Certified Ethical Hacker Course Overview

Length: 5 Days

Summary: The Certified Ethical Hacking course is a hands-on, five-day intensive workshop immersing students in the concepts, tools, and techniques of ethical hacking. The course includes over 100 lab exercises designed to acquaint students of ethical hacking with the tools and techniques utilized by malicious hackers to attack and compromise information system networks. Course strategy is to impart practical knowledge of these tools and techniques for determination of vulnerabilities in an environment to be protected so that remediation can be applied.

Hacking methodology is presented beginning with the passive and active information gathering techniques that precede actual attack, such as network, port, and wireless scanning, and the fingerprinting of installed applications and operating systems. This is followed by exposure of techniques used to gain privileged access, exercise remote command execution, install backdoor access mechanisms, and hide evidence of the compromise. The network hacking cycle is covered from start to finish with special emphasis given to the countermeasures used to mitigate the various attacks.

Upon completion of this class students will have had hands-on experience applying best of breed security tools in the context of an ethical hacking methodology.

Intended Audience: This course will significantly benefit systems administrators, network administrators, auditors, security professionals, site administrators, or anyone else concerned with the integrity and security of their systems and network infrastructure, as well as those interested in systems and application security. This course is also designed for those interested in taking the EC-Council Certified Ethical Hacker (CEH) exam (312-50).

Course Objective: To familiarize those responsible for the security of information systems with the tools and techniques used by black hat hackers to attack system vulnerabilities for the purpose of ascertaining security weaknesses present so that remediation can be planned and implemented. Skills acquired during the course support initial and ongoing vulnerability assessment and penetration testing of an information systems environment to be protected. These activities are essential for ensuring survivability of public and private enterprises utilizing information technology as an essential element of their operations.

Prerequisites: Familiarity with Windows and Linux command-line interfaces and core TCP/IP protocols, such as TCP and HTTP.

COURSE CONTENT

DAY 1

Introduction to Ethical Hacking

- Terminology
- Hacking History
- Ethical Hacking Objectives and Motivations
- Steps in Malicious Hacking
- Hacker and Ethical Hacker Characteristics and Operations
- Related Types of Computer Crime

Legality and Ethics

- Law and Legal Systems
- Computer Crime Penalties
- Ethics

Penetration Testing for Business

- Penetration Testing from a Business Perspective
- Justification of Penetration Testing through Risk Analysis

- Management Responsibilities in Risk Analysis Relating to Penetration Testing

Footprinting

- Gathering Information
- Locating the Network Range

DAY 2

Scanning

- Identifying Active Machines
- Identifying Open Ports and Available Services
- War Dialing
- War Driving and War Walking
- Fingerprinting
- Mapping the Network

Enumerating

- Protection Rings
- Windows Architecture
- Windows Security Elements
- Enumerating Techniques for Windows
- Countermeasures

System Hacking Techniques

- Password Guessing
- Privilege Escalation
- Password Cracking
- Covering Tracks

Trojans, Backdoors, and Sniffers

- Trojans and Backdoors
- Sniffers

DAY 3

Denial of Service Attacks and Session Hijacking

- Denial of Service/Distributed Denial of Service (Dos/DDoS)
- Session Hijacking

Penetration Testing Steps

- Penetration Testing Overview
- Legal and Ethical Implications
- The Three Pretest Phases
- Penetration Testing Tools and Techniques
- Wireless Network Penetration Testing

Linux Hacking Tools

- Linux History
- Scanning Networks with Linux Tools
- Linux Hacking Tools
- Linux Rootkits
- Linux Security Tools

Social Engineering and Physical Security

- Social Engineering
- Physical Security

DAY 4

SQL Injection Vulnerabilities

- SQL Injection Testing and Attacks
- SQL Injection Prevention and Remediation
- Automated SQL Injection Tools

Cryptography

- Symmetric Key Cryptography
- Public Key Cryptosystems
- Public Key Certificates
- Cryptanalysis
- Managing Encryption Keys
- Email Security
- Electronic Transaction Security
- Wireless Security
- Disk Encryption
- Hacking Tools

Cracking Web Passwords

- Authentication
- Password Considerations and Issues

DAY 5

Wireless Network Attacks and Countermeasures

- Wireless Technology
- The IEEE 802.11 Family
- WLAN Operational Modes

- The Wireless Application Protocol (WAP)
- Wired Equivalent Privacy (WEP)
- WPA and WPA2
- 802.1x and EAP
- WLAN Threats
- Wireless Hacking Tools
- Securing WLANs

Firewalls, Intrusion Detection Systems, and Honeypots

- Firewalls
- Intrusion Detection and Response
- Incident Handling
- Honeypots