

# CEH™

## Official Certified Ethical Hacker

### Introduction

The Certified Ethical Hacker (CEH) exam was developed by the International Council of E-Commerce Consultants (EC-Council) to provide an industry-wide means of certifying the competency of security professionals. The CEH certification is granted to those who have attained the level of knowledge and troubleshooting skills needed to provide capable support in the field of computer and network security. The CEH exam is periodically updated to keep the certification applicable to the most recent hardware and software. This is necessary because a CEH must be able to work on the latest equipment. The most recent revisions to the objectives—and to the whole program—were enacted in 2006 and are reflected in this Training.

### What Is CEH Certification?

The CEH certification was created to offer a wide-ranging certification, in the sense that it's intended to certify competence with many different makers/vendors. This certification is designed for security officers, auditors, security professionals, site administrators, and anyone who deals with the security of the network infrastructure on a day-to-day basis. The goal of ethical hackers is to help organizations take preemptive measures against malicious attacks by attacking systems themselves, all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief by thinking like a thief. As technology advances organizations increasingly depend on technology, and information assets have evolved into critical components of survival. You need to pass only a single exam to become a CEH. But obtaining this certification doesn't mean you can provide services to a company—this is just the first step. By obtaining your CEH certification, you'll be able to obtain more experience, build on your interest in networks, and subsequently pursue more complex and in-depth network knowledge and certifications.

### COURSE CONTENT

- Introduction to Ethical Hacking, Ethics, and Legality
- Footprinting and Social Engineering
- Scanning and Enumeration
- System Hacking
- Trojans, Backdoors, Viruses, and Worms
- Sniffers
- Denial of Service and Session Hijacking
- Hacking Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques
- SQL Injection and Buffer Overflows
- Wireless Hacking
- Physical Security
- Linux Hacking
- Evading IDSs, Honeypots, and Firewalls
- Cryptography
- Penetration Testing Methodologies



The Only Way to STOP a  
**HACKER**  
is to Think Like One