CompTIA PenTest+ Certification Exam Objectives

EXAM NUMBER: PT0-001

About the Exam

The CompTIA PenTest+ exam will certify the successful candidate has the knowledge and skills required to:

- Plan and scope an assessment
- Understand legal and compliance requirements
- Perform vulnerability scanning and penetration testing using appropriate tools and techniques
- Analyze the results

In addition, the candidate will be able to:

- Produce a written report containing proposed remediation techniques
- Effectively communicate results to management
- Provide practical recommendations

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	PT0-001
Number of questions	Maximum of 80
Type of questions	Multiple choice and performance-based
Length of test	165 minutes
Recommended experience	3 –4 years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management
Passing score	750

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
Total	**100%**

1.0 Planning and Scoping

1.1 Explain the importance of planning for an engagement.

- **Understanding the target audience**
- **Rules of engagement**
- **Communication escalation path**
- **Resources and requirements**
  - Confidentiality of findings
  - Known vs. unknown
- **Budget**
- **Impact analysis and remediation timelines**
- **Disclaimers**
  - Point-in-time assessment
  - Comprehensiveness
- **Technical constraints**
- **Support resources**
  - WSDL/WADL
  - SOAP project file
  - SDK documentation
  - Swagger document
  - XSD
  - Sample application requests
  - Architectural diagrams

1.2 Explain key legal concepts.

- **Contracts**
  - SOW
  - MSA
  - NDA
- **Environmental differences**
  - Export restrictions
  - Local and national government restrictions
  - Corporate policies
- **Written authorization**
  - Obtain signature from proper signing authority
  - Third-party provider authorization when necessary

1.3 Explain the importance of scoping an engagement properly.

- **Types of assessment**
  - Goals-based/objectives-based
  - Compliance-based
  - Red team
- **Special scoping considerations**
  - Premerger
  - Supply chain
- **Target selection**
  - Targets
    - Internal
      - On-site vs. off-site
    - External
    - First-party vs. third-party hosted
    - Physical
    - Users
    - SSIDs
    - Applications
  - Considerations
    - White-listed vs. black-listed
    - Security exceptions
      - IPS/WAF whitelist
      - NAC
      - Certificate pinning
      - Company's policies
- **Strategy**
  - Black box vs. white box vs. gray box
- **Risk acceptance**
- **Tolerance to impact**
- **Scheduling**
- **Scope creep**
- **Threat actors**
  - Adversary tier
    - APT
    - Script kiddies
    - Hacktivist
    - Insider threat
  - Capabilities
  - Intent
  - Threat models

1.4 Explain the key aspects of compliance-based assessments.

- **Compliance-based assessments, limitations, and caveats**
    - Rules to complete assessment
    - Password policies
    - Data isolation
    - Key management
    - Limitations
        - Limited network access
        - Limited storage access
- **Clearly defined objectives based on regulations**

2.0 Information Gathering and Vulnerability Identification

2.1 Given a scenario, conduct information gathering using appropriate techniques.

- **Scanning**
- **Enumeration**
    - Hosts
    - Networks
    - Domains
    - Users
    - Groups
    - Network shares
    - Web pages
    - Applications
    - Services
    - Tokens
    - Social networking sites
- **Packet crafting**
- **Packet inspection**
- **Fingerprinting**
- **Cryptography**
    - Certificate inspection
- **Eavesdropping**
    - RF communication monitoring
    - Sniffing
        - Wired
        - Wireless
- **Decompilation**
- **Debugging**
- **Open Source Intelligence Gathering**
    - Sources of research
        - CERT
        - NIST
        - JPCERT
        - CAPEC
        - Full disclosure
        - CVE
        - CWE

2.2 Given a scenario, perform a vulnerability scan.

- **Credentialed vs. non-credentialed**
- **Types of scans**
    - Discovery scan
    - Full scan
    - Stealth scan
    - Compliance scan
- **Container security**
- **Application scan**
    - Dynamic vs. static analysis
- **Considerations of vulnerability scanning**
    - Time to run scans
    - Protocols used
    - Network topology
    - Bandwidth limitations
    - Query throttling
    - Fragile systems/non-traditional assets

