Training: CompTIA
CompTIA PenTest+ Prep Course

CompTIA Authorized Partner DELIVERY PARTNER

TRANING TERMS

2025-06-16 | 5 days | Virtual Classroom

TRAINING GOALS:

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and security consulting.

What Skills Will You Learn?

- Engagement Management
  - Includes updated techniques emphasizing scoping and organizational/customer requirements, governance, risk and compliance concepts, reporting, communication, remediation recommendations and demonstrating an ethical hacking mindset
- Attacks and Exploits
  - Includes new techniques to analyze targets, select the best approach, and perform network attacks, wireless attacks, application-based attacks, and cloud attacks. Learn about artificial intelligence (AI) attacks and scripting automation
- Reconnaissance and Enumeration
  - Expanded coverage of information gathering, enumeration, and passive/active reconnaissance, with the goal of conducting inventory. Includes identifying scripts and explaining use cases of various scripting languages (scripting or coding is not required)
- Post-exploitation and Lateral Movement
  - Additional focus on maintaining persistence, lateral movement, staging, exfiltration and post-exploitation, including clean up and restoration activities
- Vulnerability Discovery and Analysis
  - Updated skills that cover vulnerability scanning tools, analysis, management, and physical security weaknesses

PenTest+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program.

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.

Each participant in an authorized training CompTIA PenTest+ Prep Course held in Compendium CE will

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

receive a free PT0-003 CompTIA PenTest+ Certification Exam vouchers.

Who Should Attend

- Penetration Tester
- Cybersecurity Analyst
- Security Consultant
- Cloud Penetration Tester
- Web App Penetration Tester
- Cloud Security Specialist
- Network & Security Specialist

CONSPECT:

- Engagement Management
  - Summarize pre-engagement activities
    - Scope definition
    - Shared responsibility model
    - Legal and ethical considerations
  - 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
  - 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 Worldwide Application Security Project (OWASP) Top 10
    - OWASP Mobile Application Security Verification Standard (MASVS)

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Purdue model
        - Threat modeling frameworks
    - Explain the components of a penetration test report
        - Format alignment
        - Documentation specifications
        - Risk scoring
        - Definitions
        - Report components
        - Test limitations and assumptions
        - Reporting considerations
    - Given a scenario, analyze the findings and recommend the appropriate remediation within a report
        - Technical controls
        - Administrative controls
        - Operational controls
        - Physical controls
- Reconnaissance and Enumeration
    - Given a scenario, apply information gathering techniques
        - Active and passive reconnaissance
        - Open-source intelligence (OSINT)
        - Network reconnaissance
        - Protocol scanning
        - Certificate transparency logs
        - Information disclosure
        - Search engine analysis/enumeration
        - Network sniffing
        - Banner grabbing
        - Hypertext Markup Language (HTML) scraping
    - Given a scenario, apply enumeration techniques
        - Operating system (OS) fingerprinting
        - Service discovery
        - Protocol enumeration
        - DNS enumeration
        - Directory enumeration
        - Host discovery
        - Share enumeration

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Local user enumeration
- Email account enumeration
- Wireless enumeration
- Permission enumeration
- Secrets enumeration
- Attack path mapping
- Web application firewall (WAF) enumeration
- Web crawling
- Manual enumeration

- Given a scenario, modify scripts for reconnaissance and enumeration
  - Information gathering
  - Data manipulation
  - Scripting languages
  - Logic constructs
  - Use of libraries, functions, and classes
- Given a scenario, use the appropriate tools for reconnaissance and enumeration
  - Wayback Machine
  - Maltego
  - Recon-ng
  - Shodan
  - SpiderFoot
  - WHOIS
  - nslookup/dig
  - io
  - io
  - DNSdumpster
  - Amass
  - Nmap
  - theHarvester
  - net
  - InSSIDer
  - com
  - Wireshark/tcpdump
  - Aircrack-ng

- Vulnerability Discovery and Analysis
  - Given a scenario, conduct vulnerability discovery using various techniques

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Types of scans
- Industrial control systems (ICS) vulnerability assessment
- Tools
  - Nikto
  - Greenbone/Open Vulnerability Assessment Scanner (OpenVAS)
  - TruffleHog
  - BloodHound
  - Tenable Nessus
  - PowerSploit
  - Grype
  - Trivy
  - Kube-hunter
- Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases
  - Validate scan, reconnaissance, and enumeration results
  - Public exploit selection
  - Use scripting to validate results
- Explain physical security concepts
  - Tailgating
  - Site surveys
  - Universal Serial Bus (USB) drops
  - Badge cloning
  - Lock picking

- Attacks and Exploits
  - Given a scenario, analyze output to prioritize and prepare attacks
    - Target prioritization
    - Capability selection
  - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Packet crafting
    - Tools
        - Metasploit
        - Netcat
        - Nmap
        - Impacket
        - CrackMapExec (CME)
        - Wireshark/tcpdump
        - msfvenom
        - Responder
        - Hydra
- 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
- Given a scenario, perform host-based attacks using the appropriate tools

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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)

- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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/DirBuster
  - Wfuzz
  - WPScan

- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Docker Bench
- Kube-hunter
- Prowler
- ScoutSuite
- Cloud-native vendor tools

- 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
- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Credential harvesting
- Tools
  - Social Engineering Toolkit (SET)
  - Gophish
  - Evilginx
  - theHarvester
  - Maltego
  - Recon-ng
  - Browser Exploitation Framework (BeEF)
- 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)

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Bluestrike
    - Given a scenario, use scripting to automate attacks
        - PowerShell
        - Bash
        - Python
        - Breach and attack simulation (BAS)
- Post-exploitation and Lateral Movement
    - 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
        - Rootkit
        - Browser extensions
        - Tampering security controls
    - Given a scenario, perform tasks to move laterally throughout the environment
        - Pivoting
        - Relay creation
        - Enumeration
        - Service discovery
        - Window Management Instrumentation (WMI)
        - Window Remote Management (WinRM)
        - Tools
            - LOLBins
            - Covenant
            - CrackMapExec
            - Impacket
            - Netcat
            - sshuttle
            - Proxychains
            - PowerShell ISE

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Batch files
- Metasploit
- PsExec
- Mimikatz

- Summarize concepts related to staging and exfiltration
  - File encryption and compression
  - Covert channel
  - Email
  - Cross-account resources
  - Cloud storage
  - Alternate data streams
  - Text storage sites
  - Virtual drive mounting
- 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

REQUIREMENTS:

Network+, Security+ or equivalent knowledge. 3–4 years in a penetration tester job role.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA PenTest+ certification exam, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA PenTest+ Prep Course held in Compendium CE will receive a free PT0-003 CompTIA PenTest+ Certification Exam vouchers.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

TRAINER:

Authorized CompTIA Trainer.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007