



**EC-Council**

# 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

## Who Should 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.

## Duration:

5 days (9:00 – 5:00)

## 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.

## Course Outline Version 6

### Module 1: Introduction to Ethical Hacking

- Problem Definition -Why Security?
- Essential Terminologies
- Elements of Security
- The Security, Functionality and Ease of Use Triangle
- Case Study
- What does a Malicious Hacker do?

### Module 2: Hacking Laws

### **Module 3: Footprinting**

- Revisiting Reconnaissance
- Defining Footprinting
- Why is Footprinting Necessary
- Areas and Information which Attackers Seek
- Information Gathering Methodology

### **Module 4: Google Hacking**

### **Module 5: Scanning**

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

### **Module 6: Enumeration**

- Overview of System Hacking Cycle
- What is Enumeration?
- Techniques for Enumeration
- NetBIOS Null Sessions

### **Module 7: System Hacking**

### **Module 8: Trojans and Backdoors**

- Effect on Business
- What is a Trojan?

### **Module 9: Viruses and Worms**

- Virus History
- Characteristics of Virus
- Working of Virus

### **Module 10: Sniffers**

- Definition - Sniffing
- Protocols Vulnerable to Sniffing
- Tool: Network View – Scans the Network for Devices
- The Dude Sniffer
- Wireshark
- Display Filters in Wireshark
- Following the TCP Stream in Wireshark
- Cain and Abel
- Tcpdump
- Tcpdump Commands
- Types of Sniffing

## **Module 11: Social Engineering**

- What is Social Engineering?
- Human Weakness
- “Rebecca” and “Jessica”
- Office Workers
- Types of Social Engineering

## **Module 12: Phishing**

## **Module 13: Hacking Email Accounts**

## **Module 14: Denial-of-Service**

- Real World Scenario of DoS Attacks
- What are Denial-of-Service Attacks
- Goal of DoS
- Impact and the Modes of Attack
- Types of Attacks
- DoS Attack Classification

## **Module 15: Session Hijacking**

- What is Session Hijacking?
- Spoofing v Hijacking
- Steps in Session Hijacking
- Types of Session Hijacking
- Session Hijacking Levels
- Network Level Hijacking
- The 3-Way Handshake
- TCP Concepts 3-Way Handshake
- Sequence Numbers
- Sequence Number Prediction
- TCP/IP hijacking
- IP Spoofing: Source Routed Packets
- RST Hijacking

## **Module 16: Hacking Web Servers**

- How Web Servers Work
- How are Web Servers Compromised
- Web Server Defacement

## **Module 17: Web Application Vulnerabilities**

- Web Application Setup
- Web application Hacking
- Anatomy of an Attack
- Web Application Threats
- Cross-Site Scripting/XSS Flaws

## **Module 18: Web-Based Password Cracking Techniques**

- Authentication - Definition
- Authentication Mechanisms

## **Module 19: SQL Injection**

- What is SQL Injection
- Exploiting Web Applications
- Steps for performing SQL injection
- What You Should Look For
- What If It Doesn't Take Input
- OLE DB Errors
- Input Validation Attack
- SQL injection Techniques
- How to Test for SQL Injection Vulnerability
- How Does It Work
- BadLogin.aspx.cs
- BadProductList.aspx.cs
- Executing Operating System Commands
- Getting Output of SQL Query
- Getting Data from the Database Using ODBC Error Message
- How to Mine all Column Names of a Table
- How to Retrieve any Data
- How to Update/Insert Data into Database
- SQL Injection in Oracle
- SQL Injection in MySql Database
- Attacking Against SQL Servers
- SQL Server Resolution Service (SSRS)
- Osql -L Probing
- SQL Injection Automated Tools
- Automated SQL Injection Tool: AutoMagic SQL
- Absinthe Automated SQL Injection Tool

## **Module 20: Hacking Wireless Networks**

### **Module 21: Physical Security**

- Security Facts
- Understanding Physical Security
- Physical Security
- What Is the Need for Physical Security
- Who Is Accountable for Physical Security
- Factors Affecting Physical Security
- Physical Security Checklist

### **Module 22: Linux Hacking**

### **Module 23: Evading IDS, Firewalls and Detecting Honey Pots**

## **Module 24: Buffer Overflows**

- Why are Programs/Applications Vulnerable
- Buffer Overflows
- Reasons for Buffer Overflow Attacks
- Knowledge Required to Program Buffer Overflow Exploits
- Understanding Stacks
- Understanding Heaps
- Types of Buffer Overflows: Stack-based Buffer Overflow

## **Module 25: Cryptography**

## **Module 26: Penetration Testing**

## **Module 27: Covert Hacking**

## **Module 28: Writing Virus Codes**

## **Module 29: Assembly Language Tutorial**

## **Module 30: Exploit Writing**

- Exploits Overview
- Prerequisites for Writing Exploits and Shellcodes
- Purpose of Exploit Writing
- Types of Exploits
- Stack Overflow
- Heap Corruption

