

EC-COUNCIL

CEH v13 — Certified Ethical Hacker Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

40 HOURS

5 DAYS

At a glance

COURSE	CEH v13 — Certified Ethical Hacker
TRACK	EC-Council
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Twenty modules, mapped one-for-one to the official CEH v13 blueprint and taught in the same order, so nothing on the exam is left uncovered.

What separates v13 from earlier versions is artificial intelligence. It is not a bolt-on module at the end — AI runs through all five phases of the attack lifecycle, on both sides. You learn to use AI to do the work faster, and you learn to attack AI systems themselves. Every module below carries that thread.

Half the classroom time is hands-on. Techniques are practised against a target estate we have already broken on purpose, so you are finding real weaknesses rather than following a script to a known answer.

Module 01 — Introduction to Ethical Hacking

The ground rules: what information security actually protects, how attacks are structured, and where your authority begins and ends.

- Information security fundamentals: confidentiality, integrity, availability, and why they trade against each other
- The cyber kill chain and MITRE ATT&CK as ways of describing an intrusion
- Hacker classes, threat actors and their motivations
- The five phases of ethical hacking, which the rest of the course follows
- AI-driven ethical hacking: where automation genuinely helps and where it misleads you
- Information security controls, defence in depth and the assurance lifecycle
- Laws, standards and regulations — including the Indian IT Act, GDPR and PCI DSS
- Scoping, rules of engagement, and getting authorisation in writing before you touch anything

Module 02 — Footprinting and Reconnaissance

Everything an attacker can learn about your organisation before sending a single packet to your infrastructure.

- Footprinting methodology and what a complete reconnaissance picture looks like
- Search engine, advanced Google operators and dark-web footprinting
- Social media and people-search reconnaissance, and what your staff leak without knowing
- Website, email header and competitive-intelligence footprinting
- Whois, DNS and network range enumeration
- AI-assisted OSINT: using language models to collect, dedupe and rank findings at speed
- Automating reconnaissance, and reading the output critically rather than trusting it
- Footprinting countermeasures and reducing your own external exposure

Module 03 — Scanning Networks

Turning a reconnaissance picture into a map of live hosts, open ports and running services.

- Host discovery and the trade-off between thoroughness and noise
- Port and service scanning techniques, and what each one reveals to a defender
- Scanning beyond IDS and firewall inspection
- OS fingerprinting and banner grabbing
- Network topology discovery and drawing an accurate map
- AI-assisted scanning: prioritising which hosts deserve attention first

- Interpreting scan output without drowning in it
- Scanning countermeasures and detecting a scan against your own estate

Module 04 – Enumeration

Pulling usernames, shares, services and configuration detail out of the protocols that will give them up.

- Enumeration concepts and why it matters more than scanning
- NetBIOS, SNMP, LDAP and NTP/NFS enumeration
- SMTP, DNS and DNSSEC zone-walking enumeration
- IPsec, VoIP, RPC, Unix/Linux and Telnet enumeration
- AI-supported enumeration and correlation across sources
- Building an attack surface picture from enumeration results
- Enumeration countermeasures and protocol hardening

Module 05 – Vulnerability Analysis

Running an assessment is easy. Reading it properly is the skill.

- Vulnerability classification, research and the disclosure lifecycle
- CVSS scoring, CVE, CWE and the National Vulnerability Database
- Vulnerability assessment types, phases and tool selection
- AI-enhanced scanning and automated triage of findings
- Separating exploitable findings from noise and false positives
- Assessing vulnerabilities in cloud, container and OT environments
- Writing a vulnerability report that a system owner will act on

Module 06 – System Hacking

Gaining access, keeping it, and leaving without a trace — on Windows and Linux.

- The system hacking methodology, end to end
- Password cracking, hash extraction and pass-the-hash techniques
- Vulnerability exploitation and buffer-overflow fundamentals
- Privilege escalation on Windows and on Linux
- Maintaining access: persistence, remote execution and backdoors
- AI-automated exploitation, and the judgement it cannot replace
- Steganography and data-hiding techniques
- Covering tracks, clearing logs — and how a defender spots that it happened

Module 07 – Malware Threats

What malicious code does, how it hides, and how you analyse it safely.

- Malware taxonomy: trojans, viruses, worms, rootkits and fileless malware
- Advanced Persistent Threats and the stages of a long-running intrusion
- Malware delivery, droppers, packers and obfuscation
- Static and dynamic malware analysis in a contained environment
- AI-generated malware and AI-assisted detection
- Indicators of compromise and building detection from analysis

- Anti-malware controls, sandboxing and countermeasures

Module 08 — Sniffing

Reading traffic that was never meant for you, and stopping others from doing it.

- Packet sniffing concepts, and the difference between passive and active
- MAC flooding, ARP poisoning and switch-level attacks
- DHCP starvation and rogue server attacks
- DNS poisoning and spoofing techniques
- Capturing and analysing traffic with protocol analysers
- AI-assisted traffic analysis and anomaly detection at scale
- Sniffing detection and network-level countermeasures

Module 09 — Social Engineering

The attack surface that no firewall covers.

- Social engineering concepts and the psychology they exploit
- Human-based techniques: pretexting, impersonation, tailgating, dumpster diving
- Computer-based techniques: phishing, spear-phishing, business email compromise
- Mobile-based techniques and malicious applications
- AI-generated phishing, deepfake voice and video, and why they work
- Insider threats and how they differ from external attacks
- Identity theft and its consequences for the organisation
- Running an authorised social engineering test without harming your own staff
- Countermeasures, awareness programmes and reporting culture

Module 10 — Denial-of-Service

Making a service unavailable, and making sure yours stays up.

