

Certified Ethical Hacker (CEH)

- **Course Number:** CEH
- **Length:** 5 Day(s)

Certification Exam

This course will help you prepare for the following exams:

- **Exam 312-50:** Certified Ethical Hacker

Course Overview

The CEH course shows you how to scan, test, hack and secure your own systems. The intensive lab demonstrations give each student in-depth knowledge and practical experience with current security systems. You will begin by understanding how perimeter defenses work and then be lead into scanning and attacking your own networks. You will then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

Prerequisites

Students taking the CEH course should have several years of IT and TCP/IP experience. CompTIA Security+ is also recommended.

Audience

This course is for administrators and other technical professionals who require effective methodologies to protect systems.

Course Outline

- Chapter 1
- Introduction to Ethical Hacking
- Can Hacking be Ethical
- What does a Malicious Hacker Do?
- Classification of Hackers
- What do Ethical Hackers Do?
- Modes of Ethical Hacking
- Chapter 2
- Footprinting
- Revisiting Reconnaissance
- Demo - Sam Spade & VisualRoute
- Demo - Using Google

- Network Range, Traceroute & Tools
- Demo - Email Tracking
- Information Gathering Methodology
- Chapter 3
- Scanning
- War Dialers
- TCP Three Way Handshake
- Demo - SuperScan
- Port Scanning Techniques
- Port Scanning Tools
- Scanning Tools
- Demo - Cheops & nMap
- Chapter 4
- Enumeration
- Net Bios Null Sessions
- Demo - Creating a Null User Session
- Countermeasure to Null Sessions
- Hacking Tools
- Demo - Using SolarWinds
- How to Identify Accounts
- More Hacking Tools
- Demo - Cain Enable
- Chapter 5
- System Hacking
- Password Guessing
- Hacking Tool - KerbCrack
- Demo - LoftCrack
- Privilege Escalation
- Password Cracking
- Demo - Metasploit Project
- SMBRelay
- Man-In-The-Middle Scenario
- More Hacking Tools
- Countermeasures to Installing a Rootkit
- Demo - Using an Alternate Data Stream
- Demo - BlindSide
- Chapter 6
- Trojans & Backdoors
- Backdoors
- Demo - EliteWrap
- Tools
- BOSniffer and FireKiller
- Chapter 7
- Sniffers
- Introduction to Sniffers
- Demo - Ethereal

- Passive & Active Sniffing Programs
- Demo - Using SMAC
- Sniffing HTTPS and SSH
- Demo - Sniffing with Kaine Enable
- Chapter 8
- Denial of Service
- Denial of Service Attacks
- IDS Companies & Firewalls
- Demo - Ping of Death DOS
- Chapter 9
- Social Engineering
- What is Social Engineering?
- Adding Extra Security into your Corporation
- Chapter 10
- Session Hijacking
- Understanding Session Hijacking
- Demo - T-Sight
- Protect against Session Hijacking
- Chapter 11
- Hacking Web Servers
- Hacking Tools & Countermeasures
- Demo - Simple Internet Client Attack
- Unicode Attacks & IIS Log Files
- Directory Traversal Tools
- Demo - N-Stealth Security Scanner
- Hacking Web Servers Review
- Chapter 12
- Web Application Vulnerabilities
- Understanding Web Application Security
- Demo - BlackWidow and BurpSpider
- Hidden Fields
- Demo - Man-In-The-Middle Attack
- XXS Web Application
- Demo - Performing Reconnaissance
- Chapter 13
- Web Based Password Cracking
- Password Guessing
- Demo - SnadBoy's Revelation
- Chapter 14
- SQL Injection
- Shutting Down SQL Server
- Demo - SQL Injection
- SQL Dictionary
- Chapter 15
- Hacking Wireless Networks
- Network Hacking Tools

- Demo - "The Broken" Wireless Hacking & Cracking
- Chapter 16
- IDS, Firewalls & Honey Pots
- Application Protocol Verification
- Demo - Engage Packet Builder
- TCP Replay
- Bypassing Firewalls
- Demo - KFSensor
- IDS, Firewall and Honey Pots Review
- Chapter 17
- Linux Hacking
- Compiling Programs in Linux
- Demo - Nmap Front End
- Linux Hacking Tools
- Linux Hacking Review
- Chapter 18
- Buffer Overflows
- Different Types of Buffer Overflows
- Demo - RPC Exploit
- Preventing Buffer Overflows
- Chapter 19
- Cryptography
- Different Types of Cryptography
- RC5 & Rainbow Tables
- Demo - How to Create Rainbow Tables
- Chapter 20
- Virus and Worms
- Terminologies
- How is a worm different from virus?
- Access Methods & Modes of Infections
- Life Cycle of a Virus
- Writing a Simple Virus Program
- Prevention is Better Than a Cure
- Anti-Virus Software
- Chapter 21
- Physical Security
- Understanding Physical Security
- What is the need of Physical Security?
- Company Surroundings & Premises
- Reception
- Wireless Access Points
- Security of Other Equipment
- Wiretapping, Remote Access & Spying
- Chapter 22
- Penetration Testing
- Penetration Testing Methodology

- Open Source vs Proprietary Methodologies
- Starting Point and Ending Points of Testing
- Selecting the Right Tools
- Penetration Testing Tools
- Gathering Network Information
- Different Types of Threats
- More Tools
- Demo - Nessus Security Analyzer
- Reports and Logs
- Ethical Hacker Course Closure