Appendix A

Mapping Course Content to CompTIA Certification

Achieving CompTIA PenTest+ certification requires candidates to pass Exam PT0-002. This table describes where the exam objectives for Exam PT0-002 are covered in this course.

1.0 Planning and Scoping 1.1 Compare and contrast governance, risk, and compliance concepts.	Covered in
Regulatory compliance considerations	Lesson 1, Topic B
Payment Card Industry Data Security Standard (PCI DSS)	
General Data Protection Regulatin (GDPR)	
Location restrictions	Lesson 2, Topic A
Country limitations	
Tool restrictions	
Local laws	
Local government requirements	
Privacy requirements	
Legal concepts	Lesson 2, Topic C
Service-level agreement (SLA)	
Confidentiality	
Statement of work	
Non-disclosure agreement (NDA)	
Master service agreement	
Permission to attack	Lesson 2, Topic C

1.2 Explain the importance of scoping and organizational/customer requirements	Covered in
Standards and methodologies	Lesson 2, Topic C
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)	

1.2 Explain the importance of scoping and organizational/customer requirements	Covered in
Rules of engagement	Lesson 2, Topic B
Time of day	
Types of allowed/disallowed tests	
Other restrictions	
Environmental considerations	Lesson 2, Topic A
Network	
Application	
Cloud	
Target list/in-scope assets	Lesson 2, Topic A
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	
Validate scope of engagement	Lesson 2, Topic B
Question the client/review contracts	
Time management	
Strategy	
Unknown-environment vs. known-environment testing	

1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity	Covered in
Background checks of penetration testing team	Lesson 1, Topic D
Adhere to specific scope of engagement	Lesson 2, Topic B
Identify criminal activity	Lesson 1, Topic D
Immediately report breaches/criminal activity	Lesson 1, Topic D
Limit the use of tools to a particular engagement	Lesson 2, Topic B
Limit the invasiveness based on scope	Lesson 2, Topic B
Maintain confidentiality of data/information	Lesson 1, Topic D
Risk to the professional	Lesson 1, Topic D
Fees/fines	
Criminal charges	

2.0 Information Gathering and Vulnerability Scanning	
2.1 Given a scenario, perform passive reconnaissance	**Covered in**
DNS lookups	Lesson 7, Topic B
Identify technical contacts	Lesson 3, Topic A
Administrator contacts	Lesson 3, Topic C
Cloud vs. self-hosted	Lesson 3, Topic C
Social media scraping	Lesson 3, Topic C
Key contacts/job responsibilities	
Job listing/technology stack	
Cryptographic flaws	Lesson 3, Topic C
Secure Socket Layer (SSL) certificates	
Revocation	
Company reputation/security posture	Lesson 3, Topic A
Data	Lesson 3, Topic B
Password dumps	
File metadata	
Strategic search engine analysis/enumeration	
Website archive/caching	
Public source-code repositories	
Open-source intelligence (OSINT)	Lesson 3, Topic D
Tools	
Shodan	
Recon-ng	
Sources	Lesson 1, Topic C
Common weakness enumeration (CWE)	
Common vulnerabilities and exposures (CVE)	

2.2 Given a scenario, perform active reconnaissance	**Covered in**
Enumeration	Lesson 9, Topic A
Hosts	
Services	
Domains	
Users	
Uniform resource locators (URLs)	
Website reconnaissance	Lesson 3, Topic C
Crawling websites	
Scraping websites	
Manual inspection of web links	
robots.txt	
Packet crafting	Lesson 5, Topic C
Scapy	
Defense detection	Lesson 5, Topic B
Load balancer detection	
Web application firewall (WAF) detection	
Antivirus	
Firewall	

2.2 Given a scenario, perform active reconnaissance	Covered in
Tokens	Lesson 9, Topic B
Scoping	
Issuing	
Revocation	
Wardriving	Lesson 6, Topic C
Network traffic	Lesson 6, Topic B
Capture API requests and responses	
Sniffing	
Cloud asset discovery	Lesson 9, Topic D
Third-party hosted services	Lesson 13, Topic C
Detection avoidance	Lesson 8, Topic A

