Training Course on Ethical Hacking and Penetration Testing for Digital Forensics and Incident Response Readiness

Professional Development Training Course Outline

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

Course Introduction

In today's interconnected world, **cybersecurity threats** are escalating in sophistication and frequency, making robust **digital defense** paramount for all organizations. Training Course on Ethical Hacking and Penetration Testing for Digital Forensics and Incident Response Readiness is meticulously designed to equip cybersecurity professionals with the advanced offensive and defensive skills necessary to proactively identify, exploit, and mitigate vulnerabilities, thereby significantly enhancing an organization's **Incident Response Readiness**. Participants will gain hands-on expertise in simulating real-world cyberattacks, understanding the **attacker's mindset**, and applying **forensic techniques** to effectively investigate and contain security incidents, safeguarding critical assets and maintaining **business continuity**.

The convergence of **ethical hacking methodologies** with **digital forensics** and **incident response (DFIR)** is crucial for building resilient security postures. This program goes beyond theoretical knowledge, immersing participants in practical scenarios using **industry-standard tools** and **cutting-edge techniques**. By mastering both offensive and defensive strategies, professionals will be empowered to conduct comprehensive **vulnerability assessments**, perform effective **penetration tests**, and swiftly execute **incident handling procedures**, transforming them into invaluable assets in the ongoing battle against **cybercrime** and ensuring organizational **cyber resilience**.

Programme Curriculum

Training Course on Ethical Hacking and Penetration Testing for Digital Forensics and Incident Response Readiness

Introduction

In today's interconnected world, **cybersecurity threats** are escalating in sophistication and frequency, making robust **digital defense** paramount for all organizations. Training Course on Ethical Hacking and Penetration Testing for Digital Forensics and Incident Response Readiness is meticulously designed to equip cybersecurity professionals with the advanced offensive and defensive skills necessary to proactively identify, exploit, and mitigate vulnerabilities, thereby significantly enhancing an organization's **Incident Response Readiness**. Participants will gain hands-on expertise in simulating real-world cyberattacks, understanding the **attacker's mindset**, and applying **forensic techniques** to effectively investigate and contain security incidents, safeguarding critical assets and maintaining **business continuity**.

The convergence of **ethical hacking methodologies** with **digital forensics** and **incident response (DFIR)** is crucial for building resilient security postures. This program goes beyond theoretical knowledge, immersing participants in practical scenarios using **industry-standard tools** and **cutting-edge techniques**. By mastering both offensive and defensive strategies, professionals will be empowered to conduct comprehensive **vulnerability assessments**, perform effective **penetration tests**, and swiftly execute **incident handling procedures**, transforming them into invaluable assets in the ongoing battle against **cybercrime** and ensuring organizational **cyber resilience**.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Master Advanced Penetration Testing techniques for network, web, and cloud environments.
2. Conduct comprehensive Vulnerability Assessments and exploit identified weaknesses ethically.
3. Implement Red Teaming and Blue Teaming strategies for holistic security posture improvement.
4. Perform Digital Forensics Investigations to gather and analyze evidence from compromised systems.
5. Develop effective Incident Response Plans and execute them swiftly during cyber crises.
6. Understand and mitigate Zero-Day Exploits and Advanced Persistent Threats (APTs).
7. Utilize Open-Source Intelligence (OSINT) for enhanced reconnaissance and threat intelligence.
8. Apply Malware Analysis techniques for effective detection, reverse engineering, and mitigation.
9. Secure Cloud Computing Environments (AWS, Azure, GCP) against emerging threats.
10. Implement robust Network Security and Endpoint Detection and Response (EDR) solutions.
11. Conduct Mobile Device Forensics and IoT Security assessments.
12. Leverage AI and Machine Learning in cybersecurity for predictive threat analysis.
13. Adhere to Cybersecurity Compliance and Legal Frameworks in forensic investigations.

Organizational Benefits

- Proactive Cyber Defense: Shifting from reactive to proactive security, preventing breaches before they occur.
- Reduced Financial Losses: Minimizing the monetary impact of cyberattacks through effective prevention and rapid response.

- Enhanced Data Protection: Safeguarding sensitive data and intellectual property from exfiltration and compromise.
- Improved Compliance and Governance: Meeting regulatory requirements and demonstrating due diligence in cybersecurity.
- Strengthened Brand Reputation: Building trust with customers and stakeholders by demonstrating a commitment to security.
- Faster Incident Recovery: Decreasing downtime and accelerating recovery times post-incident.
- Skilled Cybersecurity Workforce: Developing an in-house team capable of handling complex cyber threats and incidents.
- Optimized Security Investments: Making informed decisions on security tools and technologies based on real-world testing.

Target Participants

This course is ideal for:

1. Cybersecurity Analysts
2. Incident Responders
3. Digital Forensic Investigators
4. Security Engineers
5. Network Administrators
6. System Administrators
7. IT Auditors
8. Security Consultants

Course Modules

Module 1: Introduction to Ethical Hacking and Cybersecurity Fundamentals

- Overview of the cyber threat landscape and common attack vectors.
- Defining ethical hacking, penetration testing, and their legal frameworks.
- Understanding the Cyber Kill Chain and MITRE ATT&CK Framework.
- Setting up a secure ethical hacking lab environment.
- **Case Study:** Analyzing the phases of a recent high-profile ransomware attack (e.g., Colonial Pipeline) and discussing initial breach vectors.