2.3 Given a scenario, analyze vulnerability scan results.

- **Asset categorization**
- **Adjudication**
    - False positives
- **Prioritization of vulnerabilities**
- **Common themes**
    - Vulnerabilities
    - Observations
    - Lack of best practices

2.4 Explain the process of leveraging information to prepare for exploitation.

- **Map vulnerabilities to potential exploits**
- **Prioritize activities in preparation for penetration test**
- **Describe common techniques to complete attack**
    - Cross-compiling code
    - Exploit modification
    - Exploit chaining
    - Proof-of-concept development (exploit development)
    - Social engineering
    - Credential brute forcing
    - Dictionary attacks
    - Rainbow tables
    - Deception

2.5 Explain weaknesses related to specialized systems.

- **ICS**
- **SCADA**
- **Mobile**
- **IoT**
- **Embedded**
- **Point-of-sale system**
- **Biometrics**
- **Application containers**
- **RTOS**

3.0 Attacks and Exploits

3.1 Compare and contrast social engineering attacks.

- Phishing
  - Spear phishing
  - SMS phishing
  - Voice phishing
  - Whaling
- Elicitation
  - Business email compromise
- Interrogation
- Impersonation
- Shoulder surfing
- USB key drop
- Motivation techniques
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear

3.2 Given a scenario, exploit network-based vulnerabilities.

- Name resolution exploits
  - NETBIOS name service
  - LLMNR
- SMB exploits
- SNMP exploits
- SMTP exploits
- FTP exploits
- DNS cache poisoning
- Pass the hash
- Man-in-the-middle
  - ARP spoofing
  - Replay
  - Relay
  - SSL stripping
  - Downgrade
- DoS/stress test
- NAC bypass
- VLAN hopping

3.3 Given a scenario, exploit wireless and RF-based vulnerabilities.

- Evil twin
  - Karma attack
  - Downgrade attack
- Deauthentication attacks
- Fragmentation attacks
- Credential harvesting
- WPS implementation weakness
- Bluejacking
- Bluesnarfing
- RFID cloning
- Jamming
- Repeating

3.4 Given a scenario, exploit application-based vulnerabilities.

- **Injections**
  - SQL
  - HTML
  - Command
  - Code
- **Authentication**
  - Credential brute forcing
  - Session hijacking
  - Redirect
  - Default credentials
  - Weak credentials
  - Kerberos exploits
- **Authorization**
  - Parameter pollution
  - Insecure direct object reference
- **Cross-site scripting (XSS)**
  - Stored/persistent
  - Reflected
  - DOM
- **Cross-site request forgery (CSRF/XSRF)**
- **Clickjacking**
- **Security misconfiguration**
  - Directory traversal
  - Cookie manipulation
- **File inclusion**
  - Local
  - Remote
- **Unsecure code practices**
  - Comments in source code
  - Lack of error handling
  - Overly verbose error handling
  - Hard-coded credentials
  - Race conditions
  - Unauthorized use of functions/unprotected APIs
  - Hidden elements
    - Sensitive information in the DOM
  - Lack of code signing

3.5 Given a scenario, exploit local host vulnerabilities.

- **OS vulnerabilities**
  - Windows
  - Mac OS
  - Linux
  - Android
  - iOS
- **Unsecure service and protocol configurations**
- **Privilege escalation**
  - Linux-specific
    - SUID/SGID programs
    - Unsecure SUDO
    - Ret2libc
    - Sticky bits
  - Windows-specific
    - Cpassword
    - Clear text credentials in LDAP
    - Kerberoasting
    - Credentials in LSASS
    - Unattended installation
    - SAM database
    - DLL hijacking
  - Exploitable services
    - Unquoted service paths
    - Writable services
  - Unsecure file/folder permissions
  - Keylogger
  - Scheduled tasks
  - Kernel exploits
- **Default account settings**
- **Sandbox escape**
  - Shell upgrade
  - VM
  - Container
- **Physical device security**
  - Cold boot attack
  - JTAG debug
  - Serial console

3.6 Summarize physical security attacks related to facilities.

- **Piggybacking/tailgating**
- **Fence jumping**
- **Dumpster diving**
- **Lock picking**
- **Lock bypass**
- **Egress sensor**
- **Badge cloning**

