



BUILDING TRAINING SOLUTIONS  
FOR THE IT WORLD

## Ethical Hacking and Countermeasures

**Days:** 5  
**Format:** Instructor-Led  
**Class Code:** CEH  
**Certification Exams:** 312-50  
**Certification Track:** None

### Recommended Course Sequence

Knowledge of prerequisites  
noted below.

*Course content is subject to change  
without notice.*

### Course Description:

CTREC Hilton IT Academy's course in Ethical Hacking and Countermeasures 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.

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.

### Target Student:

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:

Before attending this class, students should have working knowledge of TCP/IP and Windows 2000.

### Delivery Method:

Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

# Ethical Hacking and Countermeasures

---

## Course Outline

### Module 1: Ethics and Legality

Lessons
<ul style="list-style-type: none"><li>■ Why Security?</li><li>■ The Security, functionality and ease of use Triangle</li><li>■ Can Hacking be Ethical?</li><li>■ Essential Terminology.</li><li>■ Elements of Security.</li><li>■ What does a Malicious Hacker do?</li><li>■ Difference between Penetration Testing and Ethical Hacking.</li><li>■ Hacker Classes.</li><li>■ What do Ethical Hackers do?</li><li>■ Skill Profile of an Ethical Hacker.</li><li>■ Modes of Ethical Hacking.</li><li>■ Security Testing.</li><li>■ Deliverables.</li><li>■ Computer Crimes and Implications.</li><li>■ Legal Perspective (US Federal Laws).</li></ul>

### Module 2: Foot printing

Lessons
<ul style="list-style-type: none"><li>■ Defining Foot printing.</li><li>■ Information Gathering Methodology.</li><li>■ Locate the Network Range.</li><li>■ Hacking Tools</li></ul>

### Module 3: Scanning

Lessons
<ul style="list-style-type: none"><li>■ Definition of Scanning.</li><li>■ Types of scanning</li><li>■ Objectives of Scanning</li><li>■ Scanning Methodology</li><li>■ Classification of Scanning</li><li>■ Hacking Tools</li><li>■ War Dialer</li><li>■ OS Fingerprinting</li><li>■ Active Stack fingerprinting/Tool for Active Stack fingerprinting</li><li>■ Passive Fingerprinting</li><li>■ Proxy Servers/Countermeasures</li></ul>

## Ethical Hacking and Countermeasures

---

### Module 4: Enumeration

Lessons
■ What is Enumeration?
■ NetBIOS Null Sessions
■ Hacking Tools
■ Null Session Countermeasures
■ NetBIOS Enumeration
■ Simple Network Management Protocol (SNMP) Enumeration
■ SNMP Enumeration Countermeasures
■ Management Information Base (MIB)
■ Windows 2000 DNS Zone Transfer
■ Blocking Win 2k DNS Zone Transfer
■ Enumerating User Accounts

### Module 5: System Hacking

Lessons
■ Administrator Password Guessing
■ Manual Password Cracking Algorithm
■ Automated Password Cracking
■ Password Types
■ Types of Password Attacks
■ Performing Automated Password Guessing
■ Hacking Tools
■ Password Sniffing
■ NetBIOS DoS Attack
■ LAN Manager Hash
■ Password Cracking Countermeasures
■ Syskey Utility
■ Cracking NT/2000 Passwords
■ SMB Logon
■ SMBRelay Man-in-the-Middle Scenario
■ SMBRelay Weaknesses and Countermeasures
■ Privilege Escalation
■ Keystroke Loggers
■ Hiding Files
■ Creating Alternate Data Streams
■ ADS creation and detection
■ NTFS Streams Countermeasures
■ Stealing Files Using Word Documents
■ Field Code Countermeasures
■ Steganography
■ Spyware Tool - Desktop Spy
■ Steganography Detection
■ Disabling Auditing and clearing Event Logs
■ RootKit/RootKit Countermeasures
■ Planting the NT/2000 RootKit

## Ethical Hacking and Countermeasures

---

### Module 6: Trojans and Backdoors

Lessons
■ Effect on Business
■ What is a Trojan?
■ Overt and Covert Channels
■ Working of Trojans
■ Different Types of Trojans
■ What Trojan Creators look for?
■ Different ways a Trojan can get into a system
■ Indications of a Trojan Attack
■ Some famous Trojans and ports used by them
■ How to determine which ports are “Listening”?
■ Different Trojans found in the Wild
■ BoSniffer
■ Wrappers
■ Hard Disk Killer (HDKP 4.0)
■ ICMP Tunneling
■ Reverse WWW Shell – Covert Channels using HTTP
■ Hacking Tools
■ Tripwire
■ Process Viewer
■ Insider-Tracks Processes and Ports
■ System File Verification
■ Trojan horse Construction Kit
■ Anti-Trojan
■ Evading Anti-Trojan/Anti-Virus using Stealth Tools v 2.0
■ Reverse Engineering Trojans
■ Backdoor Countermeasures

