Certified Ethical Hacker v7

Prepare for the CEH certification while learning the latest ethical hacking techniques.

If you're concerned about the integrity of your network's infrastructure, you need the ethical hacking tools and techniques you will learn in Certified Ethical Hacker (CEH) v7 to enhance your network's defenses. You'll begin by learning how perimeter defenses work. Then, by scanning and attacking your own network (no real networks will be harmed), you'll learn how intruders operate and the steps you can take to secure a system.

In the interactive, lab-filled environment of this ethical hacking course, you will gain in-depth knowledge and practical experience with current, essential security systems. You will explore common ethical hacking topics, such as intrusion detection, policy creation, social engineering, DDoS attacks, buffer overflows, and virus creation.

In addition to learning how to scan, test, hack, and secure a system, you'll prepare for the latest Certified Ethical Hacker exam from EC-Council. A VUE exam voucher is included with your course registration; however, the exam will not be administered in class to allow for maximum discussion opportunities and hands-on activities.

Highlights of CEH v7 include:

- A DVD packed with the latest hacking and security tools and more than 1000 minutes of videos demonstrating hacking techniques
- Diagrams of concepts and attacks for clarity and easier interpretation
- Key industry-standard tools covered in detail
- Exclusive section for countermeasures against different attacks
- Time dedicated to penetration testing
- Results-oriented, descriptive, and analytical lab manual

What You'll Learn

- Footprinting and reconnaissance
- Hacking web servers, web applications, and wireless networks
- Cryptography
- Penetration testing
- Social engineering
- Trojans, viruses, and worms
- Evading IDS, firewalls, and honeypots
- Enumeration
- Buffer overflows

Who Needs to Attend

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

Prerequisites

At least two years of IT security experience and a strong working knowledge of TCP/IP. Security+ Prep Course is highly recommended.

- Security+ Prep Course (SYO-301)

Follow-On Courses

- Foundstone Ultimate Hacking
Certification Programs and Certificate Tracks
This course is part of the following programs or tracks:

CEH - Certified Ethical Hacker

Why Global Knowledge?
Ethical hacking is just a small part of a strong, comprehensive security solution. That's why we offer a full line of security training courses, from foundational, multi-vendor training to technology-specific and vendor-specific training. Our courses will help you understand the basic principles behind protecting and securing your information, applications, and networks.

Our security instructors are seasoned veterans who have spent considerable time in the industry. When they aren't teaching, our instructors spend considerable time on consulting projects, ensuring a thorough understanding of their subject matter and applicable real-world experience.

Course Outline
1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Viruses and Worms
8. Sniffers
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Web Servers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks
16. Evading IDS, Firewalls, and Honeypots
17. Buffer Overflows
18. Cryptography
19. Penetration Testing

Labs
Lab 1: Footprinting and Reconnaissance
  Footprinting a Target Network
  Basic Network Troubleshooting Using the Ping Utility
  Basic Network Troubleshooting Using nslookup Tool
  People Search Using the AnyWhere Online Tool
  Tracing an E-Mail Using the eMailTrackerPro Tool
  Network Route Trace Using Path Analyzer Pro
  Analyzing Domain and IP Address Queries Using SmartWhois

Lab 2: Scanning Networks
  Scanning a Target Network
  Scanning System and Network Resources Using Advanced IP Scanner
  Fingerprinting Open Ports Using the Amap tool
  Monitoring TCP/IP Connections Using the CurrPorts Tool
  Scanning for Network Vulnerabilities Using the GFI Languard Network Scanner
  Exploring and Auditing a Network Using Nmap
  Mapping a Network Using the Lansurveyor Tool
  Scanning a Network Using the Nessus Tool
Identifying Open Ports Using the Unicornscan Tool
Scanning a Network Using Hping3

Lab 3: Enumeration
- Enumerating a Target Network
- Enumerating NetBios Using the SuperScan Tool
- Enumerating Passwords from "Default Password List"
- Enumerating NetBios Using the NetBios Enumerator Tool
- Monitoring a Network Using OpUtils Network Monitoring Tools
- Enumerating a Network Using SoftPerfect Network Scanner

Lab 4: System Hacking
- Extracting Administrator Passwords Using LCP
- Hiding Files Using NTFS Streams
- Find Hidden Files Using ADS Spy
- Hiding Files Using the Masker Stenography Tool
- Extracting Administrator Passwords Using L0phtCrack
- Recover PST (Outlook) Password Using the Passware Recovery Kit Forensic Tool
- Monitoring a System Using the Alchemy Remote Executor
- System Monitoring Using RemoteExec
- Record Keystrokes and Passwords Using Powered Logger

Lab 5: Trojans and Backdoors
- Building a Server Using the Bifrost Tool
- Creating a Server Using the ProRat Tool

Lab 6: Viruses and Worms
- Creating a Virus Using the JSP Virus Maker Tool
- Generating a Worm Using Internet Worm Maker Thing Tool

Lab 7: Sniffers
- Sniffing a Network
- Sniffing the Network Using the Colasoft Packet Builder
- Sniffing the Network Using the OmniPeek Network Analyzer
- Spoofing MAC Address Using SMAC
- Sniffing a Network Using the WinArpAttacker Tool
- Analyzing a Network Using the Colasoft Capsa Network Analyzer
- Sniffing Passwords Using Wireshark
- Performing Man-in-the-Middle Attack using Cain & Abel

Lab 8: Social Engineering
- Detecting Phishing Using Netcraft
- Detecting Phishing Using Phish Tank

Lab 9: Denial of Service
- Creating a Zombie Using Poison Ivy
- SYN Flooding a Target Host Using hping3
- Creating Zombies Using Shark

Lab 10: Session Hijacking
- Hijacking Sessions
- Session Hijacking Using the Paros Proxy
- Hijacking an Established Session Using Firesheep

Lab 11: Hacking Webserver
- Footprinting Webserver Using the httprecon Tool
- Footprinting a Webserver Using ID Serve
- Cracking Remote Passwords Using Brutus
- Hacking Windows Server 2008 with Metasploit Framework

Lab 12: Hacking Web Applications
- Testing Web Applications Using the Burp Suite
- Website Vulnerability Scanning Using Acunetix WVS
Lab 13: SQL Injection
- SQL Injection Attacks on MS SQL Database
- Testing for SQL Injection Using IBM Rational AppScan Tool

Lab 14: Hacking Wireless Networks
- Cracking WEP Using AirPcap with Wireshark and Cain and Abel
- Detecting the Wireless Networks Using NetSurveyor Tool
- Discovering Wireless Networks Using Kismet
- Cracking A WEP Network with Aircrack-ng on Backtrack

Lab 15: Buffer Overflow
- Buffer Overflow Attack
- Enumerating Passwords in "Default Password List"

Lab 16: Cryptography
- Basic Data Encrypting Using HashCalc
- Basic Data Encrypting Using MD5 Calculator
- Basic Data Encrypting Using Advance Encryption Package
- Basic Data Encrypting Using TrueCrypt
- Basic Data Encrypting Using CryptTool