Network and Infrastructure Penetration Testing Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's hyper-connected digital landscape, robust Cyber Resilience is non-negotiable. Organizations face an escalating barrage of sophisticated threats targeting core network and cloud infrastructure. Network and Infrastructure Penetration Testing Training Course is designed to bridge the critical Cybersecurity Skills Gap, transforming IT professionals into elite Ethical Hackers capable of simulating real-world attacks. By mastering the principles of Red Teaming and leveraging cutting-edge tools, participants will learn to proactively discover and exploit vulnerabilities including complex Cloud Security flaws, misconfigurations in Active Directory, and emerging IoT Security risks before malicious actors can leverage them. The course emphasizes a Defense-in-Depth mindset, ensuring graduates can not only perform thorough penetration tests but also provide actionable, risk-prioritized remediation strategies to enhance the organization's Security Posture and achieve critical Compliance standards.

This intensive, hands-on program moves beyond theoretical knowledge, focusing on a practical Kill Chain methodology to conduct comprehensive Infrastructure Security Audits. We delve into the latest AI-driven Pentesting techniques, advanced Pivoting and Post-Exploitation tactics, and the security of modern environments like DevSecOps pipelines and Zero Trust Architecture. Utilizing a state-of-the-art Cyber Range environment, every module is reinforced with Case Studies and Capture The Flag (CTF) exercises, enabling participants to develop the muscle memory required for effective Vulnerability Management and Incident Response. Graduates will emerge as highly proficient security experts, ready to lead Threat Modeling and execute high-value Penetration Testing Engagements in any enterprise or cloud environment.

Programme Curriculum

Network and Infrastructure Penetration Testing Training Course

Introduction

In today's hyper-connected digital landscape, robust Cyber Resilience is non-negotiable. Organizations face an escalating barrage of sophisticated threats targeting core network and cloud infrastructure. Network and Infrastructure Penetration Testing Training Course is designed to bridge the critical Cybersecurity Skills Gap, transforming IT professionals into elite Ethical Hackers capable of simulating real-world attacks. By mastering the principles of Red Teaming and leveraging cutting-edge tools, participants will learn to proactively discover and exploit vulnerabilities including complex Cloud Security flaws, misconfigurations in Active Directory, and emerging IoT Security risks before malicious actors can leverage them. The course emphasizes a Defense-in-Depth mindset, ensuring graduates can not only perform thorough penetration tests but also provide actionable, risk-prioritized remediation strategies to enhance the organization's Security Posture and achieve critical Compliance standards.

This intensive, hands-on program moves beyond theoretical knowledge, focusing on a practical Kill Chain methodology to conduct comprehensive Infrastructure Security Audits. We delve into the latest AI-driven Pentesting techniques, advanced Pivoting and Post-Exploitation tactics, and the security of modern environments like DevSecOps pipelines and Zero Trust Architecture. Utilizing a state-of-the-art Cyber Range environment, every module is reinforced with Case Studies and Capture The Flag (CTF) exercises, enabling participants to develop the muscle memory required for effective Vulnerability Management and Incident Response. Graduates will emerge as highly proficient security experts, ready to lead Threat Modeling and execute high-value Penetration Testing Engagements in any enterprise or cloud environment.

Course Duration

10 days

Course Objectives

1. Master the Penetration Testing Kill Chain from reconnaissance to final reporting.
2. Perform advanced Open-Source Intelligence and Active Reconnaissance on network and cloud targets.
3. Identify, enumerate, and exploit common network service vulnerabilities using tools like Metasploit and Nmap Scripting Engine (NSE).
4. Conduct comprehensive security assessments of modern Cloud Infrastructure
5. Exploit and remediate weaknesses in Active Directory (AD), including common attack paths like Kerberoasting and Pass-the-Hash.
6. Execute advanced techniques such as Pivoting, Lateral Movement, and Privilege Escalation within complex networks.
7. Analyze and bypass modern defensive controls, including Firewalls, IDS/IPS, and Endpoint Detection and Response (EDR) solutions.
8. Perform thorough Wireless Network Penetration Testing and exploit IoT/OT device vulnerabilities.
9. Develop custom exploits and scripts to automate and enhance testing, focusing on Binary Exploitation fundamentals.
10. Integrate Threat Intelligence and the MITRE ATT&CK Framework into testing and reporting.
11. Effectively communicate Risk Assessment findings and craft professional, actionable Penetration Test Reports.
12. Adhere to Ethical Hacking principles, scoping, and regulatory Compliance
13. Apply AI-Driven Security Testing tools and methodologies for enhanced efficiency and coverage.

Target Audience

1. Aspiring Penetration Testers / Ethical Hackers

2. Security Analysts / Security Consultants
3. Network Engineers / System Administrators
4. Security Architects / DevSecOps Engineers
5. IT Auditors seeking technical skill validation
6. Vulnerability Management Specialists
7. Incident Response Team Members
8. Anyone pursuing advanced Offensive Security certifications.

Course Modules

Module 1: Ethical Hacking and Reconnaissance Foundation

- Ethical Hacking Principles and Legal Frameworks.
- Deep OSINT Techniques
- Active Network Reconnaissance
- Footprinting Tools Mastery
- Case Study: The pre-engagement reconnaissance that led to the SolarWinds supply chain attack.