### Module 7: Sniffers

Lessons
■ Definition of sniffing
■ How a Sniffer works?
■ Passive Sniffing
■ Active Sniffing
■ Man-in-the-Middle Attacks
■ Spoofing and Sniffing Attacks
■ ARP Poisoning and countermeasures
■ Hacking Tools
■ Sniffing Countermeasures

## Ethical Hacking and Countermeasures

---

### Module 8: Denial of Service

Lessons
■ What is Denial of Service?
■ Goal of DoS(Denial of Service)
■ Impact and Modes of Attack
■ DoS Attack Classification
■ Hacking Tools
■ Distributed DOS Attacks and Characteristics
■ Agent Handler Model
■ IRC-Based DDoS Attack Model
■ DDoS Attack taxonomy
■ DDoS Tools
■ Reflected DOS Attacks
■ Reflection of the Exploit
■ Countermeasures for Reflected DoS
■ Tools for Detecting DDOS Attacks
■ DDoS Countermeasures

### Module 9: Social Engineering

Lessons
■ What is Social Engineering?
■ Art of Manipulation
■ Human Weakness
■ Common Types of Social Engineering
■ Human Based Impersonation
■ Computer Based Social Engineering
■ Reverse Social Engineering
■ Policies and procedures
■ Security Policies-checklist

### Module10: Session Hijacking

Lessons
■ Understanding Session Hijacking
■ Spoofing vs Hijacking
■ Steps in Session Hijacking
■ Types of Session Hijacking
■ TCP Concepts 3 Way Handshake
■ Sequence numbers
■ Hacking Tools
■ Dangers Posed by Session Hijacking
■ Protection against Session Hijacking
■ IP Security

## Ethical Hacking and Countermeasures

---

### Module 11: Hacking Web Servers

Lessons
■ How Web Servers Work?
■ How are Web Servers Compromised?
■ Popular Web Servers and Common Security Threats
■ Apache Vulnerability
■ Attack against IIS
■ IIS Components
■ Sample Buffer Overflow Vulnerabilities
■ ISAPI.DLL Exploit
■ Code Red and ISAPI.DLL Exploit
■ Unicode Directory Traversal Vulnerability
■ Hacking Tools
■ Msw 3prt IPP Vulnerability
■ IPP Buffer Overflow Countermeasures
■ Unspecified Executed Path Vulnerability
■ File System Traversal Countermeasures
■ WebDAV/ ntdll.dll Vulnerability
■ Real World instance of WebDAV Exploit
■ RPCDCOM Vulnerability
■ ASN Exploits
■ IIS Logs
■ Escalating Privileges on IIS
■ Hot Fixes and Patches
■ Cacls.exe Utility
■ Vulnerability Scanners
■ Network Tools
■ Countermeasures
■ Increasing Web Server Security

### Module 12: Web Application Vulnerabilities

Lessons
■ Web Application Set-up
■ Web Application Hacking
■ Anatomy of an Attack
■ Web Application Threats
■ Cross Site Scripting/XSS Flaws
■ SQL Injection
■ Command Injection Flaws
■ Cookie/Session Poisoning
■ Parameter/Form Tampering
■ Buffer Overflow
■ Directory Traversal/Forceful Browsing
■ Cryptographic Interception
■ Authentication Hijacking
■ Log Tampering

## Ethical Hacking and Countermeasures

---

- Error Message Interception
- Attack Obfuscation
- Platform Exploits
- Internet Explorer Exploits
- DMZ Protocol Attacks
- Security Management Exploits
- Web Services Attacks
- Zero Day Attacks
- Network Access Attacks
- TCP Fragmentation
- Hacking Tools

### Module 13: Web Based Password Cracking Techniques

#### Lessons

- Authentication- Definition
- Authentication Mechanisms
- HTTP Authentication
- Basic Authentication
- Digest Authentication
- Integrated Windows (NTLM) Authentication
- Negotiate Authentication
- Certificate-based Authentication
- Forms-based Authentication
- Microsoft Passport Authentication
- What is a Password Cracker?
- Modus Operandi of an Attacker using Password Cracker
- How does a Password Cracker work?
- Attacks- Classification
- Password Guessing
- Query String
- Cookies
- Dictionary Maker
- Password Crackers Available
- Hacking Tools
- “Mary had a Little Lamb” Formula

