# CEH - Certified Ethical Hacker v13 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

The **Certified Ethical Hacker (CEH)** program from **EC-Council** is globally recognized as the **gold standard in ethical hacking and penetration testing certifications.**
The new **CEH v13** has been completely re-engineered to reflect today's evolving cyber threats — integrating **AI-assisted hacking simulations, cloud-based cyber ranges**, and **real-world threat environments** for a cutting-edge learning experience.

This hands-on program teaches participants how to **think like a hacker**, identify and exploit vulnerabilities ethically,
and strengthen organizational defenses across networks, applications, systems, and cloud infrastructures.

Delivered by **EC-Council-accredited instructors**, CEH v13 provides both theoretical mastery and extensive real-world practice,
preparing participants for **two globally recognized certification exams**: the **CEH Knowledge Exam** and the **CEH Practical Exam**.

### Why Choose CEH v13?

The CEH v13 introduces innovations that transform ethical hacking training into a true cyber warfare simulation:

- **AI-Driven Attack Simulation:** Practice with machine learning–powered exploit automation.
- **Cloud Security Scenarios:** AWS, Azure, and Google Cloud Penetration Testing Labs.
- **Real-Time Vulnerability Environments:** Live, unpatched systems for realistic training.
- **Cyber Range Integration:** 100+ cloud-based guided labs.
- **Dual Exam Structure:** Knowledge + Practical for full CEH certification.
- **Updated for Modern Threats:** Ransomware, APTs, Zero-Days, Fileless Malware, IoT Exploitation.

The **EC-Council Certified Ethical Hacker (CEH) v13** program is the most comprehensive and advanced pathway for cybersecurity professionals to build elite ethical hacking skills.

This certification not only validates your ability to **think like a hacker**
but also empowers you to **defend like a cybersecurity strategist**.

Through AI-enhanced labs, practical exams, and real-world attack simulations,
you'll emerge as a **globally recognized cybersecurity professional**
capable of identifying, exploiting, and defending against evolving cyber threats.

# CEH - Certified Ethical Hacker v13 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

**Bilginç IT Academy** is an **Official Accredited Training Partner of EC-Council**, delivering EC-Council-authorized cybersecurity trainings and certification programs globally.

## Prerequisites

While there are no mandatory prerequisites, participants are expected to have:

- A basic understanding of **Windows and Linux/Unix** operating systems.
- Familiarity with **networking concepts** (TCP/IP, ports, routing, firewalls).
- A foundational awareness of **cybersecurity principles and best practices**.

## Who Should Attend

This training is ideal for:

- Cybersecurity Professionals and Network Security Engineers
- System and Network Administrators
- Security Analysts and Information Security Officers
- IT Managers and Auditors
- Penetration Testers and Vulnerability Analysts
- Cloud Security and Risk Professionals
- Individuals pursuing **EC-Council CEH Certification**

## What You Will Learn

After completing the **CEH v13** program, participants will be able to:

- Understand ethical hacking principles, frameworks, and legal aspects.
- Conduct reconnaissance and vulnerability assessments effectively.
- Execute exploitation on systems, applications, networks, and cloud environments.
- Analyze malware types — Trojans, worms, ransomware, and advanced persistent threats (APTs).
- Perform web, mobile, and IoT penetration testing.
- Apply countermeasures for DDoS, SQL injection, phishing, and social engineering.
- Evade firewalls, IDS/IPS, and honeypots using advanced obfuscation methods.
- Implement secure communication using cryptography and PKI.
- Utilize AI-driven penetration testing tools and frameworks.
- Successfully pass both CEH Knowledge and CEH Practical exams.

# CEH - Certified Ethical Hacker v13 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Outline

### Ethical Hacking Foundations

- Introduction to cybersecurity, threat landscape, and hacker taxonomy
- Understanding legal frameworks and compliance standards (ISO 27001, NIST, GDPR)
- Security controls, frameworks, and defensive strategies

### Reconnaissance and Information Gathering

- Open Source Intelligence (OSINT) and footprinting techniques
- DNS, Whois, and email tracking
- Network scanning and active enumeration

### Scanning and Enumeration

- Port scanning, service detection, and banner grabbing
- SNMP, LDAP, NetBIOS enumeration
- Exploiting exposed services

### System Hacking

- Password cracking and privilege escalation
- Creating and hiding backdoors
- Steganography and anti-forensic techniques

### Malware Threats

- Analysis of Trojans, viruses, and worms
- Fileless malware and rootkits
- Malware detection and mitigation strategies

### Social Engineering and Phishing

- Psychological manipulation and impersonation tactics
- Real-world phishing simulations and prevention
- Social engineering countermeasures

### Denial of Service (DoS/DDoS) Attacks

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Types of flooding and amplification attacks
- Defensive configurations and mitigation tools
- Network hardening against distributed attacks

### Session Hijacking and IDS Evasion

- Session management vulnerabilities and exploitation
- Man-in-the-Middle (MITM) attacks
- Evasion techniques for IDS/IPS and firewalls

### Web Application and Database Security

- OWASP Top 10 vulnerabilities
- SQL injection, XSS, and command injection
- Web server security hardening and monitoring

### Wireless, Mobile, and IoT Security

- Wi-Fi attacks (Evil Twin, WPA2 cracking, deauthentication)
- Mobile application exploitation (Android/iOS)
- IoT and OT infrastructure security assessment

### Cloud Security

- Security threats across AWS, Azure, and GCP
- Cloud IAM and network segmentation
- Virtualization and container security

### Cryptography and Secure Communication

- Encryption standards (AES, RSA, ECC)
- Digital signatures, PKI, SSL/TLS
- VPNs and secure tunnel configurations

### AI-Augmented Ethical Hacking

- Using AI for exploit automation and vulnerability prioritization
- Machine learning in threat detection
- AI-based penetration test simulations and predictive defense

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


## Exams and Assessments

The programme includes two EC-Council certification assessments that are taken after the course:

- **CEH Knowledge Exam:** 125 multiple-choice questions with a four-hour duration
- **CEH Practical Exam:** 20 scenario-based tasks with a six-hour duration

## Hands-On Cyber Range Labs

Participants will gain real-world experience through:

- Over **100 hands-on labs** in a **cloud-based Cyber Range**
- Realistic network and system vulnerabilities
- **OWASP Top 10 exploit labs** and security configuration challenges
- **AI-assisted hacking exercises** with automated defense detection
- Wireshark, Nmap, Metasploit, Burp Suite, and Splunk integration