Certified Ethical Hacker 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

The digital landscape is rapidly evolving, leading to an unprecedented surge in sophisticated cyber threats and zero-day vulnerabilities. Modern enterprises, relying heavily on Cloud Computing, IoT/OT ecosystems, and complex network infrastructures, require a proactive and offensive defense strategy. Certified Ethical Hacker Training Course provides a comprehensive, hands-on methodology in adversarial simulation and penetration testing, positioning participants as vital assets in the global fight against cybercrime. Professionals who complete this program will master the five phases of ethical hacking reconnaissance, scanning, gaining access, maintaining access, and covering tracks using the same advanced tools and techniques employed by black-hat hackers, but within a legal and ethical framework. The course emphasizes AI-enhanced defense, threat intelligence, and vulnerability remediation to ensure a robust security posture in the face of next-generation attacks.

This immersive, lab-intensive training is crucial for transitioning from a defensive mindset to an offensive one, enabling security teams to identify, validate, and strategically mitigate critical weaknesses across the entire organizational attack surface. Participants will gain real-world experience through simulated attacks on live targets in a safe, controlled environment, solidifying their expertise in areas like Web Application Hacking, Wireless Network Security, and Mobile Platform Exploitation. The CEH certification is a globally recognized, vendor-neutral credential that validates the holder's mastery of the essential ethical hacking skills required for roles ranging from Penetration Tester to Security Analyst, making it a cornerstone for a successful career in offensive security.

Programme Curriculum

Certified Ethical Hacker Training Course

Introduction

The digital landscape is rapidly evolving, leading to an unprecedented surge in sophisticated cyber threats and zero-day vulnerabilities. Modern enterprises, relying heavily on Cloud Computing, IoT/OT ecosystems, and complex network infrastructures, require a proactive and offensive defense strategy. Certified Ethical Hacker Training Course provides a comprehensive, hands-on methodology in adversarial simulation and penetration testing, positioning participants as vital assets in the global fight against cybercrime. Professionals who complete this program will master the five phases of ethical hacking reconnaissance, scanning, gaining access, maintaining access, and covering tracks using the same advanced tools and techniques employed by black-hat hackers, but within a legal and ethical framework. The course emphasizes AI-enhanced defense, threat intelligence, and vulnerability remediation to ensure a robust security posture in the face of next-generation attacks.

This immersive, lab-intensive training is crucial for transitioning from a defensive mindset to an offensive one, enabling security teams to identify, validate, and strategically mitigate critical weaknesses across the entire organizational attack surface. Participants will gain real-world experience through simulated attacks on live targets in a safe, controlled environment, solidifying their expertise in areas like Web Application Hacking, Wireless Network Security, and Mobile Platform Exploitation. The CEH certification is a globally recognized, vendor-neutral credential that validates the holder's mastery of the essential ethical hacking skills required for roles ranging from Penetration Tester to Security Analyst, making it a cornerstone for a successful career in offensive security.

Course Duration

10 days

Course Objectives

1. Apply the Five Phases of Hacking to perform comprehensive penetration tests.
2. Conduct deep-dive OSINT (Open-Source Intelligence) and passive/active footprinting using advanced tools.
3. Execute sophisticated network scanning and vulnerability analysis to map attack surfaces.
4. Gain and maintain system access using contemporary methods like buffer overflows and privilege escalation.
5. Understand, analyze, and defend against advanced threats, including fileless malware and Advanced Persistent Threats (APTs).
6. Identify and exploit flaws in web applications based on the OWASP Top 10
7. Secure and test the integrity of Wi-Fi networks and mobile platforms
8. Assess and secure environments in Cloud Computing and containerization technologies.
9. Discover and mitigate vulnerabilities in Internet of Things (IoT) and Operational Technology (OT)/Industrial Control Systems.
10. Implement techniques to bypass and detect common security controls like Firewalls, IDS, and Honeypots.
11. Simulate and defend against human-centric attacks, including phishing and pretexting.
12. Understand and apply modern cryptographic algorithms and Public Key Infrastructure (PKI) for data protection.
13. Develop clear, actionable penetration testing reports with effective vulnerability remediation strategies.

Target Audience

1. Security Analysts and Security Specialists
2. Penetration Testers and Ethical Hackers

3. Network Architects and Engineers
4. System and Database Administrators
5. Information Security Managers and Auditors
6. Cybersecurity Consultants and Risk Professionals
7. Application Developers and Software Engineers
8. Anyone interested in mastering the skills of an Offensive Security professional.

Course Modules

Module 1: Introduction to Ethical Hacking and Reconnaissance

- Understanding the Cyber Kill Chain and Ethical Hacking phases.
- Legal and ethical considerations for penetration testing.
- Passive and Active Footprinting and OSINT.
- Tools and techniques for advanced Google hacking and DNS enumeration.
- Case Study: Analysis of a major corporate data breach resulting from social media and public-record OSINT that provided initial entry vectors.

Module 2: Scanning Networks

- Network scanning techniques
- Using Nmap for host discovery, service identification, and OS fingerprinting.
- Evasion, Firewalking, and Banner Grabbing.
- Proxy server chains and Tor usage for anonymization.
- Case Study: A real-world example where poor network configuration and inadequate Nmap scripting detection allowed an attacker to map the entire network and services undetected.

