Ethics in Cybersecurity and Hacking Training Course

Professional Development Training Course Outline

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

Course Introduction

Ethics in Cybersecurity and Hacking Training Course provides a comprehensive and cutting-edge curriculum in Ethics in Cybersecurity and Hacking Training. In today's hyper-connected and AI-driven world, the digital landscape is fraught with sophisticated cyber threats like Ransomware-as-a-Service and complex supply chain attacks. Organizations face an urgent, global demand for highly skilled ethical hackers and penetration testers who possess both technical mastery of offensive security techniques and an unwavering ethical compass. This program moves beyond mere tool usage, establishing a strong foundation in cyber ethics, legal compliance, and the profound responsibility accompanying privileged access to sensitive systems. Participants will master the methodologies of white-hat hacking from reconnaissance to post-exploitation while strictly adhering to professional conduct and disclosure protocols. Graduates will be prepared to not only identify and remediate critical zero-day vulnerabilities but also to champion a culture of proactive security within their organizations, ensuring adherence to the core principles of Confidentiality, Integrity, and Availability.

Our structured, hands-on course is specifically designed to bridge the skill gap between theoretical knowledge and real-world cyber defense practices, emphasizing the critical interplay between technical ability and ethical decision-making. We leverage a dynamic Cyber Range environment for scenario-based practice labs to simulate real-time threat scenarios, including advanced cloud security misconfigurations and IoT device vulnerabilities. The curriculum integrates current MITRE ATT&CK Framework tactics and techniques, preparing participants for advanced roles like Red Team Engineers and Threat Hunters. By focusing heavily on the legal and regulatory frameworks governing digital security, we empower students to conduct authorized penetration testing and vulnerability assessments responsibly. This unique dual-focus approach marrying offensive security with a rigorous code of conduct produces cybersecurity professionals who are highly sought after by global enterprises to safeguard critical infrastructure and intellectual property against the next generation of AI-powered cyberattacks.

Programme Curriculum

Ethics in Cybersecurity and Hacking Training Course

Introduction

Ethics in Cybersecurity and Hacking Training Course provides a comprehensive and cutting-edge curriculum in Ethics in Cybersecurity and Hacking Training. In today's hyper-connected and AI-driven world, the digital landscape is fraught with sophisticated cyber threats like Ransomware-as-a-Service and complex supply chain attacks. Organizations face an urgent, global demand for highly skilled ethical hackers and penetration testers who possess both technical mastery of offensive security techniques and an unwavering ethical compass. This program moves beyond mere tool usage, establishing a strong foundation in cyber ethics, legal compliance, and the profound responsibility accompanying privileged access to sensitive systems. Participants will master the methodologies of white-hat hacking from reconnaissance to post-exploitation while strictly adhering to professional conduct and disclosure protocols. Graduates will be prepared to not only identify and remediate critical zero-day vulnerabilities but also to champion a culture of proactive security within their organizations, ensuring adherence to the core principles of Confidentiality, Integrity, and Availability.

Our structured, hands-on course is specifically designed to bridge the skill gap between theoretical knowledge and real-world cyber defense practices, emphasizing the critical interplay between technical ability and ethical decision-making. We leverage a dynamic Cyber Range environment for scenario-based practice labs to simulate real-time threat scenarios, including advanced cloud security misconfigurations and IoT device vulnerabilities. The curriculum integrates current MITRE ATT&CK Framework tactics and techniques, preparing participants for advanced roles like Red Team Engineers and Threat Hunters. By focusing heavily on the legal and regulatory frameworks governing digital security, we empower students to conduct authorized penetration testing and vulnerability assessments responsibly. This unique dual-focus approach marrying offensive security with a rigorous code of conduct produces cybersecurity professionals who are highly sought after by global enterprises to safeguard critical infrastructure and intellectual property against the next generation of AI-powered cyberattacks.

Course Duration

5 days

Course Objectives

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

1. Master the Five Phases of Ethical Hacking methodology for comprehensive security assessments.
2. Implement robust Open-Source Intelligence and advanced reconnaissance techniques ethically and legally.
3. Execute professional-grade vulnerability analysis and penetration testing using industry-standard tools like Nmap and Metasploit.
4. Understand and apply key cyber ethics principles, professional codes of conduct, and responsible vulnerability disclosure.
5. Identify and mitigate common web application vulnerabilities, specifically the OWASP Top 10, including SQL Injection and XSS.
6. Analyze and defend against sophisticated malware, ransomware-as-a-service, and Advanced Persistent Threats.
7. Secure cloud environments by addressing common misconfigurations in platforms like AWS and Azure.
8. Apply regulatory compliance frameworks, including GDPR and CCPA, to ethical hacking engagements.

