply chain<br>3. Target selection<br>• Targets<br>Internal<br>On-site vs. off-site<br>External<br>First-party vs. third-party hosted<br>Physical<br>Users<br>SSIDs<br>Applications<br>• Considerations<br>White-listed vs. black-listed<br>Security exceptions<br>IPS/WAF whitelist<br>NAC<br>Certificate pinning<br>Company's policies<br>4. Strategy<br>• Black box vs. white box vs. gray box<br>5. Risk acceptance<br>6. Tolerance to impact<br>7. Scheduling<br>8. Scope creep<br>9. Threat actors |

| Topic | Details |
|---|---|
| | - Adversary tier<br>APT<br>Script kiddies<br>Hacktivist<br>Insider threat<br>- Capabilities<br>- Intent<br>- Threat models |
| Explain the key aspects of compliance-based assessments. | 1. Compliance-based assessments, limitations and caveats<br>- Rules to complete assessment<br>- Password policies<br>- Data isolation<br>- Key management<br>- Limitations<br>Limited network access<br>Limited storage access<br>2. Clearly defined objectives based on regulations |
| **Information Gathering and Vulnerability Identification - 22%** | |
| Given a scenario, conduct information gathering using appropriate techniques. | 1. Scanning<br>2. Enumeration<br>- Hosts<br>- Networks<br>- Domains<br>- Users<br>- Groups<br>- Network shares<br>- Web pages<br>- Applications<br>- Services<br>- Tokens<br>- Social networking sites<br>3. Packet crafting<br>4. Packet inspection<br>5. Fingerprinting<br>6. Cryptography |

| Topic | Details |
|---|---|
| | • Certificate inspection<br>7. Eavesdropping<br>• RF communication monitoring<br>• Sniffing<br>Wired<br>Wireless<br>8. Decompilation<br>9. Debugging<br>10. Open Source Intelligence Gathering<br>• Sources of research<br>CERT<br>NIST<br>JPCERT<br>CAPEC<br>Full disclosure<br>CVE<br>CWE |
| Given a scenario, perform a vulnerability scan. | 1. Credentialed vs. non-credentialed<br>2. Types of scans<br>• Discovery scan<br>• Full scan<br>• Stealth scan<br>• Compliance scan<br>3. Container securit<br>4. Application scan<br>• Dynamic vs. static analysis<br>5. Considerations of vulnerability scanning<br>• Time to run scans<br>• Protocols used<br>• Network topology<br>• Bandwidth limitations<br>• Query throttling<br>• Fragile systems/non-traditional assets |

| Topic | Details |
|---|---|
| Given a scenario, analyze vulnerability scan results. | 1. Asset categorization<br>2. Adjudication<br>- False positives<br>3. Prioritization of vulnerabilities<br>4. Common themes<br>- Vulnerabilities<br>- Observations<br>- Lack of best practices |
| Explain the process of leveraging information to prepare for exploitation. | 1. Map vulnerabilities to potential exploits<br>2. Prioritize activities in preparation for penetration test<br>3. Describe common techniques to complete attack<br>- Cross-compiling code<br>- Exploit modification<br>- Exploit chaining<br>- Proof-of-concept development (exploit development)<br>- Social engineering<br>- Credential brute forcing<br>- Dictionary attacks<br>- Rainbow tables<br>- Deception |
| Explain weaknesses related to specialized systems. | 1. ICS<br>2. SCADA<br>3. Mobile<br>4. IoT<br>5. Embedded<br>6. Point-of-sale system<br>7. Biometrics<br>8. Application containers<br>9. RTOS |
| **Attacks and Exploits - 30%** | |
| Compare and contrast social engineering attacks. | 1. Phishing<br>- Spear phishing<br>- SMS phishing<br>- Voice phishing |

| Topic | Details |
|---|---|
| | - Whaling<br>2. Elicitation<br>- Business email compromise<br>3. Interrogation<br>4. Impersonation<br>5. Shoulder surfing<br>6. USB key drop<br>7. Motivation techniques<br>- Authority<br>- Scarcity<br>- Social proof<br>- Urgency<br>- Likeness<br>- Fear |
| Given a scenario, exploit network-based vulnerabilities. | 1. Name resolution exploits<br>- NETBIOS name service<br>- LLMNR<br>2. SMB exploits<br>3. SNMP exploits<br>4. SMTP exploits<br>5. FTP exploits<br>6. DNS cache poisoning<br>7. Pass the hash<br>8. Man-in-the-middle<br>- ARP spoofing<br>- Replay<br>- Relay<br>- SSL stripping<br>- Downgrade<br>9. DoS/stress test<br>10. NAC bypass<br>11. VLAN hopping |
| Given a scenario, exploit wireless and RF-based vulnerabilities. | 1. Evil twin<br>- Karma attack<br>- Downgrade attack |

