



COURSE SYLLABUS

Certified Ethical Hacker (CEH)

Learn the tools and methods attackers use, from reconnaissance to web, wireless and cloud attacks, and prepare for the EC-Council CEH v13 (312-50) exam.

\$2,995 per person, including the 312-50 (CEH v13) exam voucher

19 course hours (on-demand video and labs) plus 1.5 hours of coaching

On-demand asynchronous training with online support, plus 1.5 hours of coaching.

Certified Ethical Hacker (CEH)

Learn the tools and methods attackers use, from reconnaissance to web, wireless and cloud attacks, and prepare for the EC-Council CEH v13 (312-50) exam.

Credential type	Certificate, issued by We Can Code IT
Clock hours	20.5 (19 course hours plus 1.5 hours of coaching)
Price	\$2,995 per person, including the 312-50 (CEH v13) exam voucher
Time	19 course hours (on-demand video and labs) plus 1.5 hours of coaching
Delivery	On-demand asynchronous training with online support, plus 1.5 hours of coaching.
Exam	EC-Council Certified Ethical Hacker (CEH) (312-50 (CEH v13)). This course prepares you for the CEH v13 knowledge exam (312-50), and one exam attempt is included. The exam has 125 multiple-choice questions over four hours. EC-Council lets you sit the exam only if you have two years of information security experience and an approved eligibility application, unless you trained through an EC-Council Accredited Training Center. We Can Code IT is not an EC-Council Accredited Training Center, so every learner in this course must submit the eligibility application with verifiable proof of two years of information security experience and be approved before the voucher is used. The eligibility application fee is included in the course price. Learners without that experience cannot sit the exam. Most learners need substantial additional lab practice and self-study beyond the course hours. Passing is not guaranteed.
Who it is for	This course is for security administrators, cybersecurity analysts, penetration testers and network or systems professionals with security duties who want to understand attacks from the attacker's side. It is intended for learners who already have at least two years of information security experience.
Prerequisites	At least 2 years of information security experience, which EC-Council requires for the eligibility application; Working knowledge of networking, operating systems and the command line; Comfort running and configuring a virtual machine
Requirements	A computer that can run a Kali Linux virtual machine; Some lab tools run only on x86 processors, so check compatibility before you start if you use an Apple-silicon Mac

About this course

This course follows the domains of the EC-Council Certified Ethical Hacker exam blueprint, starting with the law and rules of engagement and moving through reconnaissance, system hacking, network attacks, web applications, wireless, mobile, IoT, cloud and cryptography. You will practice each phase of an attack in a Kali Linux lab environment so you understand how weaknesses are found and how to defend against them. The course is built for people who already work in information security, because EC-Council requires security experience to sit the exam.

What you will be able to do

- You will be able to explain the legal limits, scope and rules of engagement for an authorized ethical hacking test.
- You will be able to perform footprinting, network scanning and enumeration against a lab target and document what you find.
- You will be able to identify vulnerabilities in a lab system and describe how an attacker would escalate access and how to block it.
- You will be able to demonstrate common network attacks such as sniffing, session hijacking and social engineering, and recommend countermeasures.
- You will be able to test a lab web application for SQL injection and other common web vulnerabilities.
- You will be able to describe attack techniques against wireless, mobile, IoT, OT and cloud systems and the cryptographic controls that protect them.

Syllabus

Module	Hours
1. Ethical hacking foundations, law and rules of engagement Information security concepts, Ethical hacking phases, Laws and standards, Scope and rules of engagement, Setting up the lab. Lab: You will set up your Kali Linux lab environment and write a scope and rules-of-engagement statement for a sample test.	1.5 h
2. Footprinting, scanning and enumeration Footprinting and open-source intelligence, Network scanning, Enumeration of services and users, Documenting findings. Lab: You will gather open-source information on a fictional organization and scan and enumerate a lab network.	3 h
3. Vulnerability analysis, system hacking and malware Vulnerability assessment, Password attacks, Privilege escalation, Malware types and analysis basics, Covering tracks. Lab: You will run a vulnerability scan on a lab host, exploit a known weakness and record how it could have been prevented.	3 h
4. Network and perimeter attacks Sniffing, Social engineering, Denial of service, Session hijacking, Evading firewalls and intrusion detection. Lab: You will capture and analyze lab network traffic, demonstrate a session hijack and propose perimeter defenses.	4 h
5. Web server and web application attacks Web server attacks, Web application vulnerabilities, SQL injection, Input validation and defenses. Lab: You will test a deliberately vulnerable lab web application for SQL injection and write up the fix.	2.5 h

6. Wireless, mobile, IoT and OT attacks

3 h

Wireless encryption and attacks, Mobile platform threats, IoT attack surfaces, Operational technology risks.

Lab: You will assess a sample wireless and IoT environment and produce a risk summary with recommended controls.

7. Cloud security, cryptography and exam review

2 h

Cloud computing threats, Cryptography and PKI, Cryptographic attacks, Exam strategy and practice questions.

Lab: You will encrypt and verify files with public key tools and complete a timed set of practice questions across all domains.

Coaching sessions

1.5 h

1.5 hours of coaching. One-on-one or small-group coaching, scheduled with your coach.

Live online or in-person sessions are available for an additional fee. Email admissions@wecancodeit.org for details.

Provider

We Can Code IT, LLC, 26300 Cedar Rd, Suite 1105, Beachwood, OH 44122. Registered with the Ohio State Board of Career Colleges and Schools, Registration No. 15-03-2064T. Contact: admissions@wecancodeit.org. Syllabus version 2026-10-10.