3.7 Given a scenario, perform post-exploitation techniques.

- **Lateral movement**
  - RPC/DCOM
    - PsExec
    - WMI
    - Scheduled tasks
  - PS remoting/WinRM
  - SMB
  - RDP
  - Apple Remote Desktop
  - VNC
  - X-server forwarding
  - Telnet
  - SSH
  - RSH/Rlogin
- **Persistence**
  - Scheduled jobs
  - Scheduled tasks
  - Daemons
  - Back doors
  - Trojan
  - New user creation
- **Covering your tracks**

4.0 Penetration Testing Tools

4.1 Given a scenario, use Nmap to conduct information gathering exercises.

- **SYN scan (-sS) vs. full connect scan (-sT)**
- **Port selection (-p)**
- **Service identification (-sV)**
- **OS fingerprinting (-O)**
- **Disabling ping (-Pn)**
- **Target input file (-iL)**
- **Timing (-T)**
- **Output parameters**
  - -oA
  - -oN
  - -oG
  - -oX

4.2 Compare and contrast various use cases of tools.

(**The intent of this objective is NOT to test specific vendor feature sets.)

- **Use cases**
  - Reconnaissance
  - Enumeration
  - Vulnerability scanning
  - Credential attacks
    - Offline password cracking
    - Brute-forcing services
  - Persistence
  - Configuration compliance
  - Evasion
  - Decompilation
  - Forensics
  - Debugging
  - Software assurance
    - Fuzzing
    - SAST
    - DAST
- **Tools**
  - Scanners
    - Nikto
    - OpenVAS
    - SQLmap
    - Nessus
  - Credential testing tools
    - Hashcat
    - Medusa
    - Hydra
    - Cewl
    - John the Ripper
    - Cain and Abel
    - Mimikatz
    - Patator
    - Dirbuster
    - W3AF
  - Debuggers
    - OLLYDBG
    - Immunity debugger
    - GDB
    - WinDBG
    - IDA
  - Software assurance
    - Findbugs/findsecbugs
    - Peach
    - Dynamo
    - AFL
    - SonarQube
    - YASCA
  - OSINT
    - Whois
    - Nslookup
    - Foca
    - Theharvester
    - Shodan
    - Maltego
    - Recon-NG
    - Censys
  - Wireless
    - Aircrack-NG
    - Kismet
    - WiFite
  - Web proxies
    - OWASP ZAP
    - Burp Suite
  - Social engineering tools
    - SET
    - BeEF
  - Remote access tools
    - SSH
    - NCAT
    - NETCAT
    - Proxychains
  - Networking tools
    - Wireshark
    - Hping
  - Mobile tools
    - Androzer
    - APKX
    - APK studio
  - MISC
    - Searchsploit
    - Powersploit
    - Responder
    - Impacket
    - Empire
    - Metasploit framework

4.3 Given a scenario, analyze tool output or data related to a penetration test.

- Password cracking
- Pass the hash
- Setting up a bind shell
- Getting a reverse shell
- Proxying a connection
- Uploading a web shell
- Injections

4.4 Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

- Logic
  - Looping
  - Flow control
- I/O
  - File vs. terminal vs. network
- Substitutions
- Variables
- Common operations
  - String operations
  - Comparisons
- Error handling
- Arrays
- Encoding/decoding

5.0 Reporting and Communication

5.1 Given a scenario, use report writing and handling best practices.

- **Normalization of data**
- **Written report of findings and remediation**
  - Executive summary
  - Methodology
  - Findings and remediation
  - Metrics and measures
    - Risk rating
  - Conclusion
- **Risk appetite**
- **Storage time for report**
- **Secure handling and disposition of reports**

5.2 Explain post-report delivery activities.

- **Post-engagement cleanup**
  - Removing shells
  - Removing tester-created credentials
  - Removing tools
- **Client acceptance**
- **Lessons learned**
- **Follow-up actions/retest**
- **Attestation of findings**