Module 3: System Hacking and Gaining Access

- Password Cracking methodologies
- Privilege Escalation techniques on Windows and Linux.
- Steganography and Covering Tracks
- Executing and analyzing Kernel-level Exploits.
- Case Study: The use of a local exploit to escalate privileges from a low-level user account to a domain administrator, demonstrating the failure of **least privilege** principle.

Module 4: Malware Threats and Analysis

- Trojans, Viruses, Worms, Rootkits, and Ransomware.
- Fileless Malware and APT Lifecycle.
- Static and Dynamic Malware Analysis techniques and sandboxing.
- Countermeasures for Botnets and Malware Communication.
- Case Study: Dissection of a recent Ransomware attack, focusing on its propagation method and decryption cost calculation.

Module 5: Sniffing and Session Hijacking

- Network sniffing techniques
- Using Wireshark for deep packet analysis and extracting credentials.
- Session Hijacking at the network and application layer.
- Countermeasures for sniffing and secure session management.

- Case Study: A simulated Man-in-the-Middle attack using a public Wi-Fi hotspot to intercept and decrypt a user's web traffic, highlighting the need for mandatory HTTPS/TLS.

Module 6: Denial-of-Service

- Understanding DoS/DDoS Attack types
- Botnet creation and management for Distributed Denial of Service.
- Identifying and exploiting vulnerabilities leading to DoS.
- Cloud-based DDoS protection and mitigation strategies.
- Case Study: The impact analysis of a major DDoS attack on an e-commerce platform, detailing the financial loss and the steps for effective CDN and rate-limiting defense.

Module 7: Social Engineering and Human-Level Hacking

- The psychology of Social Engineering
- Simulating effective Phishing and Spear Phishing campaigns.
- Physical security attacks and human-based vulnerabilities.
- Employee training and security awareness countermeasures.
- Case Study: A corporate incident of a successful CEO Fraud email scam that resulted in a six-figure wire transfer, emphasizing the failure of internal verification protocols.

Module 8: Hacking Web Servers and Applications

- Web server and platform security hardening
- Identifying Web Server Misconfigurations and exploiting default installations.
- In-depth analysis of the OWASP Top 10 vulnerabilities.
- Using Burp Suite for manual and automated web application penetration testing.
- Case Study: Exploiting a known vulnerability on a live simulated web server to gain remote command execution

Module 9: SQL Injection and Database Attacks

- Types of SQL Injection
- Exploiting database misconfigurations and accessing sensitive data.
- Using automated tools like sqlmap for injection attacks.
- Database hardening and code review countermeasures.
- Case Study: The extraction of a simulated customer database using a basic Blind SQL Injection attack, illustrating the severe impact of poor input validation.

Module 10: Hacking Wireless Networks

- Wireless encryption standards: WEP, WPA/WPA2/WPA3
- Cracking Wi-Fi passwords using brute-force and dictionary attacks
- Attacks on wireless infrastructure
- Securing wireless networks and access points.
- Case Study: Performing a successful WPA2 handshake capture and dictionary attack to gain unauthorized access to a simulated corporate Wi-Fi network.

Module 11: Mobile Platform Hacking

- Mobile Platform Attack Vectors
- App-level attacks: Insecure Data Storage, Broken Cryptography.

- Mobile Malware and Reverse Engineering of mobile applications.
- Implementing Mobile Device Management and secure coding.
- Case Study: Analyzing a popular mobile application for Insecure Local Data Storage to extract unencrypted user credentials or API keys.

Module 12: IoT and Operational Technology (OT) Hacking

- Vulnerabilities in IoT Devices
- Hacking Smart Home and Wearable Technology.
- Introduction to SCADA/Industrial Control Systems and their unique vulnerabilities.
- Security best practices for securing the Internet of Everything.
- Case Study: Identifying and exploiting an unpatched vulnerability in a simulated Smart Camera or PLC to disrupt service.

Module 13: Cloud Computing Security

- Cloud deployment models and shared responsibility model.
- Common Cloud Misconfigurations
- Attacks on Serverless Computing and Containerization
- Cloud Security Posture Management and best practices.
- Case Study: Exploiting a misconfigured IAM policy in a simulated AWS environment to gain unauthorized access to a critical database instance.

Module 14: Evading IDS, Firewalls, and Honeypots

- Techniques for bypassing Intrusion Detection Systems and Firewalls.
- Fragmentation, IP Spoofing, and Evasion methodologies.
- Detection and analysis of Honeypots and decoy systems.
- Countermeasures and defensive security architectures.
- Case Study: Successfully launching a covert scan that evades a simulated Snort IDS rule by using advanced packet manipulation techniques.

Module 15: Cryptography and Public Key Infrastructure (PKI)

- Modern encryption algorithms and their applications.
- Understanding and attacking Public Key Infrastructure (PKI).
- Disk and Email Encryption techniques and tools.
- Introduction to Post-Quantum Cryptography and future challenges.
- Case Study: Cracking a weakly protected encrypted file or disk partition using an effective brute-force attack and demonstrating a better encryption policy.

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