

## Certified Ethical Hacker Training (CEH)

### 5 Days

**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

**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.

### Certification

The Certified Ethical Hacker certification exam 312-50 can be optionally taken by participants. 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.

### Prerequisites

- Administering Windows 2000 Servers
- TCP/IP Technical background
- NetBIOS and Windows file sharing
- DNS, WINS and DHCP
- NTFS and File Permissions
- Linux basics skills
- Linux Configuring IP address
- Linux Configuring Routing
- Linux Compiling and running programs

[Do I really need Linux?](#)

### Course Contents

## Module 1: Ethics and Legality

What is an Exploit?  
The security functionality triangle  
The attacker's process  
Passive reconnaissance  
Active reconnaissance  
Types of attacks  
Categories of exploits  
Goals attackers try to achieve  
Ethical hackers and crackers - who are they  
Self proclaimed ethical hacking  
Hacking for a cause (Hacktivism)  
Skills required for ethical hacking  
Categories of Ethical Hackers  
What do Ethical Hackers do?  
Security evaluation plan  
Types of Ethical Hacks  
Testing Types  
Ethical Hacking Report  
Cyber Security Enhancement Act of 2002  
Computer Crimes  
Overview of US Federal Laws  
Section 1029  
Section 1030  
Hacking Punishment

## Module 2: Footprinting

What is Footprinting  
Steps for gathering information  
Whois  
<http://tucows.com>  
Hacking Tool: Sam Spade  
Analyzing Whois output  
NSLookup  
Finding the address range of the network  
ARIN  
Traceroute  
Hacking Tool: NeoTrace  
Visual Route  
Visual Lookout  
Hacking Tool: Smart Whois  
Hacking Tool: eMailTracking Pro  
Hacking Tool: MailTracking.com

## Module 3: Scanning

Determining if the system is alive?  
Active stack fingerprinting  
Passive stack fingerprinting  
Hacking Tool: Pinger  
Hacking Tool: Friendly Pinger  
Hacking Tool: WS\_Ping\_Pro  
Hacking Tool: Netscan Tools Pro 2000  
Hacking Tool: Hping2  
Hacking Tool: KingPing  
Hacking Tool: icmpenum  
Hacking Tool: SNMP Scanner  
Detecting Ping sweeps  
ICMP Queries  
Hacking Tool: netcraft.com  
Port Scanning  
TCPs 3-way handshake  
TCP Scan types  
Hacking Tool: IPEye  
Hacking Tool: IPSECSCAN  
Hacking Tool: nmap  
Port Scan countermeasures

Hacking Tool: HTTrack Web Copier  
Network Management Tools  
SolarWinds Toolset  
NeoWatch  
War Dialing  
Hacking Tool: THC-Scan  
Hacking Tool: PhoneSweep War Dialer  
Hacking Tool: Telesweep  
Hacking Tool: Queso  
Hacking Tool: Cheops  
Proxy Servers  
Hacking Tool: SocksChain  
Surf the web anonymously  
TCP/IP through HTTP Tunneling  
Hacking Tool: HTTPort  
Hacking Tool: Tunneld  
Hacking Tool: BackStealth

## Module 4: Enumeration

What is Enumeration  
NetBios Null Sessions  
Null Session Countermeasures  
NetBIOS Enumeration  
Hacking Tool: DumpSec  
Hacking Tool: Hyena  
Hacking Tool: NAT  
SNMP Enumeration  
SNMPUtil  
Hacking Tool: IP Network Browser  
SNMP Enumeration Countermeasures  
Windows 2000 DNS Zone transfer  
Identifying Win2000 Accounts  
Hacking Tool: User2SID  
Hacking Tool: SID2User  
Hacking Tool: Enum  
Hacking Tool: UserInfo  
Hacking Tool: GetAcct  
Hacking Tool: smbfbf  
SMB Auditing Tools  
Active Directory Enumeration  
W2K Active Directory attack