| Topic | Details |
|---|---|
|  | 2. Deauthentication attacks<br>3. Fragmentation attacks<br>4. Credential harvesting<br>5. WPS implementation weakness<br>6. Bluejacking<br>7. Bluesnarfing<br>8. RFID cloning<br>9. Jamming<br>10. Repeating |
| Given a scenario, exploit application-based vulnerabilities. | 1. Injections<br>• SQL<br>• HTML<br>• Command<br>• Code<br>2. Authentication<br>• Credential brute forcing<br>• Session hijacking<br>• Redirect<br>• Default credentials<br>• Weak credentials<br>• Kerberos exploits<br>3. Authorization<br>• Parameter pollution<br>• Insecure direct object reference<br>4. Cross-site scripting (XSS)<br>• Stored/persistent<br>• Reflected<br>• DOM<br>5. Cross-site request forgery (CSRF/XSRF)<br>6. Clickjacking<br>7. Security misconfiguration<br>• Directory traversal<br>• Cookie manipulation<br>8. File inclusion |

| Topic | Details |
|---|---|
| | • Local<br>• Remote<br>9. Unsecure code practices<br>• Comments in source code<br>• Lack of error handling<br>• Overly verbose error handling<br>• Hard-coded credentials<br>• Race conditions<br>• Unauthorized use of functions/unprotected APIs<br>• Hidden elements<br>• Lack of code signing |
| Given a scenario, exploit local host vulnerabilities. | 1. OS vulnerabilities<br>• Windows<br>• Mac OS<br>• Linux<br>• Android<br>• iOS<br>2. Unsecure service and protocol configurations<br>3. Privilege escalation<br>• Linux-specific<br>SUID/SGID programs<br>Unsecure SUDO<br>Ret2libc<br>Sticky bits<br>• Windows-specific<br>Cpassword<br>Clear text credentials in LDAP<br>Kerberoasting<br>Credentials in LSASS<br>Unattended installation<br>SAM database<br>DLL hijacking<br>• Exploitable services<br>Unquoted service paths<br>Writable services<br>• Unsecure file/folder permissions<br>• Keylogger |

| Topic | Details |
|---|---|
|  | • Scheduled tasks<br>• Kernel exploits<br>4. Default account settings<br>5. Sandbox escape<br>• Shell upgrade<br>• VM<br>• Container<br>6. Physical device security<br>• Cold boot attack<br>• JTAG debug<br>• Serial console |
| Summarize physical security attacks related to facilities. | 1. Piggybacking/tailgating<br>2. Fence jumping<br>3. Dumpster diving<br>4. Lock picking<br>5. Lock bypass<br>6. Egress sensor<br>7. Badge cloning |
| Given a scenario, perform post-exploitation techniques. | 1. Lateral movement<br>• RPC/DCOM<br>PsExec<br>WMI<br>Scheduled tasks<br>• PS remoting/WinRM<br>• SMB<br>• RDP<br>• Apple Remote Desktop<br>• VNC<br>• X-server forwarding<br>• Telnet<br>• SSH<br>• RSH/Rlogin<br>2. Persistence<br>• Scheduled jobs<br>• Scheduled tasks |

| Topic | Details |
|---|---|
| | • Daemons<br>• Back doors<br>• Trojan<br>• New user creation<br>3. Covering your tracks |
| | **Penetration Testing Tools - 17%** |
| Given a scenario, use Nmap to conduct information gathering exercises. | 1. SYN scan (-sS) vs. full connect scan (-sT)<br>2. Port selection (-p)<br>3. Service identification (-sV)<br>4. OS fingerprinting (-O)<br>5. Disabling ping (-Pn)<br>6. Target input file (-iL)<br>7. Timing (-T)<br>8. Output parameters<br>• oA<br>• oN<br>• oG<br>• oX |
| Compare and contrast various use cases of tools. | 1. Use cases<br>• Reconnaissance<br>• Enumeration<br>• Vulnerability scanning<br>• Credential attacks<br>Offline password cracking<br>Brute-forcing services<br>• Persistence<br>• Configuration compliance<br>• Evasion<br>• Decompilation<br>• Forensics<br>• Debugging<br>• Software assurance<br>Fuzzing<br>SAST<br>DAST<br>2. Tools |

| Topic | Details |
|---|---|
|  | • Scanners<br>Nikto<br>OpenVAS<br>SQLmap<br>Nessus<br>• Credential testing tools<br>Hashcat<br>Medusa<br>Hydra<br>Cewl<br>John the Ripper<br>Cain and Abel<br>Mimikatz<br>Patator<br>Dirbuster<br>W3AF<br>• Debuggers<br>OLLYDBG<br>Immunity debugger<br>GDB<br>WinDBG<br>IDA<br>• Software assurance<br>Findbugs/findsecbugs<br>Peach<br>AFL<br>SonarQube<br>YASCA<br>• OSINT<br>Whois |

| Topic | Details |
|---|---|
| | Nslookup<br>Foca<br>Theharvester<br>Shodan<br>Maltego<br>Recon-NG<br>Censys<br>• Wireless<br>Aircrack-NG<br>Kismet<br>WiFite<br>• Web proxies<br>OWASP ZAP<br>Burp Suite<br>• Social engineering tools<br>SET<br>BeEF<br>• Remote access tools<br>SSH<br>NCAT<br>NETCAT<br>Proxychains<br>• Networking tools<br>Wireshark<br>Hping<br>• Mobile tools<br>Drozer<br>APKX<br>APK studio<br>• MISC<br>Searchsploit<br>Powersploit<br>Responder<br>Impacket<br>Empire<br>Metasploit framework |
| Given a scenario, analyze tool output | 1. Password cracking<br>2. Pass the hash |

