Certified Ethical Hacker (CEH v13 with AI)

Become a job-ready ethical hacker who thinks like an attacker and uses AI to test, break, and defend modern systems.

Duration: 2 months | Prepares for: EC-Council CEH v13 | Format: Online or onsite, 1-on-1 or batch | Target exam: 312-50 (CEH) | NUEXUS certificate on completion

OVERVIEW

This is a hands-on, mentor-led program that trains you in the full offensive security lifecycle covered by EC-Council's Certified Ethical Hacker v13, the first CEH edition to integrate AI into every phase of ethical hacking. Over roughly two months you work through live labs across all 20 CEH modules, learning to perform reconnaissance, exploit vulnerabilities, escalate access, and report findings the way real penetration testers do, while using AI to accelerate recon, analysis, and payload work. The course is exam-aligned to the current CEH v13 blueprint and job-focused, so you finish with both a recognized credential path and practical skills you can apply in a SOC, red team, or VAPT role. You earn a NUEXUS completion certificate on finishing, and separately you can pursue the official EC-Council CEH exam.

SKILLS YOU WILL GAIN

Footprinting & Reconnaissance | Scanning Networks | Enumeration | Vulnerability Analysis | System Hacking | Malware Threats | Sniffing | Social Engineering | Denial-of-Service | Session Hijacking | Evading IDS, Firewalls & Honeypots | Hacking Web Servers | Hacking Web Applications | SQL Injection | Hacking Wireless Networks | Hacking Mobile Platforms | IoT & OT Hacking | Cloud Computing | Cryptography | AI-Driven Ethical Hacking

WHAT YOU WILL BE ABLE TO DO

- Plan and run a structured penetration test through all five phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks
- Perform footprinting, network scanning, enumeration, and vulnerability analysis using industry-standard tools and AI-assisted techniques
- Exploit systems, web applications, wireless networks, and web servers, then perform privilege escalation and post-exploitation
- Test for the common web attacks including SQL injection, cross-site scripting, and session hijacking, and assess web servers and web apps
- Identify and exploit weaknesses in cloud, IoT, OT, and mobile environments, and understand cryptography and its attacks
- Use AI to accelerate reconnaissance, vulnerability triage, and analysis, and document findings in a clear, professional penetration test report

WHO IT IS FOR

- IT, network, or system administrators who want to move into offensive security and penetration testing
- Aspiring ethical hackers and red teamers targeting the EC-Council CEH v13 credential
- SOC analysts and blue team members who want to understand attacker techniques to defend better
- Computer science and cybersecurity students building a job-ready practical skill set
- Security professionals who need a globally recognized, HR-friendly certification for career growth

PREREQUISITES

- Basic networking knowledge (TCP/IP, ports, protocols, the OSI model) and comfort with IP addressing
- Familiarity with at least one operating system at the command line, ideally both Windows and Linux basics
- General IT literacy; EC-Council recommends around two years of information security experience, though motivated career changers with strong fundamentals are welcome
- A laptop able to run virtual machines for the lab environment; no prior hacking experience required

WHAT'S INCLUDED

- Mentor-led live sessions, online or onsite, in batch or 1-on-1
- Hands-on labs and real-world projects, not slides alone
- Recordings of your own sessions to revisit anytime
- Exam-aligned study material and practice questions
- Doubt-clearing and revision support through the program
- A verifiable NUEXUS completion certificate
- Career and next-step guidance after you finish

COURSE CURRICULUM

1 Introduction to Ethical Hacking and AI-Driven Security

- Information security overview, threats, and attack vectors
- Cyber Kill Chain, MITRE ATT&CK, and hacking phases
- Ethical hacking concepts, scope, and legal and compliance considerations
- How AI is changing offensive and defensive security in CEH v13

2 Footprinting and Reconnaissance

- Passive and active footprinting methodology
- OSINT, WHOIS, DNS, and search engine reconnaissance
- Website, email, and social media footprinting
- AI-assisted reconnaissance and footprinting countermeasures

3 Scanning Networks and Enumeration

- Host discovery, port and service scanning with Nmap
- Banner grabbing, OS fingerprinting, and evasion techniques
- Enumeration of NetBIOS, SNMP, LDAP, NFS, SMTP, and DNS
- Mapping the attack surface and scanning countermeasures

4 Vulnerability Analysis

- Vulnerability assessment concepts and lifecycle
- Using vulnerability scanners and interpreting results
- CVSS scoring, prioritization, and vulnerability research sources
- AI-assisted vulnerability triage and reporting

5 System Hacking and Malware Threats

- Password cracking, privilege escalation, and gaining access
- Maintaining access, persistence, and clearing logs and tracks
- Malware types: trojans, viruses, worms, and fileless malware
- Steganography, rootkits, and malware analysis basics

6 Sniffing, Social Engineering, and Denial of Service

- Packet sniffing, MAC and DHCP attacks, and ARP poisoning
- Social engineering techniques, phishing, and human-layer attacks
- DoS and DDoS attack techniques and botnets
- Session hijacking at network and application layers

7 Web Server, Web Application, and Database Hacking

- Web server attacks, misconfigurations, and countermeasures
- Web application threats and common attack classes
- SQL injection discovery, exploitation, and defense
- Cross-site scripting, authentication, and session flaws

8 Wireless, Mobile, IoT, and OT Hacking

- Wireless encryption, WEP and WPA attacks, and rogue access points
- Mobile platform attack vectors on Android and iOS
- IoT and OT threats, architecture, and hacking methodology
- Bluetooth and wireless security countermeasures

9 Cloud Computing and Cryptography

- Cloud concepts, container and serverless security
- Cloud attacks, misconfigurations, and shared responsibility
- Cryptography fundamentals, algorithms, and PKI
- Cryptanalysis, encryption attacks, and defensive controls

10 Penetration Testing Workflow and Reporting

- End-to-end pentest engagement and rules of engagement
- Chaining techniques across the CEH attack phases in the lab
- Evidence collection and professional report writing
- CEH exam readiness, question types, and lab-based practice

CAREER OUTCOMES

Penetration Tester · Ethical Hacker · SOC Analyst · Vulnerability Analyst · Red Team Member · Security Consultant

Entry	USD 50,000 to 75,000
Mid	USD 75,000 to 110,000
Senior	USD 110,000 to 150,000

Global averages from Glassdoor and PayScale, 2025. Actual pay varies by country, employer and experience.

CERTIFICATION PATH

NUEXUS training certificate

Issued by NUEXUS on course completion. Verifiable at nuexus.com/verify.

EC-Council CEH v13

Earned by passing the official exam. Issued and verified by the certification body itself, not by NUEXUS.

Exam	312-50 (CEH)
Questions	125 multiple-choice questions
Format	Multiple choice. The hands-on CEH Practical (20 challenges, 6 hours) is a separate exam
Duration	4 hours
Passing score	Cut scores are set per exam form and range from 60% to 85% (EC-Council policy)
Delivery	EC-Council ECC EXAM portal or Pearson VUE; remote proctoring available

The official EC-Council exam voucher and the eligibility application are arranged separately with EC-Council and quoted per engagement. Even when NUEXUS arranges your exam voucher, the resulting certification is issued and verified by the certification body directly.