

312-50: Certified Ethical Hacker (CEH)

Learn how attackers work so you can defend against them — with hands-on labs and structured preparation for the CEH 312-50 exam.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

15 modules · 9 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Ethical hackers use the same tools and techniques as attackers, with permission, to show organisations where they are exposed. Understanding that attacker mindset is useful well beyond penetration testing: defenders, auditors and architects all make better decisions when they know how systems are actually broken into. This five-day course is exam-aligned preparation for the CEH 312-50 exam, built around hands-on practice.

Day one introduces information security and ethical hacking concepts, legal considerations and the attack methodology, followed by footprinting and reconnaissance. Day two covers scanning networks, enumeration and vulnerability analysis. Day three focuses on system hacking, malware threats, sniffing and social engineering. Day four addresses denial of service, session hijacking, evading IDS and firewalls, and web server and web application attacks, including SQL injection. Day five covers wireless networks, mobile platforms, IoT and OT, cloud computing and cryptography, finishing with exam readiness.

Every module includes practical work in an isolated lab, and the trainer explains the countermeasure for each technique so that you leave with both offensive and defensive understanding. Ethics and authorisation are emphasised throughout.

This is independent, exam-aligned training; it does not use EC-Council courseware and Ace Skills Consulting does not claim to be an EC-Council Accredited Training Centre. Exam eligibility, registration and vouchers are handled through EC-Council's official channels, so confirm the current exam version and requirements with EC-Council before booking.

Highlights

- 40 hours of live, lab-driven preparation
- Five phases of ethical hacking in practice
- Web, wireless, mobile, IoT and cloud attack labs
- Mapped to the published CEH exam blueprint areas
- Practice questions with explanations

What's included

- Isolated lab environment for safe practice
- Countermeasures taught alongside every attack
- Web application and SQL injection labs
- Wireless, cloud and IoT attack coverage
- Practice questions mapped to blueprint areas
- Course completion certificate from Ace Skills Consulting
- Post-training doubt support while you prepare

Who this course is for

Who should attend

- Security analysts and SOC staff
- Network and system administrators
- Aspiring penetration testers
- IT auditors who assess technical controls
- Security+ holders progressing to offensive skills

Prerequisites

- Networking fundamentals including TCP/IP
- Familiarity with Windows and Linux
- Security+ level knowledge recommended

Detailed curriculum — 5 days, 40 hours, 15 modules, 9 hands-on labs

Day 1 Foundations & Reconnaissance

8 hours

1.1 Ethical hacking concepts

- Information security elements and attack classes
- Laws, standards and authorisation
- Hacking methodology and frameworks
- Information assurance and risk

1.2 Footprinting and reconnaissance

- Search engine and social media footprinting
- Network footprinting
- WHOIS and DNS footprinting
- Countermeasures

LAB Perform passive footprinting of a fictional organisation · 45 min

1.3 Lab environment

- Kali Linux and target systems
- Documenting findings

Day 2 Scanning, Enumeration & Vulnerability Analysis

8 hours

2.1 Scanning networks

- Host discovery
- OS fingerprinting
- Port and service scanning
- Scanning beyond IDS and firewalls

LAB Scan the lab network with Nmap using different techniques · 50 min

2.2 Enumeration

- NetBIOS and SMB enumeration
- DNS and NTP enumeration
- SNMP and LDAP enumeration

LAB Enumerate users and shares on a Windows target · 40 min

2.3 Vulnerability analysis

- Vulnerability classification and scoring
- Reading assessment reports
- Assessment tools

LAB Run a vulnerability assessment and rank findings · 35 min

Day 3 System Hacking, Malware, Sniffing & Social Engineering

8 hours

3.1 System hacking

- Gaining access and password cracking
- Maintaining access
- Privilege escalation
- Clearing tracks

LAB Crack password hashes and escalate privileges · 50 min

3.2 Malware threats

- Trojans, viruses and worms
- Malware analysis basics
- Fileless malware
- Countermeasures

3.3 Sniffing and social engineering

- MAC, DHCP and ARP attacks
- Social engineering techniques
- DNS poisoning
- Insider threats and identity theft

LAB Capture credentials with ARP spoofing in the lab · 40 min

Day 4 Network & Web Application Attacks

8 hours

4.1 Denial of service and session hijacking

- DoS and DDoS techniques
- Application and network session hijacking
- Botnets
- Countermeasures

4.2 Evading defences

- IDS, IPS and firewall evasion
- Evasion countermeasures
- Honeypots

4.3 Web servers and applications

- Web server attacks
- SQL injection techniques
- OWASP Top 10 vulnerabilities
- Web API and webhook attacks

LAB Exploit SQL injection and cross-site scripting in a vulnerable app · 60 min

Day 5 Wireless, Mobile, IoT, Cloud, Cryptography & Exam Readiness

8 hours

5.1 Wireless and mobile

- Wireless encryption and attacks
- Android and iOS attack vectors
- Bluetooth threats
- Mobile device management

LAB Analyse a captured WPA2 handshake · 30 min

5.2 IoT, OT and cloud

- IoT and OT attack surfaces
- Container and serverless security
- Cloud service models and threats
- Cloud hacking countermeasures

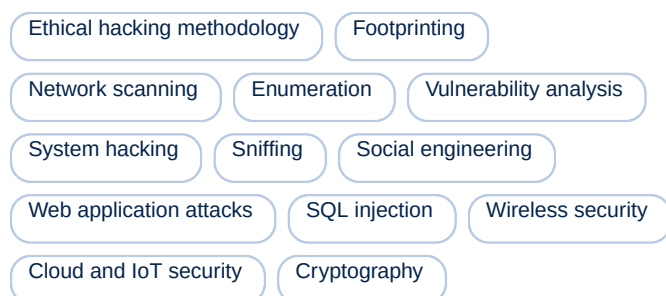
5.3 Cryptography and exam readiness

- Encryption algorithms and PKI
- Practice questions and review
- Cryptanalysis and attacks

LAB Encrypt, sign and verify data with OpenSSL · 25 min

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Certified Ethical Hacker (CEH)
Exam code	312-50
Questions	125
Duration	240 minutes
Format	Multiple choice
Official page	https://www.eccouncil.org/

Exam skill areas covered

Exam skill areas covered:

- Reconnaissance and Information Gathering
- Network Scanning and Enumeration
- Vulnerability Assessment and Exploitation
- Password Attacks and Cracking
- Wireless Network Attacks
- Social Engineering and Phishing
- Malware Analysis and Detection
- Denial of Service (DoS) Attacks
- Cryptography and Secure Communications
- Incident Response and Forensics
- Ethical Hacking Overview
- Advanced Penetration Testing Techniques

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

How do I register for the CEH exam?

You register for the exam through EC-Council's official channels, which set the eligibility rules, including the application process for candidates who have not attended official training. We guide you through the steps but cannot issue vouchers ourselves.

Is this official EC-Council training?

No. This is independent, exam-aligned preparation using our own material; it does not use EC-Council courseware.

Which CEH version does the course follow?

The course follows the current published exam areas. EC-Council updates CEH versions periodically, so confirm the active version before booking.

Is hacking practice legal?

Yes, within our isolated lab. You must only test systems you are explicitly authorised to test.

Should I take CEH or PenTest+?

CEH covers a broad range of attack techniques, while PenTest+ focuses more on the full engagement and reporting. We can help you choose based on your goals.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/312-50-certified-ethical-hacker-ceh · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur

New Delhi 110092

Office: 98180 12523

CEH, CHFI and CND are trademarks of the International Council of E-Commerce Consultants (EC-Council). All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website.

Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.