# Certified Ethical Hacking v9 (CEH)

Duration 5 Days

## COURSE DESCRIPTION

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment,

This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, “To beat a hacker, you need to think like a hacker”. This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver’s seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can approach your target and succeed at breaking in every time! The ¬five phases include 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 to help you identify when an attack has been used against your own targets. Why then is this training called the Certified Ethical Hacker Course? This is because by using the same techniques as the bad guys, you can assess the security posture of an organization with the same approach these malicious hackers use, identify weaknesses and ¬x the problems before they are identified by the enemy, causing what could potentially be a catastrophic damage to your respective organization.

Throughout the CEH course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

## WHAT WILL YOU LEARN?

Students going through CEH training will learn:

- Key issues plaguing the information security world, incident management process, and penetration testing
- Various types of footprinting, footprinting tools, and countermeasures
- Enumeration techniques and enumeration countermeasures
- Network scanning techniques and scanning 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



NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- 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, jailbreaking iOS, windows phone 8 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

## TARGET AUDIENCE

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.

## CERTIFICATION

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online exam to receive CEH certification.

## OUTLINE

CEHv9 consists of 18 core modules designed to facilitate a comprehensive ethical hacking and penetration testing training.

- **Module 1:** Introduction to Ethical Hacking
- **Module 2:** Footprinting and Reconnaissance
- **Module 3:** Scanning Networks
- **Module 4:** Enumeration
- **Module 5:** System Hacking
- **Module 6:** Malware Threats
- **Module 7:** Sniffing
- **Module 8:** Social Engineering
- **Module 9:** Denial of Service
- **Module 10:** Session Hijacking
- **Module 11:** Hacking Web servers
- **Module 12:** Hacking Web Applications
- **Module 13:** SQL Injection
- **Module 14:** Hacking Wireless Networks
- **Module 15:** Hacking Mobile Platforms
- **Module 16:** Evading IDS, Firewalls, and Honeypot
- **Module 17:** Cloud Computing
- **Module 18:** Cryptography



**NETWORK TRAINING CENTER CO.,LTD. (NTC)** | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th