



CompTIA PenTest+ Certification Exam Objectives

EXAM NUMBER: PT0-003



About the Exam

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

- Plan, scope, and perform information gathering as part of a penetration test.
- Perform attacks that are aligned to and fulfill legal and compliance requirements.
- Perform each phase of a penetration test using and modifying appropriate tools and use the appropriate tactics, techniques, and procedures.
- Analyze the results of each phase of a penetration test to develop a written report, effectively communicate findings to stakeholders and provide practical recommendations.

EXAM ACCREDITATION

The CompTIA PenTest+ exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT 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”), they 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 | PT0-003 |
| Number of questions | Maximum of 90 |
| Types of questions | Multiple-choice and performance-based |
| Length of test | |
| Recommended experience | 3–4 years in a penetration tester job role |
| 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 | Engagement Management | 13% |
| 2.0 | Reconnaissance and Enumeration | 21% |
| 3.0 | Vulnerability Discovery and Analysis | 17% |
| 4.0 | Attacks and Exploits | 35% |
| 5.0 | Post-exploitation and Lateral Movement | 14% |
| Total | | 100% |



1.0 Engagement Management

1.1 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

1.2 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

1.3 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 Web 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)



1.4 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
 - Legal
 - Ethical
 - Quality control (QC)
 - Artificial intelligence (AI)

1.5 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



2.0 Reconnaissance and Enumeration

2.1 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
 - 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

2.2 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

2.3 Given a scenario, modify scripts for reconnaissance and enumeration.

- Information gathering
- Data manipulation
- Scripting languages
 - Bash
 - Python
 - PowerShell
- Logic constructs
 - Loops
 - Conditionals
 - Boolean operator
 - String operator
 - Arithmetic operator
- Use of libraries, functions, and classes



2.4 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



3.0 Vulnerability Discovery and Analysis

3.1 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)
 - » Infrastructure as Code (IaC)
 - » Source code analysis
 - Mobile scan
 - 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
 - BloodHound
 - Tenable Nessus
 - PowerSploit
 - Grype
 - Trivy
 - Kube-hunter

- **Industrial control systems (ICS) vulnerability assessment**

- Manual assessment
- Port mirroring
- **Tools**
 - Nikto
 - Greenbone/Open Vulnerability Assessment Scanner (OpenVAS)
 - TruffleHog

3.2 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**

3.3 Explain physical security concepts.

- Tailgating
- Site surveys
- Universal Serial Bus (USB) drops
- Badge cloning
- Lock picking



4.0 Attacks and Exploits

4.1 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

4.2 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)
 - Wireshark/tcpdump
 - msfvenom
 - Responder
 - Hydra

4.3 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



4.4 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
- Unquoted service path injection
- **Tools**
 - Mimikatz
 - Rubeus
 - Certify
 - Seatbelt
 - PowerShell/PowerShell Integrated Scripting Environment (ISE)
 - PsExec
 - Evil-WinRM
 - Living off the land binaries (LOLBins)

4.5 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/DorBuster
 - Wfuzz
 - WPScan

4.6 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



4.7 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
 - Kismet

4.8 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)

4.9 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
- **Tools**
 - Scapy
- tcprelay
- Wireshark/tcpdump
- MobSF
- Frida
- Drozer
- Android Debug Bridge (ADB)
- Bluecrack

4.10 Given a scenario, use scripting to automate attacks.

- **PowerShell**
 - Empire/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



5.0 Post-exploitation and Lateral Movement

5.1 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

5.2 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
 - explore.exe
 - ftp.exe
 - mmc.exe
 - rundll
 - msbuild
 - route
 - strings/findstr.exe
- Covenant
- CrackMapExec
- Impacket
- Netcat
- sshuttle
- Proxychains
- PowerShell ISE
- Batch files
- Metasploit
- PsExec
- Mimikatz



5.3 Summarize concepts related to staging and exfiltration.

- File encryption and compression
- Covert channel
 - Steganography
 - DNS
 - Internet Control Message Protocol (ICMP)
 - HTTPS
- Email
- Cross-account resources
- Cloud storage
- Alternate data streams
- Text storage sites
- Virtual drive mounting

5.4 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 PenTest+ PT0-003 Acronym List

The following is a list of acronyms that appear on the CompTIA PenTest+ PT0-003 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