2.3 Given a scenario, analyze the results of a reconnaissance exercise	Covered in
Fingerprinting	Lesson 7, Topic A
Operating systems (OSs)	
Networks	
Network devices	
Software	
Analyze output from:	Lesson 7, Topic B
DNS lookups	Lesson 7, Topic B
Crawling websites	Lesson 3, Topic C
Network traffic	Lesson 7, Topic B
Address Resolution Protocol (ARP) traffic	Lesson 6, Topic B
Nmap scans	Lesson 7, Topic B
Web logs	Lesson 7, Topic B

2.4 Given a scenario, perform vulnerability scanning	Covered in
Considerations of vulnerability scanning	Lesson 5, Topic A
Time to run scans	
Protocols	
Network topology	
Bandwidth limitations	
Query throttling	
Fragile systems	
Non-traditional assets	
Scan identified targets for vulnerabilities	Lesson 6, Topic A
Set scan settings to avoid detection	Lesson 6, Topic A
Scanning methods	Lesson 6, Topic A
Stealth scan	
Transmission Control Protocol (TCP) connect scan	
Credentialed vs. non-credentialed	

2.4 Given a scenario, perform vulnerability scanning	**Covered in**
Nmap	Lesson 7, Topic A
Nmap Scripting Engine (NSE) scripts	
Common options	
A	
sV	
sT	
Pn	
O	
sU	
sS	
T 1-5	
script=vuln	
p	
Vulnerability testing tools that facilitate automation	Lesson 9, Topic B

3.0 Attacks and Exploits	
3.1 Given a scenario, research attack vectors and perform network attacks	**Covered in**
Stress testing for availability	Lesson 9, Topic B
Exploit resources	Lesson 9, Topic C
Exploit database (DB)	
Packet storm	
Attacks	Lesson 9, Topic B
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	Lesson 7, Topic C
Virtual local area network (VLAN) hopping	Lesson 9, Topic B
Network access control (NAC) bypass	Lesson 8, Topic A
Media access control (MAC) spoofing	Lesson 9, Topic B
Link-Local Multicast Name Resolution (LLMNR)/NetBIOS-Name Service (NBT-NS) poisoning	Lesson 9, Topic B
New Technology LAN Manager (NTLM) relay attacks	Lesson 9, Topic B
Tools	Lesson 9, Topic C
Metasploit	Lesson 9, Topic C
Netcat	Lesson 14, Topic B
Nmap	Lesson 7, Topic A

3.2 Given a scenario, research attack vectors and perform wireless attacks	Covered in
Attack methods	Lesson 10, Topic A
Eavesdropping	Lesson 10, Topic A
Data modification	Lesson 5, Topic A
Data corruption	Lesson 5, Topic A
Relay attacks	Lesson 10, Topic A
Spoofing	Lesson 10, Topic A
Deauthentication	Lesson 10, Topic A
Jamming	Lesson 10, Topic A
Capture handshakes	Lesson 10, Topic A
On-path	Lesson 9, Topic B
Attacks	Lesson 10, Topic A
Evil twin	Lesson 10, Topic A
Captive portal	Lesson 10, Topic A
Bluejacking	Lesson 11, Topic B
Bluesnarfing	Lesson 11, Topic B
Radio-frequency identification (RFID) cloning	Lesson 10, Topic A
Bluetooth Low Energy (BLE) attack	Lesson 12, Topic A
Amplification attacks [Nearfield communication (NFC)]	Lesson 10, Topic A
Wi-Fi protected setup (WPS) PIN attack	Lesson 10, Topic A
Tools	Lesson 10, Topic B
Aircrack-ng suite	Lesson 10, Topic B
Amplified antenna	Lesson 6, Topic C

