CEH: Certified Ethical Hacker v13 – Lite

Course Code: CEH-LITE
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The C|EH v13 is a specialized, one-of-a-kind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry.

This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands on lab and practice range experience.

SKILLS COVERED

Armed with your attack platform (Parrot OS) and a plethora of tools used by ethical hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP, and experience the real thing in a controlled environment with no consequences. It's the ultimate learning experience to support your career as an ethical hacker! Each phase builds on the last as you progress through your ABCDorg engagement.

Phase 1: Vulnerability assessment:

- Footpringing & Reconnaissance
- Scanning
- Enumeration
- Vulnerability Analysis

Phase 2: Gaining access

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service

Phase 3: Perimeter and Web App Exploitation:

- Session Hijacking
- Evading IDS
- Firewalls
- Honeypots
- Hacking Web
- Servers
- Hacking Web
- Applications
- SQL Injection

Phase 4: Mobile, IoT, OT Exploitation:

- Hacking Wireless
- Networks
- Hacking Mobile
- Platforms
- IoT Hacking
- OT Hacking
- Cloud Computing
- Cryptography

WHO SHOULD ATTEND?

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Information Security Analyst 1
- Infosec Security Administrator
- Cybersecurity Analyst (Level 1, Level 2, & Level 3)
- Network Security Engineer
- SOC Security Analyst
- Network Engineer
- Senior Security Consultant

- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- All-Source Analyst
- Cyber Defense Incident Responder
- Research & Development Specialist
- Senior Cloud Security Analyst
- Third Party Risk Management:
- Threat Hunting Analyst
- Penetration Ttester
- Cyber Delivery Manager
- Application Security Risk
- Threat Modelling Specialist
- Web Application Penetration Testing
- SAP Vulnerability Management – Solution Delivery Advisor
- Ethical Hacker
- SIEM Threat Responder
- Product Security Engineer / Manager
- Endpoint Security Engineer
- Cybersecurity Instructor
- Red Team Specialist
- Data Protection & Privacy Officer
- SOAR Engineer
- AI Security Engineer
- Sr. IAM Engineer
- PCI Security Advisor
- Exploitation Analyst (EA)
- Zero Trust Solutions Engineer / Analyst
- Cryptographic Engineer
- AI/ML Security Engineer
- Machine Learning Security Specialist
- AI Penetration Tester
- AI/ ML Security Consultant
- Crypto Security Consultant

PREREQUISITES

You need only an internet connection, and can compete through your browser. We provide the attack platform, targets and all the required tools. You bring the skills to win.

MODULES

Module 1: Introduction to Ethical Hacking

- Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 2: Foot printing and Reconnaissance

- Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking

Module 3: Scanning Networks

- Learn different network scanning techniques and countermeasures.

Module 4: Enumeration

- Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures

Module 5: Vulnerability Analysis

- Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.

Module 6: System Hacking

- Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.

Module 7: Malware Threats

- Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures

Module 8: Sniffing

- Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

Module 9: Social Engineering

- Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10: Denial-of-Service

- Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking

- Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots

- Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13: Hacking Web Servers

- Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications

- Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures

Module 15: SQL Injection

- Learn about SQL injection attack techniques, evasiontechniques, and SQL injection countermeasures

Module 16: Hacking Wireless Networks

- Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks

Module 17: Hacking Mobile Platforms

- Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18: IoT Hacking

- Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

Module 19: Cloud Computing

- Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.

Module 20: Cryptography

- Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools

END OF PAGE