| Acronym | Spelled Out | Acronym | Spelled Out |
|----------------|--|----------------|---|
| AD | Active Directory | EPSS | Exploit Prediction Scoring System |
| ADB | Android Debug Bridge | EXIF | Exchangeable Image File Format |
| AI | Artificial Intelligence | FQDN | Fully Qualified Domain Name |
| AP | Access Point | FTP | File Transfer Protocol |
| API | Application Programming Interface | GIF | Graphic Interchange Format |
| APT | Advanced Persistent Threat | HID | Host-based Intrusion Detection |
| BAS | Breach and Attack Simulation | HSTS | HTTP Strict Transport Security |
| BeEF | Browser Exploitation Framework | HTML | Hypertext Markup Language |
| BGP | Border Gateway Protocol | HTTP | Hypertext Transfer Protocol |
| BIA | Business Intelligence Analytics | HTTPS | Hypertext Transfer Protocol Secure |
| C2 | Command and Control | IaC | Infrastructure as Code |
| CIDR | Classless Inter-domain Routing | IAM | Identity and Access Management |
| CGI | Common Gateway Interface | IAST | Interactive Application Security Testing |
| CI/CD | Continuous Integration/Continuous Delivery | ICMP | Internet Control Message Protocol |
| CLI | Command-line Interface | ICS | Industrial Control System |
| CME | CrackMapExec | IDOR | Insecure Direct Object Reference |
| CNAME | Canonical Name | IdP | Identity Provider |
| COFF | Common Object File Format | IDS | Intrusion Detection System |
| CREST | Council of Registered Ethical Security Testers | IGRP | Interior Gateway Routing Protocol |
| CSRF | Cross-site Request Forgery | IoT | Internet of Things |
| CVE | Common Vulnerabilities and Exposures | IP | Internet Protocol |
| CVSS | Common Vulnerability Scoring System | IPS | Intrusion Prevention System |
| CWE | Common Weakness Enumeration | ISE | Integrated Scripting Environment |
| DAST | Dynamic Application Security Testing | JWT | JSON Web Token |
| DCOM | Distributed Component Object Model | KDC | Key Distribution Center |
| DDoS | Distributed Denial of Service | KRBGT | Kerberos Ticket Granting Ticket |
| DMARC | Domain-based Message Authentication, Reporting, and Conformance | LDAP | Lightweight Directory Access Protocol |
| DNS | Domain Name System | LFI | Local File Inclusion |
| DoS | Denial of Service | LLMNR | Link-local Multicast Name Resolution |
| DREAD | Damage potential, Reproducibility, Exploitability, Affected users, Discoverability | LSASS | Local Security Authority Subsystem Service |
| DROWN | Decrypting RSA [Rivest-Shamir-Adleman] with Obsolete and Weakened Encryption | LOLBins | Living off the Land Binaries |
| EFSRPC | Encrypting File System Remote Protocol | LPD | Line Printer Daemon |
| ELF | Executable and Linkable Format | MAC | Media Access Control |
| | | MASVS | Mobile Application Security Verification Standard |
| | | MFA | Multifactor Authentication |
| | | MIB | Management Information Base |

| Acronym | Spelled Out |
|----------------|--|
| MMS | Multimedia Messaging Service |
| MSA | Master Services Agreement |
| MX | Mail Exchange |
| NDA | Non-disclosure Agreement |
| NFC | Near-field Communication |
| NSE | Nmap Scripting Engine |
| NTLM | New Technology LAN Manager |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| OIDC | OpenID Connect |
| OpenVAS | Open Vulnerability Assessment Scanner |
| OS | Operating System |
| OSINT | Open-source Intelligence |
| OSSTMM | Open-source Security Testing Methodology Manual |
| OT | Operational Technology |
| OWASP | Open Web Application Security Project |
| PTES | Penetration Testing Execution Standard |
| PWS | Preliminary Work Statement |
| QC | Quality Control |
| RCE | Remote Code Execution |
| RDP | Remote Desktop Protocol |
| RFI | Remote File Inclusion |
| RFID | Radio Frequency Identification |
| RPC | Remote Procedure Call |
| RIP | Routing Information Protocol |
| SaaS | Software as a Service |
| SAM | Security Account Manager |
| SAML | Security Assertion Markup Language |
| SAST | Static Application Security Testing |
| SCA | Software Composition Analysis |
| SCADA | Supervisory Control and Data Acquisition |
| SDK | Software Development Kit |
| SDLC | Software Development Life Cycle |
| SDR | Software-defined Radio |
| SET | Social Engineering Toolkit |
| SIEM | Security Information and Event Management |

| Acronym | Spelled Out |
|----------------|---|
| SMB | Server Message Block |
| SMS | Short Message Service |
| SNMP | Simple Network Management Protocol |
| SOA | Start of Authority |
| SOC | Security Operations Center |
| SoW | Statement of Work |
| SPN | Service Principal Name |
| SQL | Structured Query Language |
| SQLi | Structured Query Language Injection |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSO | Single Sign-on |
| SSL | Secure Socket Layer |
| SSRF | Server-side Request Forgery |
| STRIDE | Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege |
| TCP | Transmission Control Protocol |
| TGS | Ticket Granting Service |
| TLS | Transport Layer Security |
| ToS | Terms of Service |
| TTP | Techniques, Tactics, Procedures |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| VLAN | Virtual Local Area Network |
| VNC | Virtual Network Computing |
| VPN | Virtual Private Network |
| WAF | Web Application Firewall |
| WinRM | Windows Remote Management |
| WLAN | Wireless Local Area Network |
| WinRM | Windows Remote Management |
| WMI | Windows Management Instrumentation |
| WPAD | Web Proxy Auto Discovery |
| WPS | Wi-Fi Protected Setup |
| XSS | Cross-site Scripting |
| ZAP | Zed Attack Proxy |

PenTest+ Proposed Hardware and Software List

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

Hardware

- Computers
- Wireless access points
- Servers
- Switches
- Cabling
- Firewalls
- Router
- Host-based intrusion detection (HID)/door access controls
- Wireless adapters capable of packet injection
- Directional antenna
- Mobile device
- IoT equipment (cameras, micro-computer, smart TV, etc.)
- Bluetooth adapter
- Multifunction printers (wired/wireless enabled)
- NFC/RFID cloning equipment
- Lock pick kit (where applicable)
- Biometric device
- Programmable logic controller
 - Software-defined radio (SDR) kit
- USB flash drives

Software

- Access to cloud environment
 - Command-line interface (CLI) access
 - Management console access
 - Instances of cloud services
- OS licensing
- Open-source OS
- Penetration testing frameworks
- Virtual machine software
- Scanning tools
 - Vulnerability scanning tools
 - SAST
 - DAST
- Credential testing tools
 - Spraying tools
 - Password crackers
- Application security tools
- Debuggers
- Wireless testing tools
- Web proxy tools
- Social engineering tools
- Remote access tools
- Network tools
 - Protocol analyzers
 - Sniffing tools
- Mobility testing tools
- Open-source or publicly available security information and event management (SIEM)/intrusion detection system (IDS)/intrusion prevention system (IPS)/endpoint security tools
- C2 tools