ETHICAL HACKING AND COUNTERMEASURES V.10

Well Trained People,
Better Served Customers.

COURSE OVERVIEW

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, but the landscape is changing. Cyber Security as a profession is evolving, the barrier to entry is rising, the demand for Skilled Cyber professionals continues to grow, but it is being refined, demanding a higher level of skill and ability.

DURATION: 40 HRS | EXAM CODE: CEHV10

COURSE PREREQUISITES

- The knowledge and skills that a learner must have before attending this course is as follows:
- Have successfully completed EC-Council's Certified Network Defender (CND) course or
- Have successfully completed Comptia's Security+ (IN-SE) course

There is a minimum age requirement that applies and attendance of the Ethical Hacking and Countermeasures training course or attempts at the relevant exam, is restricted to candidates who are at least 18 years old.

COURSE OBJECTIVE

- 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

- ntroduction 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

TARGET AUDIENCE

Ethical hackers, System Administrators, Network Administrators and Engineers, Webmanagers, Auditors, Security Professionals in general.

SaniSoft
information technologies

410, AL-DANA CENTER, AL MAKTOUM ROAD DEIRA, DUBAI, UAE

+971 55 3575426 +971 4 2238786 training@sanisoft-it.com