| Topic | Details |
|---|---|
| or data related to a penetration test. | 3. Setting up a bind shell<br>4. Getting a reverse shell<br>5. Proxying a connection<br>6. Uploading a web shell<br>7. Injections |
| Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell). | 1. Logic<br>• Looping<br>• Flow control<br>2. I/O<br>• File vs. terminal vs. network<br>3. Substitutions<br>4. Variables<br>5. Common operations<br>• String operations<br>• Comparisons<br>6. Error handling<br>7. Arrays<br>8. Encoding/decoding |
| **Reporting and Communication - 16%** | |
| Given a scenario, use report writing and handling best practices. | 1. Normalization of data<br>2. Written report of findings and remediation<br>• Executive summary<br>• Methodology<br>• Findings and remediation<br>• Metrics and measures<br>Risk rating<br>• Conclusion<br>3. Risk appetite<br>4. Storage time for report<br>5. Secure handling and disposition of reports |
| Explain post-report delivery activities. | 1. Post-engagement cleanup<br>• Removing shells<br>• Removing tester-created credentials |

| Topic | Details |
|---|---|
| | - Removing tools<br>2. Client acceptance<br>3. Lessons learned<br>4. Follow-up actions/retest<br>5. Attestation of findings |
| Given a scenario, recommend mitigation strategies for discovered vulnerabilities. | 1. Solutions<br>- People<br>- Process<br>- Technology<br>2. Findings<br>- Shared local administrator credentials<br>- Weak password complexity<br>- Plain text passwords<br>- No multifactor authentication<br>- SQL injection<br>- Unnecessary open services<br>3. Remediation<br>- Randomize credentials/LAPS<br>- Minimum password requirements/password filters<br>- Encrypt the passwords<br>- Implement multifactor authentication<br>- Sanitize user input/parameterize queries<br>- System hardening |
| Explain the importance of communication during the penetration testing process. | 1. Communication path<br>2. Communication triggers<br>- Critical findings<br>- Stages<br>- Indicators of prior compromise<br>3. Reasons for communication<br>- Situational awareness<br>- De-escalation<br>- De-confliction<br>4. Goal reprioritization |

# CompTIA PT0-001 Sample Questions:

## Question: 1

A potential customer is looking to test the security of its network. One of the customer's primary concerns is the security awareness of its employees.

Which type of test would you recommend that the company perform as part of the penetration test?

a) Social engineering testing
b) Wireless testing
c) Network testing
d) Web application testing

**Answer: a**

## Question: 2

The SELinux and AppArmor security frameworks include enforcement rules that attempt to prevent which of the following attacks?

a) Lateral movement
b) Sandbox escape
c) Cross-site request forgery (CSRF)
d) Cross-site- scripting (XSS)

**Answer: b**

## Question: 3

Which of the following can be used for post-exploitation activities?

a) WinDbg
b) IDA
c) Maltego
d) PowerShell

**Answer: d**

## Question: 4

You can find XSS vulnerabilities in which of the following?

a) Search fields that echo a search string back to the user
b) HTTP headers
c) Input fields that echo user data
d) All of the above

**Answer: d**

## Question: 5

What elements should you be sure to remove from an exploited system before finalizing a penetration test?

a) User accounts created
b) Shells spawned
c) Any files left behind
d) Administrator account

**Answer: a, b, c**

## Question: 6

Software developers should escape all characters (including spaces but excluding alphanumeric characters) with the HTML entity &#xHH; format to prevent what type of attack?

a) DDoS attacks
b) XSS attacks
c) CSRF attacks
d) Brute-force attacks

**Answer: b**

## Question: 7

When running an Nmap SYN scan, what will be the Nmap result if ports on the target device do not respond?

a) Open
b) Closed
c) Filtered
d) Listening

**Answer: c**

## Question: 8

Which of the following can be used with John the Ripper to crack passwords?

a) Wordlists
b) Nmap
c) Meterpreter
d) PowerSploit

**Answer: a**

## Question: 9

Which tool included in Kali is most helpful in compiling a quality penetration testing report?

a) Nmap
b) Metasploit
c) Dradis
d) SET

**Answer: c**

## Question: 10

A _______ vulnerability scan would typically be focused on a specific set of requirements.

a) Full
b) Stealth
c) Compliance
d) Discovery

**Answer: c**

# Study Guide to Crack CompTIA PenTest+ PT0-001 Exam:

- Getting details of the PT0-001 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 PT0-001 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 PT0-001 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 PT0-001 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 PT0-001 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

## Reliable Online Practice Test for PT0-001 Certification

Make EduSum.com your best friend during your CompTIA PenTest+ exam preparation. We provide authentic practice tests for the PT0-001 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual PT0-001 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 PT0-001 exam.

**Start Online practice of PT0-001 Exam by visiting URL**
**https://www.edusum.com/comptia/pt0-001-comptia-pentest-plus**