ATTACK

C|EH

CERTIFIED ETHICAL HACKER

CORE

COURSE DESCRIPTION

The Certified Ethical Hacker (C|EH v10) program is a trusted and respected ethical hacking training program that any information security professional will need. Since its inception in 2003, the Certified Ethical Hacker has been the absolute choice of the industry globally. It is a respected certification in the industry and is listed as a baseline certification on the United States Department of Defense Directive 8570. The C|EH exam is ANSI 17024 compliant adding credibility and value to credential members.

C|EH is used as a hiring standard and is a core sought after certification by many of the Fortune 500 organizations, governments, cybersecurity practices, and a cyber staple in education across many of the most prominent degree programs in top universities around the globe.

Hundreds of thousands of InfoSec professionals as well as career starters have challenged the exam and for those who passed, nearly all are gainfully employed with successful careers. Cyber Security as a profession is evolving, the barrier to entry is rising, the demand for skilled cyber professionals continues to grow demanding a higher level of skill and ability.

This course in its 10th iteration, is updated to provide you with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse you into a “Hacker Mindset” in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver’s seat with a hands-on training environment employing a systematic ethical hacking process.

You are constantly exposed to creative techniques of achieving optimal information security posture in the target organization; by hacking it! You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into reconnaissance, gaining access, enumeration, maintaining access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach and absolutely no other program offers you the breadth of learning resources, labs, tools and techniques than the C|EH v10 program.

WHAT YOU WILL LEARN

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.

- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various cloud computing concepts, threats, attacks, and security techniques and tools.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely.

COURSE OUTLINE

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

C|EH (ANSI)

EXAM TITLE:
Certified Ethical Hacker (ANSI)

EXAM CODE:
312-50 (ECC EXAM), 312-50 (VUE)

NUMBER OF QUESTIONS:
125

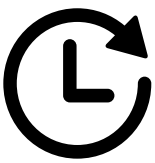
DURATION:
4 hours

AVAILABILITY:
ECCEXAM / VUE

TEST FORMAT:
Multiple Choice

PASSING SORCE:
Please refer to
https://cert.eccouncil.org/faq.html

TARGET AUDIENCE
Ethical hackers, System Administrators, Network Administrators, and Engineers, Webmasters, Aduitors, Security Professionals in general.



COURSE DURATION
5 days (9am - 5pm) | Minimum 40 hours

CERTIFICATION
The C|EH exam can be challenged post the completion of attending the complete official C|EH course. Candidates that successfully passes the exam will recieve their C|EH certificate and membership privileges. Members are expected to adhere to recertification requirements through EC-Council's Continuing Education Requirements.
As powerful addition to the C|EH exam, the new C|EH (Practical) exam is now available adding even more value to the C|EH certification through practical validation of skills and abilities.