



Ethical Hacking and Countermeasures

Course Description

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students 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. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50

Duration:

50 Hours (1 month)

Certification

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online Prometric exam to receive CEH certification.

Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Course Outline Version 5

Module 1: Introduction to Ethical Hacking

- Why Security?
- Elements of Security
- Types of Hacker Attacks
- Hacker Classes and Ethical Hacking
- How to Become an Ethical Hacker?
- Vulnerability Research Tools
- Ethical Hacking Testing
- Computer Crimes and Implications
- Legal Perspective

Module 3: Scanning

- Definition & Types of Scanning
- Objectives of Scanning
- CEH Scanning Methodology

Module 5: System Hacking

- Cracking Passwords, Escalating Privileges
- Executing applications, Hiding Files, Covering tracks

Module 6: Trojans and Backdoors

- What is a Trojan?
- Indications of a Trojan Attack
- Ports Used by Trojans
- How to Determine which Ports are "Listening"?
- Wrapping Tools
- Packaging Tool: WordPad
- RemoteByMail
- Tool: Icon Plus
- HTTP Trojan (HTTP RAT)
- Shttpd Trojan - HTTP Server
- Reverse Connecting Trojans
- Backdoor Countermeasures
- Tools
- How to Avoid a Trojan Infection?

Module 2: Footprinting

- Defining of Footprinting
- Finding a Company's URL
- Footprinting Through Job Sites
- Passive Information Gathering
- Competitive Intelligence Gathering
- Competitive Intelligence
- Public and Private Websites
- Tools & Steps to Perform Footprinting

Module 4: Enumeration

- Techniques for Enumeration
- Netbios Null Sessions
- Tool
- PStools & SNMP Enumeration
- Management Information Base
- Tools: SNMPutil, Solarwinds, SNScan V1.05, Getif SNMP MIB Browser
- SNMP UNIX Enumeration
- Tools: Winfingerprint, Windows Active Directory Attack Tool, IP Tools Scanner
- Steps to Perform Enumeration

Module 7: Sniffers

- Definition of Sniffing
- Protocols Vulnerable to Sniffing
- ARP - What is Address Resolution Protocol?
- MAC Flooding
- Threats of ARP Poisoning

Module 8: Denial of Service

- What are Denial of Service Attacks?
- Goal of DoS
- DoS Attack Tools
- Botnets
- Characteristics of DDoS Attacks
- Amplification Attack
- Reflective DNS Attacks

- Countermeasures
- Countermeasures

Module 13: Web-based Password Cracking

- Definition of Authentication
- Authentication Mechanisms
- What is a Password Cracker?
- Password Guessing
- Available Password Crackers
- Hacking Tools
- Countermeasures

Getting Out
How to Retrieve any Data?

Module 15: Hacking Wireless Networks

- Wired Network vs. Wireless Network
- Related Technology and Carrier Networks
- Antennas, Cantenna
- Wireless Access Points
- Steps for Hacking Wireless Networks

Module 17: Physical Security

- Security Statistics
- Physical Security Breach Incidents
- Physical Security Checklist
- Information Security
- Wireless Security
- Laptop Theft: Security Statistics
- Tools to Locate Stolen Laptops

Module 19: Evading IDS, Firewalls, and

- Introduction to Intrusion Detection
- Terminologies: Intrusion Detection, Firewall, Honey-pot

Module 20: Buffer Overflow

- Buffer Overflow
- Reasons for
- NOPS
- Tools
- Vulnerability
-

1