Certified Ethical Hacker

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 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 .

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

INTRODUCTION TO ETHICAL HACKING

Information Security Overview
Cyber Kill Chain Concepts
Hacking Concepts
Ethical Hacking Concepts
Information Security Controls
Information Security Laws and Standards

FOOT-PRINTING AND RECONNAISSANCE

Footprinting Concepts
Footprinting through Search Engines
Footprinting through Web Services
Footprinting through Social Networking Sites
Website Footprinting
Email Footprinting
Who is Footprinting
DNS Footprinting
Network Footprinting
Footprinting through Social Engineering
Footprinting Tools
Footprinting Countermeasures

SCANNING NETWORKS
Network Scanning Concepts
Scanning Tools
Host Discovery
Port and Service Discovery
OS Discovery (Banner Grabbing/OS Fingerprinting)
Scanning Beyond IDS and Firewall
Draw Network Diagrams

ENUMERATION
Enumeration Concepts
NetBIOS Enumeration
SNMP Enumeration
LDAP Enumeration
NTP and NFS Enumeration
SMTP and DNS Enumeration
Other Enumeration Techniques
Enumeration Countermeasures

VULNERABILITY ANALYSIS
Vulnerability Assessment Concepts
Vulnerability Classification and Assessment Types
Vulnerability Assessment Solutions and Tools
Vulnerability Assessment Reports

SYSTEM HACKING
System Hacking Concepts
Gaining Access
Escalating Privileges
Maintaining Access
Clearing Logs

MALWARE THREATS
Malware Concepts
APT Concepts
Trojan Concepts
Virus and Worm Concepts
Fileless Malware Concepts
Malware Analysis
Countermeasures
Anti-Malware Software

SNIFFING
Sniffing Concepts
Sniffing Technique: MAC Attacks
Sniffing Technique: DHCP Attacks
Sniffing Technique: ARP Poisoning
Sniffing Technique: Spoofing Attacks
Sniffing Technique: DNS Poisoning
Sniffing Tools
Countermeasures
Sniffing Detection Techniques

SOCIAL ENGINEERING
Social Engineering Concepts
Social Engineering Techniques
Insider Threats
Impersonation on Social Networking Sites
Identity Theft
Countermeasures

DENIAL-OF-SERVICE
DoS/DDoS Concepts
DoS/DDoS Attack Techniques
BotnetsDDoS Case Study
DoS/DDoS Attack Tools
Countermeasures
DoS/DDoS Protection Tools

SESSION HIJACKING
Session Hijacking Concepts
Application Level Session Hijacking
Network Level Session Hijacking
Session Hijacking Tools
Countermeasures

EVADING IDS, FIREWALLS, AND HONEYPOTS
IDS, IPS, Firewall, and Honeypot Concepts
IDS, IPS, Firewall, and Honeypot Solutions
Evading IDS
Evading Firewalls
IDS/Firewall Evading Tools
Detecting Honeypots
IDS/Firewall Evasion Countermeasures

HACKING WEB SERVERS
Web Server Concepts
Web Server Attacks
Web Server Attack Methodology
Web Server Attack Tools
Countermeasures
Patch Management
Web Server Security Tools

HACKING WEB APPLICATIONS
Web Application Concepts
Web Application Threats
Web Application Hacking Methodology
Web API, Webhooks, and Web Shell
Web Application Security

SQL INJECTION
SQL Injection Concepts
Types of SQL Injection
SQL Injection Methodology
SQL Injection Tools
Evasion Techniques
Countermeasures

HACKING WIRELESS NETWORKS
Wireless Concepts
Wireless Encryption
Wireless Threats
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Countermeasures
Wireless Security Tools

HACKING MOBILE PLATFORMS
Mobile Platform Attack Vectors
Hacking Android OS
Hacking iOS
Mobile Device Management
Mobile Security Guidelines and Tools

IOT AND OT HACKING
IoT Hacking
IoT Concepts
IoT Attacks
IoT Hacking Methodology
IoT Hacking Tools
Countermeasures
OT Hacking
OT Concepts
OT Attacks
OT Hacking Methodology
OT Hacking Tools
Countermeasures

CLOUD COMPUTING
Cloud Computing Concepts
Container Technology
Serverless Computing
Cloud Computing Threats
Cloud Hacking
Cloud Security

CRYPTOGRAPHY
Cryptography Concepts
Encryption Algorithms
Cryptography Tools
Public Key Infrastructure (PKI)
Email Encryption
Disk Encryption
Cryptanalysis
Countermeasures