## Module 5: System Hacking

Administrator Password Guessing  
Performing Automated Password Guessing  
Legion  
NTInfoScan  
Defending Against Password Guessing  
Monitoring Event Viewer Logs  
VisualLast  
Eavesdroppin on Network Password Exchange  
Hacking Tool: L0phtCrack  
Hacking Tool: KerbCrack  
Privilege Escalation  
Hacking Tool: GetAdmin  
Hacking Tool: hk  
Manual Password Cracking Algorithm  
Automatic Password Cracking Algorithm  
Password Types  
Types of Password Attacks  
Dictionary Attack  
Brute Force Attack  
Distributed Brute Force Attack  
Password Change Interval  
Hybrid Attack  
Cracking Windows 2000 Passwords  
Retrieving the SAM file

Redirecting SMB Logon to the Attacker  
SMB Redirection  
Hacking Tool: SMBRelay  
Hacking Tool: SMBRelay2  
Hacking Tool: pwdump2  
Hacking Tool: SAMdump  
Hacking Tool: C2MYAZZ  
Win32 Create Local Admin User  
Offline NT Password Resetter  
Hacking Tool: psexec  
Hacking Tool: remexec  
SMBRelay Man-in-the-Middle (MITM)  
SMBRelay MITM Countermeasures  
Hacking Tool: SMBGrinder  
Hacking Tool: SMBDie  
Hacking Tool: NBTDeputy  
NetBIOS DoS Attack  
Hacking Tool: nbname  
Hacking Tool: John the Ripper  
LanManager Hash  
Password Cracking Countermeasures  
Keystroke Logger  
Hacking Tool: Spector  
AntiSpector  
Hacking Tool: eBlaster  
Hacking Tool: SpyAnywhere  
Hacking Tool: IKS Software Logger  
Hacking Tool: Fearless Key Logger  
Hacking Tool: E-mail Keylogger  
Hardware Tool: Hardware Key Logger  
Hacking Tool: Rootkit  
Planting Rootkit on Windows 2000 Machine  
\_rootkit\_ embedded TCP/IP Stack  
Rootkit Countermeasures  
MD5 Checksum utility  
Tripwire  
Covering Tracks  
Disabling Auditing  
Auditpol  
Clearing the Event Log  
Hacking Tool: Elslave  
Hacking Tool: Winzapper  
Hacking Tool: Evidence Eliminator  
Hiding Files  
NTFS File Streaming  
Hacking Tool: makestrm  
NTFS Streams Countermeasures  
LNS  
Steganography  
Hacking Tool: ImageHide  
Hacking Tool: BlindSide  
Hacking Tool: MP3Stego  
Hacking Tool: Snow  
Hacking Tool: Camera/Shy  
Steganography Detection  
StegDetect  
Hacking Tool: Stealth Files  
Encrypted File System  
Hacking Tool: dskprobe  
Hacking Tool: EFSView  
Buffer Overflows  
Creating Buffer Overflow Exploit  
Outlook Buffer Overflow  
Hacking Tool: Outoutlook

## Module 6: Trojans and Backdoors

What is a Trojan Horse?  
Overt and Covert

Hacking Tool: QAZ  
Hacking Tool: Tini  
Hacking Tool: Netcat  
Hacking Tool: Donald Dick  
Hacking Tool: SubSeven  
Hacking Tool: BackOrifice 2000  
Back Orifice Plug-ins  
BoSniffer  
Hacking Tool: NetBus  
ComputerSpy Key Logger  
Hacking Tool: Beast Trojan  
Hacking Tool: CyberSpy Telnet Trojan  
Hacking Tool: SubRoot Telnet Trojan  
Hacking Tool: LetMeRule  
Wrappers  
Hacking Tool: Graffiti  
Hacking Tool: Silk Rope 2000  
Hacking Tool: EliteWrap  
Hacking Tool: IconPlus  
Packaging Tool: Microsoft WordPad  
Hacking Tool: Whack a Mole  
Trojan Construction Kit  
Writing Trojans in Java  
Hacking Tool: FireKiller 2000  
Covert Channels  
ICMP Tunneling  
Hacking Tool: Loki  
Reverse WWW Shell  
Backdoor Countermeasures  
BO Startup and Registry Entries  
NetBus Startup and Registry Keys  
Port Monitoring Tools  
fPort  
TCPView  
Process Viewer  
Inzider - Tracks Processes and Ports  
Trojan Maker  
Hacking Tool: Hard Disk Killer  
Man-in-the-Middle Attack  
Hacking Tool: dsniff  
System File Verification  
TripWire