### Module 14: SQL Injection

#### Lessons

- Attacking SQL Servers
- SQL Server Resolution Service (SSRS)
- Osql-L Probing
- Port Scanning
- Sniffing, Brute Forcing and finding Application Configuration Files
- Tools for SQL Server Penetration Testing

## Ethical Hacking and Countermeasures

---

- OLE DB Errors
- Input Validation Attack
- Login Guessing & Insertion
- Shutting Down SQL Server
- Extended Stored Procedures
- SQL Server Talks
- Preventive Measures

### Module 15: Hacking Wireless Networks

#### Lessons

- Introduction to Wireless Networking
- Business and Wireless Attacks
- Wireless Basics
- Components of Wireless Network
- Types of Wireless Network
- Setting up WLAN
- Detecting a Wireless Network
- How to access a WLAN
- Advantages and Disadvantages of Wireless Network
- Antennas
- SSIDs
- Access Point Positioning
- Rogue Access Points
- Tools to Generate Rogue Access Points
- What is Wireless Equivalent Privacy (WEP)?
- WEP Tool
- Related Technology and Carrier Networks
- MAC Sniffing and AP Spoofing
- Tool to detect MAC Address Spoofing: Wellenreiter v2
- Terminology
- Denial of Service Attacks
- DoS Attack Tool: FATAjack
- Man-in-the-Middle Attack (MITM)
- Scanning Tools
- Sniffing Tools
- WIDZ- Wireless Detection Intrusion System
- Securing Wireless Networks
- Out of the box Security
- Radius: Used as Additional layer in security
- Maximum Security: Add VPN to Wireless LAN

## Ethical Hacking and Countermeasures

---

### Module 16: Virus and Worms

Lessons
■ Virus Characteristics
■ Symptoms of ‚virus-like’ attack
■ What is a Virus Hoax?
■ Terminologies
■ How is a worm different from virus?
■ Indications of a Virus Attack
■ Virus History
■ Virus damage
■ Effect of Virus on Business
■ Access Methods of a Virus
■ Mode of Virus Infection
■ Life Cycle of a virus
■ What Virus Infect?
■ How virus infect?
■ Virus/worm found in the wild
■ Writing a simple virus program.
■ Writing DDOS Zombie Virus
■ Virus Construction Kits
■ Virus Creation Scripts
■ Virus Detection Methods
■ Virus Incident Response
■ What is Sheep Dip?
■ Prevention is better than Cure
■ Anti-Virus Software
■ Popular Anti-Virus packages
■ New Virus found in 2004
■ Virus Checkers
■ IDAPro
■ Virus Analyzers

### Module 17: Physical Security

Lessons
■ Security statistics
■ Physical Security breach incidents
■ Understanding Physical Security
■ What is the need of Physical Security?
■ Who is Accountable for Physical Security?
■ Factors affecting Physical Security
■ Physical Security checklist
■ Lock Picking Techniques
■ Spying Technologies

## Ethical Hacking and Countermeasures

---

### Module 18: Linux Hacking

Lessons
■ Why Linux?
■ Linux basics
■ Chrooting
■ Why is Linux Hacked?
■ Linux Vulnerabilities in 2003
■ How to apply patches to vulnerable programs
■ Scanning Networks
■ Cheops
■ Port Scan detection tools
■ Password cracking in Linux.
■ Password cracking tools
■ IPChains
■ IPTables
■ IPChains vs. IPfwadm
■ How to Organize Firewall Rules
■ Security Auditor's Research Assistant (SARA)
■ Hacking Tools
■ Linux Loadable Kernel Modules
■ Linux RootKit
■ RootKit countermeasures
■ Linux Security Tools
■ Advanced Intrusion Detection System (AIDE)
■ Linux Security testing tools
■ Linux Encryption Tools
■ Linux Security Auditing Tool (LSAT)
■ Linux Security countermeasures• Modes of Ethical Hacking.
■ Security Testing.
■ Deliverables.
■ Computer Crimes and Implications.
■ Legal Perspective (US Federal Laws).

