

Certified Ethical Hacking 'Bootcamp' in Addis Ababa

The objective of this course is to equip cybersecurity professionals, SOC teams, and IT specialists with practical ethical hacking skills to identify, exploit, and secure vulnerabilities across modern digital environments. It offers hands-on experience in offensive security, system exploitation, malware analysis, wireless and cloud attacks, reporting, and implementing effective countermeasures.

10 FULL DAYS | <DATE - TBD> | TRAINING FACILITIES AT <LOCATION>

- The course focuses on real-world cyber-attacks, showcasing the hacker mindset and connecting every module to practical defensive relevance.
- Based on globally aligned Ethical Hacking methodologies and enhanced with guided demonstrations and exploitation labs.
- Practical scenarios with reconnaissance, scanning, enumeration, system exploitation, privilege escalation & post-exploitation.
- The program includes hands-on practice using CyCube Labs Platform with zero installation requirements.
- Dedicated lab access for practice, evaluation and strengthening of weak competency areas.
- Ideal for cybersecurity teams looking to enhance red-team and defensive security capabilities.
- Participants will gain confidence to perform ethical hacking assessments in professional environments.
- Global Certification mapping available.
- **Course prerequisites:** Basic knowledge of networking, OS (Windows/Linux), TCP/IP fundamentals and cybersecurity basics.

TARGET AUDIENCE

- Cybersecurity professionals
- SOC Analysts
- Information Security Officers
- Network and System Administrators
- Penetration Testers
- Red/Blue Team Analysts
- Security Engineers
- Anyone preparing for CEH Certification

THE INSTRUCTOR

Delivered by senior instructors with 10+ years of experience in cybersecurity and ICT systems, with strong hands-on and professional training expertise. Practical, scenario-based learning and hands-on labs are emphasized.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.



MODULE 01

INTRODUCTION TO ETHICAL HACKING

Learn the fundamentals of ethical hacking, information security principles, hacker classifications, and the five phases of hacking. Understand legal implications, policies, and security standards that guide authorized penetration testing.

MODULE 02

FOOTPRINTING AND RECONNAISSANCE

Explore passive and active reconnaissance methods. Learn to collect intelligence using open sources, identify an organization's digital footprint, and understand how attackers map targets during the pre-attack phase.

MODULE 03

SCANNING NETWORKS

Understand network discovery methods, port scanning, and service enumeration. Learn how scanning tools identify vulnerabilities and how network administrators can interpret and mitigate such activities.

MODULE 04

ENUMERATION

Study enumeration techniques for extracting usernames, network shares, and services. Learn about SNMP, LDAP, SMB, and NFS enumeration, and their implications in organizational security.

MODULE 05

VULNERABILITY ANALYSIS

Gain theoretical knowledge of vulnerability identification and risk prioritization. Understand vulnerability assessment processes, classification standards (CVSS, CWE), and common automated tools used by security professionals.

MODULE 06

SYSTEM HACKING

Understand how attackers gain system access through password attacks, privilege escalation, and backdoors. Learn defensive mechanisms such as patching, hardening, and system monitoring.

MODULE 07

MALWARE THREATS

Study malware types including viruses, worms, Trojans, ransomware, APTs, and fileless malware. Learn infection vectors, analysis methods, and defensive approaches.

MODULE 08

SNIFFING

Understand packet sniffing principles, ARP poisoning, MAC flooding, and Man-in-the-Middle attacks. Learn detection techniques and network hardening measures to prevent interception.

MODULE 09

SOCIAL ENGINEERING

Analyze psychological manipulation techniques used by attackers. Learn phishing, pretexting, baiting, vishing, and employee-awareness strategies to reduce human vulnerability.

MODULE 10

DENIAL-OF-SERVICE (DOS) & DDOS ATTACKS

Explore DoS/DDoS mechanisms, attack tools, and defense strategies. Understand how attackers exhaust system resources and how to mitigate service disruption.

MODULE 11

SESSION HIJACKING

Understand TCP/IP session hijacking, session fixation, and authentication manipulation. Learn cookie theft prevention and secure session management techniques.

MODULE 12

EVADING IDS, FIREWALLS & HONEYPOTS

Study evasion techniques using packet obfuscation, tunneling, and fragmentation. Learn configuration strategies and countermeasures to strengthen network defenses.

MODULE 13

HACKING WEB SERVERS

Understand web server architecture, attack vectors like directory traversal and misconfiguration exploitation. Learn best practices in server hardening and patch management.

MODULE 14

HACKING WEB APPLICATIONS

Study OWASP Top 10 vulnerabilities such as XSS, file inclusion, and command injection. Understand secure coding and application security fundamentals.

MODULE 15

SQL INJECTION

Understand SQL injection theory, detection, exploitation techniques, and prevention using validation and sanitization methods.

MODULE 16

HACKING WIRELESS NETWORKS

Study wireless security protocols (WEP, WPA2, WPA3), rogue AP attacks, evil twin techniques, and wireless security measures.

MODULE 17

HACKING MOBILE PLATFORMS

Learn Android & iOS vulnerability landscape, mobile malware, rooting/jailbreaking risks, and secure mobile development considerations.

MODULE 18

IOT & OT HACKING

Understand vulnerabilities in IoT devices and operational technology systems. Learn about weak authentication, firmware tampering, and network exposure scenarios.

MODULE 19

CLOUD COMPUTING SECURITY

Study cloud architecture, shared responsibility model, misconfiguration risks, insecure APIs, and cloud-specific attack vectors.

MODULE 20

CRYPTOGRAPHY

Learn encryption fundamentals, hashing, symmetric & asymmetric algorithms, PKI, and cryptographic attack methods.