- DoS and DDoS attack concepts and their business impact
- Volumetric, protocol and application-layer attack categories
- Botnets, amplification and reflection techniques
- Attacks against APIs and mobile back-ends
- AI-assisted detection of attack traffic against normal load
- DoS/DDoS protection tools, scrubbing and rate limiting
- Auditing your own estate for denial-of-service exposure

Module 11 — Session Hijacking

Taking over an authenticated session instead of stealing a password.

- Session hijacking concepts and where the weakness sits
- Application-level hijacking: session tokens, cookies, cross-site attacks
- Network-level hijacking: TCP/IP, RST and man-in-the-middle
- Session token prediction and fixation
- AI-assisted detection of anomalous session behaviour
- Hijacking countermeasures, secure token handling and transport security

Module 12 — Evading IDS, Firewalls, and Honeypots

Understanding evasion is how you learn to tune your own detection.

- IDS, IPS, firewall and honeypot concepts and placement
- Evasion techniques: fragmentation, obfuscation, encoding, timing
- Firewall and application-gateway bypass techniques
- Detecting honeypots from an attacker's perspective
- AI-powered evasion, and AI-powered detection of it
- Hardening detection so evasion attempts surface rather than succeed

Module 13 — Hacking Web Servers

The server underneath the application, and the misconfigurations that expose it.

- Web server architecture, components and common weaknesses
- Web server attack methodology
- Directory traversal, misconfiguration and default-credential attacks
- Web server password attacks and cracking
- Patch management failures and why they persist
- AI-assisted web server reconnaissance
- Web server hardening, secure configuration and countermeasures

Module 14 — Hacking Web Applications

The OWASP Top 10, practised rather than recited.

- Web application architecture, components and threat model
- Web application attack methodology
- Broken access control and authentication failures
- Injection flaws, insecure design and security misconfiguration
- Cross-site scripting and cross-site request forgery
- Insecure deserialisation and vulnerable component use
- API and web services testing — REST, SOAP and GraphQL
- AI-driven application testing and the OWASP Top 10 for LLM applications
- Secure development practice and application-level countermeasures

Module 15 — SQL Injection

One flaw class, in real depth, because it still works.

- SQL injection concepts and how the flaw arises
- In-band, blind and out-of-band injection types
- SQL injection methodology, from detection to data extraction
- Evasion techniques against filters and web application firewalls
- Automating injection with AI assistance
- Injection against NoSQL and modern data stores
- Countermeasures: parameterised queries, least privilege, input validation

Module 16 — Hacking Wireless Networks

Attacks against the network people forget to test.

- Wireless concepts, standards, terminology and encryption
- WEP, WPA, WPA2 and WPA3 — strengths and known weaknesses
- Wireless threats: rogue access points, evil twin, jamming, KRACK
- Wireless hacking methodology and tooling
- Bluetooth and Bluetooth Low Energy attacks
- AI-assisted wireless reconnaissance and analysis
- Wireless security tools, countermeasures and secure deployment

Module 17 — Hacking Mobile Platforms

Android, iOS, and the corporate data sitting on both.

- Mobile platform attack vectors and the OWASP Mobile Top 10
- Android architecture, rooting, and Android-specific attacks
- iOS architecture, jailbreaking, and iOS-specific attacks
- Mobile application analysis, reverse engineering and instrumentation
- Mobile spyware, malicious applications and sideloading risk
- Mobile Device Management, BYOD policy and containerisation
- AI-assisted mobile application testing
- Mobile security guidelines and countermeasures

Module 18 — IoT and OT Hacking

The exposure most organisations do not know they have.

- IoT concepts, architecture, protocols and communication models
- IoT threats, attack surface areas and the OWASP IoT Top 10
- IoT hacking methodology and tooling
- Operational technology concepts: ICS, SCADA, PLCs and HMIs
- OT attack surface, protocol weaknesses and safety implications
- AI-assisted device discovery in IoT and OT environments
- IT/OT convergence, segmentation and countermeasures

Module 19 — Cloud Computing

Where the estate is someone else's, but the misconfiguration is yours.

- Cloud service and deployment models, and the shared responsibility model
- Container technology, Docker, Kubernetes and orchestration security
- Serverless computing and its distinct attack surface
- Cloud attacks: misconfiguration, identity abuse, privilege escalation, data exposure
- Cloud hacking methodology across major providers
- AI and machine learning services as a cloud attack surface
- Cloud security controls, posture management and countermeasures

Module 20 — Cryptography

The last module, and the one underneath everything else.

- Cryptography concepts, symmetric and asymmetric algorithms
- Hash functions, message digests and message authentication codes
- Public Key Infrastructure, certificates and certificate authorities
- Disk encryption, and encryption of data at rest and in transit
- Email and network encryption in practice
- Cryptanalysis and cryptographic attack techniques
- AI-assisted cryptanalysis, and the post-quantum question
- Cryptographic countermeasures and avoiding common implementation mistakes

Who should take this

Security testers and penetration testers, SOC analysts who want to understand the offensive side properly, network and system administrators moving into security, and security officers who need to assess findings rather than take them on trust.

You will need working knowledge of networking and operating systems, and to be comfortable on a command line. You do not need prior offensive security experience.

The exam

The CEH certification has two parts, both set and awarded by EC-Council:

- **CEH (Knowledge)** — 125 multiple-choice questions, four hours, proctored
- **CEH (Practical)** — 20 real-world challenges in a live range, six hours

Passing the knowledge exam earns CEH. Passing both earns CEH Master. The exam voucher is purchased separately from the certification body; we arrange it on your behalf and send you the code, and you book your own exam date.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Half the time is hands-on. Small cohorts, so everyone gets lab time rather than watching someone else have it.

Mapped to the official CEH v13 blueprint. Taught from Hacky Security's own curriculum and lab estate by instructors who also work our security operations centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/ceh-v13/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.