### Module 19: Evading Firewalls, IDS and Honeypots

Lessons
■ Intrusion Detection Systems
■ Ways to Detect Intrusion
■ Types of Intrusion Detection System
■ Intrusion Detection Tools
■ Steps to perform after an IDS detects an intrusion
■ Evading IDS systems
■ Tools to Evade IDS
■ Packet Generators
■ Introduction to Firewalls
■ Firewall Identification

## Ethical Hacking and Countermeasures

---

- Fire walking
- Banner Grabbing
- Breaching Firewalls
- Placing Backdoors through Firewalls
- Hiding Behind Covert Channel: Loki
- ACK tunneling
- Tools to Breach Firewall
- Tools for testing IDS and Firewalls
- Introduction to Honeypots
- Honeypot Project
- Types of Honeypots
- Hacking Tool
- Tools to Detect Honeypot

### Module 20: Buffer Overflows

Lessons
■ Significance of Buffer Overflow Vulnerability
■ Why are Programs/Applications Vulnerable?
■ Reasons for Buffer Overflow Attacks
■ Knowledge required writing Buffer Overflow Exploits
■ How a Buffer Overflow occurs?
■ Understanding Stacks
■ Stack Implementation
■ Stack based buffer overflow
■ Shellcode
■ Heap Based buffer overflow
■ How to detect Buffer Overflows in a Program?
■ Attacking a real program
■ NOPS
■ How to mutate a Buffer Overflow Exploit? featuring ADMutate
■ Return Address Defender (RAD)
■ StackGuard
■ Immunix System
■ Vulnerability Search - ICAT

## Ethical Hacking and Countermeasures

---

### Module 21: Cryptography

Lessons
■ Public-key Cryptography
■ Working of Encryption
■ Digital Signature
■ Digital Certificate
■ RSA (Rivest Shamir Adleman)
■ RSA Attacks
■ MD5
■ SHA (Secure Hash Algorithm)
■ SSL (Secure Socket Layer)
■ RC5
■ What is SSH?
■ Government Access to Keys (GAK)
■ RSA Challenge
■ Distributed.net
■ PGP (Pretty Good Privacy)
■ Code Breaking Methodologies
■ Cryptography Attacks
■ Disk Encryption
■ PGPCrack
■ Magic Lantern
■ WEPCrack
■ Cracking S/MIME Encryption using idle CPU Time
■ CypherCalc
■ Command Line Scriptor
■ CryptoHeaven

### Module 22: Penetration Testing

Lessons
■ Need for a Methodology
■ Penetration Test vs. Vulnerability Test
■ Reliance on Checklists and Templates
■ Phases of Penetration Testing
■ Passive Reconnaissance
■ Best Practices
■ Results that can be expected
■ Indicative passive reconnaissance steps include (but are not limited to)
■ Introduction to Penetration Testing
■ Type of Penetration Testing Methodologies
■ Open Source Vs Proprietary Methodologies
■ Security Assessment Vs Security Auditing
■ Risk Analysis
■ Types of Penetration Testing
■ Types Ethical Hacking

## Ethical Hacking and Countermeasures

---

- Vulnerability Assessment Vs Penetration Testing
- Do-it Yourself Testing
- Firms Offering Penetration Testing Services
- Penetration Testing Insurance
- Explication of Terms of Engagement
- Pen-Test Service Level Agreements
- Offer of Compensation
- Starting Point and Ending Points of Testing
- Penetration Testing Locations
- Black Box Testing/ White Box Testing/ Grey Box Testing
- Manual Penetration Testing
- Automated Penetration Testing
- Selecting the Right Tools
- Evaluating Different Types of Pen-Test Tools
- Platform on Which Tools Will be Used
- Asset Audit
- Fault Tree and Attack Trees
- GAP Analysis
- Device Inventory
- Perimeter Firewall Inventory
- Web Server Inventory
- Load Balancer Inventory
- Local Area Network Inventory
- Demilitarized Zone Firewall
- Internal Switch Network Sniffer
- Application Server Inventory
- Database Server Inventory
- Name Controller and Domain Name Server
- Physical Security
- ISP Routers
- Legitimate Network Traffic Threat
- Unauthorized Network Traffic Threat
- Unauthorized Running Process Threat
- Loss of Confidential Information
- Business Impact of Threat
- Pre-testing Dependencies/Post-testing Dependencies
- Failure Management
- Test Documentation Processes
- Penetration Testing Tools
- SANS Institute TOP 20 Security Vulnerabilities
- All Operating System Platforms
- Windows-specific
- UNIX-specific
- Penetration Testing Deliverable Templates
- Active Reconnaissance
- Attack Phase/Post Attack Phase & Activities