3.3 Given a scenario, research attack vectors and perform application-based attacks	Covered in
OWASP Top 10	Lesson 13, Topic A
Server-side request forgery	Lesson 13, Topic B
Business logic flaws	Lesson 13, Topic B
Injection attacks	Lesson 13, Topic C
Structured Query Language (SQL) injection	
Blind SQL	
Boolean SQL	
Stacked queries	
Command injection	
Cross-site scripting	
Persistent	
Reflected	
Lightweight Directory Access Protocol (LDAP) injection	

3.3 Given a scenario, research attack vectors and perform application-based attacks	**Covered in**
Application vulnerabilities	Lesson 13, Topic A
Race conditions	
Lack of error handling	
Lack of code signing	
Insecure data transmission	
Session attacks	Lesson 13, Topic B
Session hijacking	
Cross-site request forgery (CSRF)	
Privilege escalation	
Session replay	
Session fixation	
API attacks	Lesson 13, Topic B
Restful	
Extensible Markup Language-Remote Procedure Call (XML-RPC)	
Soap	
Directory traversal	Lesson 13, Topic C
Tools	Lesson 14, Topic C
Web proxies	
OWASP Zed Attack Proxy (ZAP)	
Burp Suite community edition	
SQLmap	
DirBurster	
Resources	Lesson 16, Topic A
Word lists	

3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies	**Covered in**
Attacks	Lesson 9, Topic D
Credential harvesting	
Privilege escalation	
Account takeover	
Metadata service attack	
Misconfigured cloud assets	
Identity and access management (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	Lesson 14, Topic C
Software development kit (SDK)	

3.5 Explain common attacks and vulnerabilities against specialized systems	Covered in
Mobile	Lesson 11, Topic B
Attacks	
Reverse engineering	
Sandbox analysis	
Spamming	
Vulnerabilities	Lesson 11, Topic A
Insecure storage	
Passcode vulnerabilities	
Certificate pinning	Lesson 19, Topic A
Using known vulnerable components	Lesson 11, Topic A
Dependency vulnerabilities	Lesson 11, Topic A
Patching fragmentation	Lesson 11, Topic A
Execution of activities using root	Lesson 11, Topic B
Over-reach of permissions	Lesson 11, Topic B
Biometrics integrations	Lesson 11, Topic B
Business logic vulnerabilities	Lesson 11, Topic A
Tools	Lesson 11, Topic C
Burp Suite	
Drozer	
Mobile Security Framework (MobSF)	
Postman	
Ettercap	
Frida	
Objection	
Android SDK tools	
ApkX	
APK Studio	
Internet of Things (IoT) devices	Lesson 11, Topic C
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	

3.5 Explain common attacks and vulnerabilities against specialized systems	Covered in
Data storage system vulnerabilities	Lesson 11, Topic C
Misconfigurations—on premises and cloud-based	
Default/blank username/password	
Network exposure	
Lack of user input sanitization	Lesson 13, Topic A
Underlying software vulnerabilities	Lesson 12, Topic B
Error messages and debug handling	
Injection vulnerabilities	
Single quote method	Lesson 13, Topic C
Management interface vulnerabilities	Lesson 12, Topic B
Intelligent platform management interface (IPMI)	
Vulnerabilities related to supervisory control and data acquisition (SCADA)/Industrial Internet of Things (IIoT)/industrial control system (ICS)	Lesson 12, Topic B
Vulnerabilities related to virtual environments	Lesson 12, Topic C
Virtual machine (VM) escape	
Hypervisor vulnerabilities	
VM repository vulnerabilities	
Vulnerabilities related to containerized workloads	Lesson 12, Topic C

