Penetration Testing Professional (CPENT) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Penetration Testing Professional (CPENT) Training Course equips cybersecurity practitioners with advanced offensive security skills required to identify, exploit, and remediate vulnerabilities in modern enterprise networks. This course focuses on real-world penetration testing techniques, including network exploitation, web application testing, cloud penetration testing, Active Directory compromise, wireless attacks, and post-exploitation strategies. Through intensive hands-on practice, learners develop deep technical capabilities aligned with global cybersecurity frameworks and industry-leading penetration testing standards.

As cyber threats become increasingly sophisticated and attack surfaces expand across hybrid environments, organizations require penetration testers who can simulate real-world adversarial tactics and identify systemic weaknesses before attackers exploit them. This course blends scenario-driven labs, red-team methodology, exploit development, and advanced problem-solving exercises to prepare participants for high-level assessment engagements. By the end of the training, learners will be equipped with offensive security skills necessary for enterprise-grade penetration testing and readiness for the CPENT certification exam.

Programme Curriculum

Penetration Testing Professional (CPENT) Training Course

Introduction

Penetration Testing Professional (CPENT) Training Course equips cybersecurity practitioners with advanced offensive security skills required to identify, exploit, and remediate vulnerabilities in modern enterprise networks. This course focuses on real-world penetration testing techniques, including network exploitation, web application testing, cloud penetration testing, Active Directory compromise, wireless attacks, and post-

exploitation strategies. Through intensive hands-on practice, learners develop deep technical capabilities aligned with global cybersecurity frameworks and industry-leading penetration testing standards.

As cyber threats become increasingly sophisticated and attack surfaces expand across hybrid environments, organizations require penetration testers who can simulate real-world adversarial tactics and identify systemic weaknesses before attackers exploit them. This course blends scenario-driven labs, red-team methodology, exploit development, and advanced problem-solving exercises to prepare participants for high-level assessment engagements. By the end of the training, learners will be equipped with offensive security skills necessary for enterprise-grade penetration testing and readiness for the CPENT certification exam.

Course Objectives

1. Understand advanced penetration testing concepts aligned with global cybersecurity standards.
2. Conduct reconnaissance and information gathering using trending offensive security tools.
3. Perform network-based exploitation across internal and external infrastructures.
4. Execute vulnerability assessments and map exploitable system weaknesses.
5. Conduct secure and ethical exploitation of web applications and APIs.
6. Perform privilege escalation and post-exploitation tasks in Windows and Linux systems.
7. Compromise Active Directory environments using trending attack techniques.
8. Assess security of cloud infrastructures and virtualized environments.
9. Execute wireless network attacks and identify misconfigurations.
10. Develop and customize exploits for advanced penetration testing.
11. Simulate red-team operations and adversarial attack paths.
12. Document penetration testing findings and prepare high-value reporting.
13. Strengthen organizational security posture through actionable remediation recommendations.

Organizational Benefits

- Strengthened cybersecurity resilience through proactive vulnerability identification
- Enhanced ability to detect and mitigate advanced cyber threats
- Improved security of cloud, network, and web application environments
- Reduced risk of ransomware attacks and unauthorized system access
- Increased compliance with cybersecurity frameworks and regulatory standards
- Stronger incident response preparedness
- Enhanced internal capacity to assess technology risks
- Improved system hardening and security architecture decisions
- Reduced dependence on external penetration testing services
- Increased trust and confidence from clients, partners, and stakeholders

Target Audiences

- Cybersecurity analysts and penetration testers
- IT security administrators and network engineers
- Red team and blue team security professionals
- Ethical hackers preparing for CPENT certification
- Cybersecurity managers and security architects
- Incident response and digital forensics teams
- Technical auditors and compliance officers
- Cloud and system infrastructure engineers

Course Duration: 5 days

Course Modules

Module 1: Advanced Penetration Testing Foundations

- Understand penetration testing standards and methodologies
- Examine rules of engagement and ethical testing practices
- Analyze scope definition and documentation requirements
- Review OSINT tools and information-gathering frameworks
- Develop structured penetration testing workflows
- Case Study: Misconfigured server exploited during initial recon

Module 2: Network Penetration & Exploitation Techniques

- Conduct network scanning and enumeration
- Exploit network service vulnerabilities
- Identify insecure protocols and network misconfigurations
- Penetrate internal and external network infrastructures
- Perform advanced pivoting across network segments
- Case Study: Network compromise through weak SMB configuration

Module 3: Web Application & API Penetration Testing

- Assess authentication, authorization, and session weaknesses
- Exploit common vulnerabilities such as SQL injection and XSS
- Test API endpoints and server-side flaws
- Identify insecure code and logic vulnerabilities
- Evaluate security controls for web services
- Case Study: Web application breach caused by faulty API validation

Module 4: System Exploitation & Privilege Escalation

- Exploit Windows and Linux system vulnerabilities
- Identify privilege escalation paths and misconfigurations
- Execute credential harvesting and password attacks
- Perform process injection and persistence techniques
- Utilize exploitation frameworks for post-compromise actions
- Case Study: Privilege escalation via misconfigured sudo permissions

Module 5: Active Directory Penetration Testing

- Map AD structures and privilege relationships
- Conduct Kerberoasting, Pass-the-Hash, and LDAP attacks
- Identify weak group policies and domain vulnerabilities
- Exploit misconfigured authentication mechanisms
- Compromise domain controllers and escalate privileges
- Case Study: Full domain takeover using credential replay attacks

Module 6: Cloud & Virtualization Penetration Testing

- Assess cloud service vulnerabilities and data exposure risks
- Evaluate virtualization platforms and containerized environments
- Identify insecure storage, APIs, and IAM configurations

- Perform exploitation in hybrid cloud architectures
- Test isolation boundaries in virtual machines and containers
- Case Study: Cloud breach due to improperly configured IAM policies

Module 7: Wireless Network Attacks

- Identify wireless security weaknesses and attack vectors
- Conduct wireless reconnaissance and packet captures
- Exploit WPA/WPA2 vulnerabilities and rogue AP setups
- Perform MITM attacks in wireless environments
- Evaluate wireless segmentation and access controls
- Case Study: Corporate network intrusion via unsecured guest Wi-Fi

Module 8: Reporting, Documentation & Remediation Planning

- Document exploitation paths and technical findings
- Develop detailed remediation recommendations
- Prepare executive and technical assessment reports
- Communicate risks to management and technical teams
- Build structured post-testing improvement plans
- Case Study: Security improvements implemented after penetration test report

Training Methodology

- Instructor-led technical demonstrations and guided practice
- Hands-on penetration testing labs in simulated enterprise environments
- Group analysis of offensive security case studies
- Practical exploitation exercises with real-world tools
- Step-by-step walkthroughs of advanced attack scenarios
- Structured assignments for developing penetration testing reports

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com