## **Module 31: Smashing the Stack for Fun and Profit**

- What is a Buffer?
- Static Vs Dynamic Variables
- Stack Buffers
- Data Region
- Memory Process Regions
- What Is A Stack?
- Why Do We Use A Stack?
- The Stack Region
- Stack frame
- Stack pointer
- Procedure Call (Procedure Prolog)
- Compiling the code to assembly
- Call Statement
- Return Address (RET)
- Word Size
- Stack
- Buffer Overflows
- Error
- Why do we get a segmentation violation?
- Segmentation Error
- Instruction Jump

- Guess Key Parameters
- Calculation
- Shell Code

### **Module 32: Windows Based Buffer Overflow Exploit Writing**

### **Module 33: Reverse Engineering**

### **Module 34: MAC OS X Hacking**

- Introduction to MAC OS
- Vulnerabilities in MAC

### **Module 35: Hacking Routers, cable Modems and Firewalls**

### **Module 36: Hacking Mobile Phones, PDA and Handheld Devices**

- Different OS in Mobile Phone
- Different OS Structure in Mobile Phone
- Evolution of Mobile Threat
- Threats
- What Can A Hacker Do
- Vulnerabilities in Different Mobile Phones
- Malware
- Spyware

### **Module 37: Bluetooth Hacking**

- Bluetooth Introduction
- Security Issues in Bluetooth
- Security Attacks in Bluetooth Devices

### **Module 38: VoIP Hacking**

- What is VoIP
- VoIP Hacking Steps
- Footprinting

### **Module 39: RFID Hacking**

### **Module 40: Spamming**

- Introduction
- Techniques used by Spammers
- How Spamming is performed
- Spammer: Statistics
- Worsen ISP: Statistics
- Top Spam Effected Countries: Statistics
- Types of Spam Attacks
- Spamming Tools

### **Module 41: Hacking USB Devices**

### **Module 42: Hacking Database Servers**

- Hacking Database server: Introduction
- Hacking Oracle Database Server

### **Module 43: Cyber Warfare- Hacking, Al-Qaida and Terrorism**

### **Module 44: Internet Content Filtering Techniques**

### **Module 45: Privacy on the Internet**

### **Module 46: Securing Laptop Computers**

- Statistics for Stolen and Recovered Laptops
- Statistics on Security
- Percentage of Organizations Following the Security Measures
- Laptop threats
- Laptop Theft
- Fingerprint Reader
- Protecting Laptops Through Face Recognition
- Bluetooth in Laptops
- Tools

### **Module 47: Spying Technologies**

### **Module 48: Corporate Espionage- Hacking Using Insiders**

- Introduction To Corporate Espionage
- Information Corporate Spies Seek
- Insider Threat
- Different Categories of Insider Threat
- Privileged Access
- Driving Force behind Insider Attack
- Common Attacks carried out by Insiders
- Techniques Used for Corporate Espionage
- Process of Hacking
- Former Forbes Employee Pleads Guilty
- Former Employees Abet Stealing Trade Secrets
- California Man Sentenced For Hacking
- Federal Employee Sentenced for Hacking
- Facts
- Key Findings from U.S Secret Service and CERT Coordination Center/SEI study on Insider Threat
- Tools

### **Module 49: Creating Security Policies**

## **Module 50: Software Piracy and Warez**

## **Module 51: Hacking and Cheating Online Games**

- Online Games: Introduction
- Basics of Game Hacking
- Threats in Online Gaming
- Cheating in Online Computer Games
- Types of Exploits
- Example of popular game exploits
- Stealing Online Game Passwords
  - Stealing Online Game Passwords: Social Engineering and Phishing
- Online Gaming Malware from 1997-2007
- Best Practices for Secure Online Gaming
- Tips for Secure Online Gaming

## **Module 52: Hacking RSS and Atom**

## **Module 53: Hacking Web Browsers (Firefox, IE)**

## **Module 54: Proxy Server Technologies**

## **Module 55: Data Loss Prevention**

## **Module 56: Hacking Global Positioning System (GPS)**

## **Module 57: Computer Forensics and Incident Handling**

## **Module 58: Credit Card Frauds**

## **Module 59: How to Steal Passwords**

## **Module 60: Firewall Technologies**

## **Module 61: Threats and Countermeasures**

## **Module 62: Case Studies**

## **Module 63: Botnets**

## **Module 64: Economic Espionage**

## **Module 65: Patch Management**

## **Module 66: Security Convergence**

## **Module 67: Identifying the Terrorist**

© 2008 EC-Council. All rights reserved.

This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.  
EC-Council logo is registered trademarks or trademarks of EC-Council in the United States and/or other countries.