Module 2: Network Service Exploitation

- Exploiting Common Services
- Advanced Metasploit Framework and Meterpreter Usage.
- Buffer Overflow Fundamentals and Simple Binary Exploitation.
- Client-Side Attack Vectors
- Case Study: Exploitation of an outdated Apache Struts vulnerability to gain initial access.

Module 3: Advanced Windows and Active Directory Attacks

- Understanding Active Directory Structure and Enumeration.
- Credential Harvesting and Password Attacks
- Kerberoasting and AS-REP Roasting Attacks.
- Advanced Lateral Movement and Persistence Techniques
- Case Study: Analyzing a successful Domain Controller Compromise via a Pass-the-Hash attack from a single exploited workstation.

Module 4: Linux Post-Exploitation and Privilege Escalation

- Linux Enumeration Techniques
- Common Privilege Escalation vectors
- File System and System Configuration Weaknesses.
- Maintaining Persistence on Linux Targets.
- Case Study: A vulnerability in a network management tool allowed a low-privilege account to exploit a misconfiguration, achieving root access.

Module 5: Network Segmentation and Pivoting

- Identifying and Mapping Network Segmentation Flaws.
- Techniques for Pivoting using tools like SSH, Proxychains, and Metasploit.
- Double Pivoting for accessing deeply segmented networks.
- Tunneling and Evasion of Network Monitoring.
- Case Study: A tester used a compromised finance server to pivot into the highly protected HR network, bypassing the firewall rules, a scenario often missed in basic audits.

Module 6: Wireless and IoT/OT Security Testing

- Cracking WPA/WPA2/WPA3 with modern tools
- Attacks on Captive Portals and Rogue Access Points.
- Identifying and Attacking Common IoT Protocols and Misconfigurations.
- Introduction to OT/ICS Security Testing Principles
- Case Study: Exploiting weak credentials on an internal Smart Thermostat to gain a foothold in the corporate wireless network.

Module 7: Cloud Infrastructure Penetration Testing

- Cloud Architecture Security Fundamentals
- Attacking AWS and Azure
- Serverless and Container Security Testing
- Cloud-Specific API Security and Misconfiguration Exploitation.
- Case Study: The compromise of a major cloud service via an overly permissive IAM Role attached to a public-facing compute instance.

Module 8: Evasion and Defense Bypassing

- Bypassing Firewalls and Network Access Controls.
- Evading Signature-Based IDS/IPS.
- Advanced techniques to defeat Anti-Virus and EDR solutions.
- Network Traffic Obfuscation and Encoding.
- Case Study: A Red Team successfully used DNS tunneling to exfiltrate data undetected, bypassing the network?ÇÖs standard egress filters.

Module 9: Web Application & API Security Essentials

- OWASP Top 10 Review
- Testing for SQL Injection and Cross-Site Scripting.
- Exploiting Authentication and Authorization Flaws in APIs.
- Using Burp Suite for manual and automated application analysis.
- Case Study: Exploitation of a flawed API endpoint with broken object level authorization to access another user's sensitive records.

Module 10: Vulnerability Management and Reporting

- Automated and Manual Vulnerability Scanning
- Risk Ranking and Prioritization
- Structuring a Professional Penetration Test Report.
- Creating Clear, Actionable Remediation Strategies.
- Case Study: Review of a regulatory compliance-driven test where low-CVSS-score misconfigurations presented a high business risk, necessitating an adjusted remediation priority.

Module 11: Introduction to DevSecOps and CI/CD Pipeline Security

- Understanding the DevSecOps Mindset.
- Security Testing in the CI/CD Pipeline
- Code and Infrastructure-as-Code Scanning.
- Securing Git Repositories and Secrets Management.

- Case Study: An attacker compromised a CI/CD build server due to hardcoded credentials, leading to the injection of malicious code into a deployment package

Module 12: Zero Trust and Micro-Segmentation Auditing

- Principles of Zero Trust Architecture
- Auditing Identity and Access Management Controls.
- Verifying Micro-Segmentation Effectiveness.
- Testing for Weaknesses in ZTA Components
- Case Study: A tester demonstrated that a poorly configured Zero Trust policy still allowed lateral movement between two critical application segments after initial compromise.

Module 13: Advanced Social Engineering and Physical Security

- Phishing, Vishing, and Smishing Techniques for Credential Theft.
- Physical Security Weaknesses and Assessment.
- Bypassing Human Controls to Gain Network Access.
- Developing and Running a Controlled Social Engineering Campaign.
- Case Study: A targeted spear-phishing attack on a System Admin resulted in the theft of VPN credentials, providing a direct initial foothold into the internal network.

Module 14: Practical Capture The Flag Capstone

- An end-to-end, multi-stage CTF challenge in a simulated corporate environment.
- Requires applying all knowledge from the course modules.
- Focus on Double Pivoting and Red Teaming collaboration.
- Timed scenario to emulate real-world pressure.
- Case Study: Post-mortem analysis of a complex CTF environment focusing on the most sophisticated exploitation path identified by the top-performing teams.

Module 15: AI in Penetration Testing and Future Trends

- The role of AI/ML in both attack and defense.
- Tools and techniques for AI-Assisted Reconnaissance and Exploit Generation.
- Security concerns for emerging technologies
- The future of Vulnerability Research and Bug Bounty Programs.
- Case Study: Discussing the ethical implications and potential misuse of AI-driven fuzzing tools in a large-scale network assessment.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 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