3.6 Given a scenario, perform a social engineering or physical attack	Covered in
Pretext for an approach	Lesson 4, Topic A
Social engineering attacks	Lesson 4, Topic A
Email phishing	
Whaling	
Spear phishing	
Vishing	
Short message service (SMS) phishing	
Universal Serial Bus (USB) drop key	
Watering hole attack	
Physical attacks	Lesson 4, Topic B
Tailgating	
Dumpster diving	
Shoulder surfing	
Badge cloning	
Impersonation	Lesson 4, Topic A
Tools	Lesson 13, Topic D
Browser exploitation framework (BeEF)	
Social engineering toolkit	
Call spoofing tools	Lesson 4, Topic C

3.6 Given a scenario, perform a social engineering or physical attack	Covered in
Methods of influence	Lesson 4, Topic A
Authority	
Scarcity	
Social proof	
Urgency	
Likeness	
Fear	

3.7 Given a scenario, perform post-exploitation techniques	Covered in
Post-exploitation tools	Lesson 14, Topic A
Empire	
Mimikatz	
BloodHound	Lesson 16, Topic B
Lateral movement	Lesson 16, Topic B
Pass the hash	
Network segmentation testing	Lesson 6, Topic B
Privilege escalation	Lesson 13, Topic B
Horizontal	
Vertical	
Upgrading a restrictive shell	Lesson 13, Topic B
Creating a foothold/persistence	Lesson 16, Topic C
Trojan	
Backdoor	
Bind shell	
Reverse shell	
Daemons	
Scheduled tasks	
Detection avoidance	Lesson 8, Topic C
Living-off-the-land techniques/fileless malware	
PsExec	
Windows Management Instrumentation (WMI)	
PowerShell (PS) remoting/Windows Remote Management (WinRM)	
Data exfiltration	
Covering your tracks	Lesson 8, Topic A
Steganography	Lesson 8, Topic B
Establishing a covert channel	Lesson 8, Topic C
Enumeration	Lesson 9, Topic A
Users	
Groups	
Forests	
Sensitive data	Lesson 5, Topic A
Unencrypted files	

4.0 Reporting and Communication	
4.1 Compare and contrast important components of written reports	**Covered in**
Report audience	Lesson 18, Topic A
C-suite	
Third-party stakeholders	
Technical staff	
Developers	
Report contents (not in a particular order)**	Lesson 18, Topic B
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	Lesson 18, Topic C
Secure distribution	Lesson 18, Topic C
Note taking	Lesson 18, Topic A
Ongoing documentation during test	
Screens	
Common themes/root causes	Lesson 18, Topic A
Vulnerabilities	
Observations	
Lack of best practices	

4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report	**Covered in**
Technical controls	Lesson 19, Topic A
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	

4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report	Covered in
Administrative controls	Lesson 19, Topic B
Role-based access control	
Secure software development life cycle	
Minimum password requirements	
Policies and procedures	
Operational controls	Lesson 19, Topic B
Job rotation	
Time-of-day restrictions	
Mandatory vacations	
User training	
Physical controls	Lesson 19, Topic C
Access control vestibule	
Biometric controls	
Video surveillance	

4.3 Explain the importance of communication during the penetration testing process.	Covered in
Communication path	Lesson 17, Topic A
Primary contact	
Technical contact	
Emergency contact	
Communication triggers	Lesson 17, Topic B
Critical findings	
Status reports	
Indicators of prior compromise	
Reasons for communication	Lesson 17, Topic B
Situational awareness	
De-escalation	
Deconfliction	
Identifying false positives	
Criminal activity	
Goal reprioritization	Lesson 17, Topic B
Presentation of findings	Lesson 17, Topic C

4.4 Explain post-report delivery activities	Covered in
Post-engagement cleanup	Lesson 20, Topic A
Removing shells	
Removing tester-created credentials	
Removing tools	
Client acceptance	Lesson 20, Topic B
Lessons learned	Lesson 20, Topic B
Follow-up actions/retest	Lesson 20, Topic B
Attestation of findings	Lesson 20, Topic B
Data destruction process	Lesson 20, Topic A