5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

- **Solutions**
  - People
  - Process
  - Technology
- **Findings**
  - Shared local administrator credentials
  - Weak password complexity
  - Plain text passwords
  - No multifactor authentication
  - SQL injection
  - Unnecessary open services
- **Remediation**
  - Randomize credentials/LAPS
  - Minimum password requirements/password filters
  - Encrypt the passwords
  - Implement multifactor authentication
  - Sanitize user input/parameterize queries
  - System hardening

5.4 Explain the importance of communication during the penetration testing process.

- **Communication path**
- **Communication triggers**
  - Critical findings
  - Stages
  - Indicators of prior compromise
- **Reasons for communication**
  - Situational awareness
  - De-escalation
  - De-confliction
- **Goal reprioritization**

CompTIA PenTest+ Acronyms

The following is a list of acronyms that appear on the CompTIA PenTest+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
ADFS	Active Directory Federation Services
AP	Access Point
API	Application Programming Interface
APNS	Apple Push Notification Service
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
BPA	Business Partnership Agreement
CA	Certificate Authority
CAPEC	Common Attack Patterns Enumeration Classification
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CIRT	Computer Incident Response Team
CORS	Cross-Origin Request Scripting
CRL	Certificate Revocation List
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Testing
DCOM	Distributed Component Object Model
DLL	Dynamic Link Library
DNS	Domain Name Service
DOM	Document Object Model
DoS	Denial of Service
EULA	End User License Agreement
FTP	File Transfer Protocol
GPO	Group Policy Object
GPP	Generic Packetized Protocol
HSTS	HTTP Strict Transport Security
HTML	HyperText Markup Language
I/O	Input/Output
ICS	Industrial Control Systems
IDOR	Indirect Object Reference
IoT	Internet of Things
IPS	Intrusion Prevention System
JPCERT	Japan Computer Emergency Response Team
JTAG	Joint Test Action Group
LAPS	Local Administrator Password Solution

ACRONYM	SPELLED OUT
LLMNR	Link Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MDM	Mobile Device Management
MFA	Multifactor Authentication
MITM	Man-in-the-Middle
MSA	Master Service Agreement
NAC	Network Access Control
NDA	Non-Disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NSE	Network Service Engine
OS	Operating System
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PS	PowerShell
RDP	Remote Desktop Protocol
RFP	Request for Proposal
RFID	Radio Frequent ID
ROE	Rules of Engagement
RPC	Remote Procedure Call
RSH	Remote Shell
RTOS	Real Time Operating System
SAM	Security Account Manager
SAN	Subject Alternative Name
SAST	Static Application Security Testing
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SDK	Software Development Kit
SGID	Set Group ID
SID	Secure Identifier
SLA	Service Level Agreement
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOC	Security Operation Center
SOW	Statement of Work
SQL	Structured Query Language

ACRONYM	SPELLED OUT
SSH	Secure Shell
SSL	Secure Sockets Layer
SUID	Set User ID
TPM	Transmission Control Protocol
UDP	User Diagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
WADL	Web Application Description Language
WAF	Web Application Firewall
WAR	Web Application Archive
WEP	Wired Equivalency Protocol
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPS	WiFi Protected Setup
WSDL	Web Services Description Language
XSD	XML Schema Document
XSS	Cross-Site Scripting
XST	Cross-Site Tracing

CompTIA PenTest+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CompTIA PenTest+ exam. This list may also be helpful for training companies who wish to create a lab component for their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

EQUIPMENT

- Laptops
- Wireless access points
- Servers
- Switches
- Cabling
- Monitors
- Firewalls
- HID/door access controls
- Wireless adapters capable of packet injection
- Directional antenna
- Mobile device

SPARE HARDWARE

- Cables
- Keyboards
- Mouse
- Power supplies
- Dongles/adapters

TOOLS

- Lock pick kit
- Badge cloner
- Fingerprint lifter

SOFTWARE

- OS licensing
- Open source OS
- Penetration testing frameworks
- Virtual machine software
- Scanning tools
- Credential testing tools
- Debuggers
- Software assurance tools
- Wireless testing tools
- Web proxying tools
- Social engineering tools
- Remote access tools
- Network tools
- Mobility testing tools

© 2017 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 04272-Oct2017