Module 2: Reconnaissance and Footprinting

- Passive and active reconnaissance techniques (OSINT, Shodan, Maltego).
- Gathering information about targets: domains, IP ranges, employees, technologies.
- Website analysis and publicly available information gathering.
- Advanced Google Hacking (Google Dorking) for sensitive data exposure.
- **Case Study:** Investigating a company's exposed information through OSINT, leading to potential attack vectors.

Module 3: Scanning Networks and Enumeration

- Network scanning tools and techniques (Nmap, Nessus).
- Port scanning, service version detection, and operating system fingerprinting.
- Enumerating users, shares, and services (SMB, SNMP, LDAP, DNS).
- Vulnerability scanning and mapping with automated tools.

- **Case Study:** Performing an authenticated vulnerability scan on a simulated corporate network and prioritizing discovered vulnerabilities.

Module 4: Vulnerability Analysis and Exploitation Fundamentals

- Understanding common vulnerabilities (OWASP Top 10, CVEs).
- Introduction to exploit frameworks (Metasploit, Exploit-DB).
- Techniques for gaining initial access: password attacks, exploiting known vulnerabilities.
- Buffer overflows and basic exploit development concepts.
- **Case Study:** Exploiting a vulnerable web application (e.g., using SQL Injection or XSS) to gain unauthorized access.

Module 5: System Hacking and Post-Exploitation

- Privilege escalation techniques on Windows and Linux systems.
- Maintaining persistence: backdoors, rootkits, scheduled tasks.
- Data exfiltration methods and countermeasures.
- Covering tracks and clearing logs.
- **Case Study:** Demonstrating lateral movement within a compromised network and establishing persistent access.

Module 6: Web Application Penetration Testing

- Understanding web application architecture and common vulnerabilities.
- Hands-on with Burp Suite for proxying, scanning, and exploitation.
- SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).
- Broken authentication, access control, and insecure deserialization.
- **Case Study:** Conducting a full penetration test on a deliberately vulnerable web application, documenting findings, and suggesting remediation.

Module 7: Wireless Network Hacking

- Wireless network fundamentals (Wi-Fi standards, encryption).
- WPA/WPA2 cracking techniques (aircrack-ng, Hashcat).
- Rogue access point attacks and Wi-Fi phishing.
- Denial-of-Service attacks on wireless networks.
- **Case Study:** Simulating a Wi-Fi phishing attack and demonstrating how easily credentials can be captured.

Module 8: Digital Forensics Fundamentals

- Introduction to digital forensics: principles, legal aspects, and ethics.
- The Digital Forensics Incident Response (DFIR) lifecycle.
- Evidence acquisition: disk imaging, memory acquisition.
- Chain of custody and proper evidence handling.
- **Case Study:** Initiating a digital forensics investigation on a simulated infected workstation, preserving volatile data.

Module 9: Host Forensics and Artifact Analysis

- Analyzing Windows artifacts: Registry, Event Logs, Prefetch files.
- Linux forensics: log files, command history, filesystem analysis.
- Memory forensics with Volatility Framework.
- Timeline analysis and correlating events.

- **Case Study:** Using memory forensics to identify malicious processes and network connections on a compromised system.

Module 10: Network Forensics and Traffic Analysis

- Packet analysis with Wireshark and network monitoring tools.
- Identifying suspicious network traffic patterns and anomalies.
- Detecting malware C2 communication and data exfiltration.
- Intrusion Detection/Prevention Systems (IDS/IPS) and SIEM logs analysis.
- **Case Study:** Analyzing captured network traffic (PCAP) to reconstruct an attack sequence and identify compromised hosts.

Module 11: Malware Analysis and Reverse Engineering

- Types of malware: viruses, worms, Trojans, ransomware, rootkits.
- Static and dynamic malware analysis techniques.
- Introduction to reverse engineering tools (IDA Pro, Ghidra, x64dbg).
- Understanding malware persistence mechanisms and anti-forensic techniques.
- **Case Study:** Performing basic static and dynamic analysis on a suspicious executable to determine its functionality and indicators of compromise (IOCs).

Module 12: Incident Response Planning and Execution

- Developing an Incident Response Plan (IRP) from scratch.
- Roles and responsibilities in an incident response team.
- Containment, eradication, and recovery strategies.
- Communication and reporting during an incident.
- **Case Study:** Leading a simulated incident response exercise, from detection to post-incident review.

Module 13: Threat Intelligence and Advanced Persistent Threats (APTs)

- Sources and types of threat intelligence.
- Integrating threat intelligence into security operations.
- Understanding the lifecycle and characteristics of APTs.
- Defending against sophisticated, targeted attacks.
- **Case Study:** Using threat intelligence feeds to identify and analyze a simulated APT campaign targeting a specific industry.

Module 14: Cloud Security and Container Security

- Cloud security models (IaaS, PaaS, SaaS) and shared responsibility.
- Penetration testing cloud environments (AWS, Azure, GCP).
- Container security (Docker, Kubernetes) vulnerabilities and best practices.
- Cloud incident response considerations.
- **Case Study:** Identifying misconfigurations in a simulated AWS S3 bucket leading to data exposure and recommending remediation.

Module 15: Legal, Ethical, and Reporting Aspects of DFIR

- Legal considerations in ethical hacking and digital forensics.
- Ethical guidelines and professional conduct.
- Creating professional penetration test and incident response reports.
- Presenting findings to technical and non-technical audiences.

- **Case Study:** Reviewing a mock penetration test report and discussing effective communication of vulnerabilities and risks to management.

Training Methodology

- Hands-on Labs and Practical Exercises
- Instructor-Led Demonstrations.
- Real-World Case Studies
- Interactive Discussions and Q&A Sessions
- Capstone Project/Simulation
- Self-Paced Learning Resources.

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

23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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