5.0 Tools and Code Analysis	
5.1 Explain the basic concepts of scripting and software development.	**Covered in**
Logic constructs	Lesson 15, Topic B
Loops	
Conditionals	
Boolean operator	
String operator	
Arithmetic operator	
Data structures	Lesson 15, Topic B
JavaScript Object Notation (JSON)	
Key value	
Arrays	
Dictionaries	
Comma-separated values (CSV)	
Lists	
Trees	
Libraries	Lesson 15, Topic B
Classes	Lesson 15, Topic B
Procedures	Lesson 15, Topic B
Functions	Lesson 15, Topic B

5.2 Given a scenario, analyze a script or code sample for use in a penetration	Covered in
Shells	Lesson 15, Topic A
Bash	
PS	
Programming languages	Lesson 15, Topic A
Python	
Ruby	
Perl	
JavaScript	

5.2 Given a scenario, analyze a script or code sample for use in a penetration	Covered in
Analyze exploit code to:	Lesson 14, Topic C
Download files	
Launch remote access	
Enumerate users	
Enumerate assets	
Opportunities for automation	Lesson 15, Topic C
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	

5.3 Explain use cases of the following tools during the phases of a penetration test	Covered in
Scanners	Lesson 5, Topic C
Nikto	
Open vulnerability assessment scanner (Open VAS)	
SQLmap	
Nessus	Lesson 17, Topic C
Open Security Content Automation Protocol (SCAP)	Lesson 6, Topic A
Wapiti	Lesson 13, Topic D
WPScan	
Brakeman	
Scout Suite	Lesson 9, Topic E
Credential testing tools	Lesson 16, Topic A
Hashcat	
Medusa	
Hydra	
CeWL	
John the Ripper	
Cain	
Mimikatz	Lesson 16, Topic B
Patator	Lesson 16, Topic A
DirBuster	
w3af	

5.3 Explain use cases of the following tools during the phases of a penetration test	**Covered in**
Debuggers	Lesson 14, Topic C
OllyDbg	
Immunity Debugger	
GNU Debugger (GDB)	
WinDbg	
Interactive Disassembler (IDA)	
Covenant	
SearchSploit	Lesson 9, Topic C
OSINT	Lesson 3, Topic A
WHOIS	
Nslookup	
Fingerprinting Organization with Collected Archives (FOCA)	Lesson 3, Topic D
theHarvester	
Shodan	
Maltego	
Recon-ng	
Censys	Lesson 5, Topic C
Wireless	Lesson 10, Topic B
Aircrack-ng suite	
Kismet	
Wifite2	
Rogue access point	Lesson 10, Topic A
EAPHammer	Lesson 10, Topic B
mdk4	
Spooftooph	
Reaver	
Wireless Geographic Logging Engine (WiGLE)	Lesson 6, Topic C
Fern	Lesson 10, Topic B
Web application tools	Lesson 13, Topic D
OWASP ZAP	
Burp Suite	
Gobuster	
Social engineering tools	Lesson 4, Topic C
Social Engineering Toolkit (SET)	
BeEF	Lesson 13, Topic D
Remote access tools	Lesson 14, Topic B
Secure Shell (SSH)	
Ncat	
Netcat	
ProxyChains	Lesson 8, Topic A

5.3 Explain use cases of the following tools during the phases of a penetration test	Covered in
Networking tools	Lesson 6, Topic B
Wireshark	
Hping	Lesson 5, Topic C
Misc.	Lesson 9, Topic C
SearchSploit	
Responder	
Impacket tools	
Empire	Lesson 14, Topic A
Metasploit	Lesson 9, Topic C
mitm6	
CrackMapExec	Lesson 13, Topic D
TruffleHog	
Censys	Lesson 5, Topic C
Steganography tools	Lesson 8, Topic B
Openstego	
Steghide	
Snow	
Coagula	
Sonic Visualiser	
TinEye	Lesson 3, Topic B
Cloud tools	Lesson 9, Topic E
Scout Suite	
CloudBrute	
Pacu	
Cloud Custodian	