Ethical Hacking (CEH Exam Prep)

Find and exploit vulnerabilities the way attackers do, legally, aligned to the CEH exam.

DURATION	FORMAT	LEVEL	LABS
45 hours	Onsite, online or hybrid	Intermediate	Cloud sandbox included

About this programme

Covers the full ethical hacking methodology across the 20 CEH modules, from reconnaissance and scanning to system and web hacking, malware, social engineering, and wireless, mobile, IoT/OT and cloud attacks, together with the countermeasures that defend against them.

Who it is for: Security analysts, network and system administrators, and penetration testers

What your team will be able to do

- Run footprinting, scanning and enumeration against a target environment
- Assess vulnerabilities and demonstrate system and web attacks in a lab
- Analyse malware, sniffing, social engineering and denial-of-service techniques
- Assess wireless, mobile, IoT/OT and cloud attack surfaces
- Recommend countermeasures for each class of attack

Before you start

- Networking fundamentals
- Linux and Windows command line
- Basic security concepts (Security+ level)

Course outline

1. Ethical hacking and reconnaissance

- Information security and ethical hacking concepts
- Footprinting and reconnaissance
- Scanning networks for live hosts, ports and services
- Enumeration of users, shares and system resources

2. Vulnerabilities and system hacking

- Vulnerability analysis and assessment tools
- System hacking: password cracking and privilege escalation
- Malware threats: trojans, viruses and worms

3. Network and human attacks

- Sniffing and packet analysis
- Social engineering
- Denial-of-service and DDoS attacks
- Session hijacking
- Evading IDS, firewalls and honeypots

4. Web application attacks

- Hacking web servers
- Hacking web applications, including cross-site scripting
- SQL injection, evasion techniques and countermeasures

5. Wireless, mobile, IoT and cloud

- Wireless networks: WEP, WPA and WPA2 weaknesses
- Android and iOS attack vectors
- IoT and OT hacking
- Cloud computing threats and defences

6. Cryptography

- Encryption algorithms and cryptography tools
- Public key infrastructure and cryptographic attacks

Sample schedule

6 days onsite, or 12 half-day sessions online. We fit days and session lengths to your team's calendar.

Day 1	8 h	Ethical hacking and reconnaissance
Day 2	8 h	Ethical hacking and reconnaissance (continued); Vulnerabilities and system hacking; Network and human attacks
Day 3	8 h	Network and human attacks (continued)
Day 4	8 h	Network and human attacks (continued); Web application attacks
Day 5	8 h	Wireless, mobile, IoT and cloud
Day 6	5 h	Wireless, mobile, IoT and cloud (continued); Cryptography

Assessment and certification

How learning is checked

- A short knowledge check on day one and again at the end, so you can see each person's progress
- Graded hands-on labs in every module, reviewed by the trainer
- A final exercise that applies the programme to a problem like your team's own
- A timed practice exam in the format of the real one, with a review of every answer

Certificate and exams

- Participants who complete the programme receive a Cognitive Networks AI certificate of completion.
- Prepares your team for the CEH exam. Exam vouchers are not included: each participant books the exam with EC-Council.

Formats and cohort size

- Onsite: At your office or a venue you choose, in full days.
- Online, live: Instructor-led over video, usually in half-day sessions so people can keep up with work.
- Hybrid: Some days in a room together, the rest online. Useful when a team works across cities.

Cohort size: 15 to 25 people per trainer. Larger teams run as parallel cohorts on the same outline, so everyone learns the same thing.

Pricing: We quote per cohort, based on duration, format and number of cohorts. There is no per-seat price list: tell us your team and we send a proposal within one business day.

Bring this programme to your team

Request a proposal at cognitivenetworks.ai/contact?programme=ceh

reachus@cognitivenetworks.ai · Bangalore +91 72043 05303 · Dallas +1 (303) 827-7415

CEH and Certified Ethical Hacker are trademarks of EC-Council. Cognitive Networks AI is not affiliated with EC-Council. This programme prepares your team for the exam. It is not an official course of EC-Council, and the exam is booked separately.