9. Develop defensive strategies based on the MITRE ATT&CK Framework for effective Threat Hunting and incident response.
10. Perform secure system hardening and privilege escalation countermeasures on Windows and Linux platforms.
11. Conduct Social Engineering assessments to test human defenses and design effective security awareness training.
12. Execute wireless network security and IoT device penetration tests to discover critical weaknesses.
13. Author clear, actionable penetration testing reports with prioritized remediation strategies and risk scorecards.

Target Audience

1. Aspiring Ethical Hackers / Penetration Testers
2. Information Security Analysts and Consultants
3. IT/Network Administrators seeking defensive skills
4. Security Engineers and Architects
5. Compliance and Audit Professionals
6. Software Developers focused on security
7. Threat Hunters and Incident Responders
8. Chief Information Security Officers and Security Managers

Course Modules

Module 1: Cyber Ethics, Law, and Core Concepts

- The CIA Triad and the role of the ethical hacker.
- Legal and Regulatory Frameworks governing penetration testing and data privacy.
- The Ethical Hacking Code of Conduct and responsible vulnerability disclosure policy.
- Case Study: Analyzing the legal fallout when a tester ignores the Scope of Work
- Understanding different types of hackers.

Module 2: Footprinting, Reconnaissance, and Scanning

- Techniques for Passive Reconnaissance using OSINT tools
- Active Reconnaissance methods.
- Advanced DNS and Network Enumeration techniques.
- Case Study: Using public records and social media to map out a target's infrastructure and personnel.
- Evading Intrusion Detection Systems and firewalls during the scanning phase.

Module 3: System Hacking and Malware Threats

- Vulnerability Analysis using scanners and manual techniques.
- Password Cracking techniques and defensive countermeasures.
- Privilege Escalation methods and maintaining persistent access.
- Case Study: Analyzing the ethical impact of Ransomware-as-a-Service and global malware spread.
- Understanding the lifecycle of Malware, Trojans, and Viruses, and basic Malware Analysis.

Module 4: Network and Wireless Security Hacking

- Sniffing and Man-in-the-Middle attacks using Wireshark and ARP Poisoning.
- Hacking Wireless Networks and implementing robust security controls.
- Denial of Service attacks and mitigation techniques.

- Case Study: Examining a massive IoT device powered DDoS attack and the defense strategies.
- Securing TCP/IP Protocols and exploiting common network service vulnerabilities.

Module 5: Web Application and Cloud Security

- Exploiting the OWASP Top 10 vulnerabilities.
- Using Burp Suite for intercepting, analyzing, and modifying web traffic.
- Identifying and exploiting common Cloud Security misconfigurations.
- Case Study: Analyzing a major breach due to a misconfigured cloud firewall and its ethical implications for data trust.
- Secure Coding Principles and effective input validation and output encoding.

Module 6: Social Engineering and Human Factors

- The psychology of Social Engineering and its role in the Cyber Kill Chain.
- Simulating and defending against Phishing, Spear Phishing, and Vishing attacks.
- Techniques for physical security penetration and Dumpster Diving.
- Case Study: A targeted Spear Phishing attack leading to a major security token compromise.
- Designing and implementing effective Security Awareness Training programs to reduce human error.

Module 7: Reporting, Mitigation, and Defence Strategy

- The Penetration Testing Phases
- Creating a professional Penetration Test Report with clear, actionable remediation plans.
- Applying the MITRE ATT&CK Framework to map attacker tactics and techniques to defensive controls.
- Case Study: How defense teams used threat intelligence and frameworks to detect and respond to a complex APT.
- Introduction to Red Team and Blue Team operations and the concept of Purple Teaming.

Module 8: Advanced Ethical Horizons

- Introduction to IoT and Operational Technology security testing and unique ethical challenges.
- Exploring the ethical considerations of AI and Machine Learning in both offensive and defensive security.
- Fundamentals of Digital Forensics and Incident Response post-exploitation.
- Case Study: Analyzing the fine line between white-hat research and unauthorized access in a live program.
- Future trends in Cybersecurity, including Quantum Computing threats and Zero Trust architectures.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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