## Module 7: Sniffers

What is a Sniffer?  
Hacking Tool: Ethereal  
Hacking Tool: Snort  
Hacking Tool: WinDump  
Hacking Tool: EtherPeek  
Passive Sniffing  
Active Sniffing  
Hacking Tool: EtherFlood  
How ARP Works?  
Hacking Tool: ArpSpoof  
Hacking Tool: DSNIFF  
Hacking Tool: Macof  
Hacking Tool: mailsnarf  
Hacking Tool: URLsnarf  
Hacking Tool: Webspay  
Hacking Tool: Ettercap  
Hacking Tool: WebMiTM  
IP Restrictions Scanner  
Hacking Tool: sTerm  
Hacking Tool: Cain and Abel  
Hacking Tool: Packet Crafter  
Hacking Tool: SMAC  
MAC Changer  
ARP Spoofing Countermeasures

Hacking Tool: WinDNSSpoof  
Hacking Tool: Distributed DNS Flooder  
Hacking Tool: WinSniffer  
Network Tool: IRIS  
Network Tool: NetInterceptor  
SniffDet  
Hacking Tool: WinTCPKill

## **Module 8: Denial of Service**

What is Denial of Service Attack?  
Types of DoS Attacks  
How DoS Work?  
What is DDoS?  
Hacking Tool: Ping of Death  
Hacking Tool: SSPing  
Hacking Tool: Land  
Hacking Tool: Smurf  
Hacking Tool: SYN Flood  
Hacking Tool: CPU Hog  
Hacking Tool: Win Nuke  
Hacking Tool: RPC Locator  
Hacking Tool: Jolt2  
Hacking Tool: Bubonic  
Hacking Tool: Targa  
Tools for Running DDoS Attacks  
Hacking Tool: Trinoo  
Hacking Tool: WinTrinoo  
Hacking Tool: TFN  
Hacking Tool: TFN2K  
Hacking Tool: Stacheldraht  
Hacking Tool: Shaft  
Hacking Tool: mstream  
DDoS Attack Sequence  
Preventing DoS Attack  
DoS Scanning Tools  
Find\_ddos  
SARA  
DDoSPing  
RID  
Zombie Zapper

## **Module 9: Social Engineering**

What is Social Engineering?  
Art of Manipulation  
Human Weakness  
Common Types of Social Engineering  
Human Based Impersonation  
Important User  
Tech Support  
Third Party Authorization  
In Person  
Dumpster Diving  
Shoulder Surfing  
Computer Impersonation  
Mail Attachments  
Popup Windows  
Website Faking  
Reverse Social Engineering  
Policies and Procedures  
Social Engineering Security Policies  
The Importance of Employee Education

## **Module 10: Session Hijacking**

What is Session Hijacking?  
Session Hijacking Steps  
Spoofing Vs Hijacking

Active Session Hijacking  
Passive Session Hijacking  
TCP Concepts - 3 way Handshake  
Sequence Numbers  
Sequence Number Example  
Guessing the Sequence Numbers  
Hacking Tool: Juggernaut  
Hacking Tool: Hunt  
Hacking Tool: TTYWatcher  
Hacking Tool: IP Watcher  
Hacking Tool: T-Sight  
Remote TCP Session Reset Utility  
Dangers Posed by Session Hijacking  
Protection against Session Hijacking

## **Module 11: Hacking Web Servers**

Apache Vulnerability  
Attacks against IIS  
IIS Components  
ISAPI DLL Buffer Overflows  
IPP Printer Overflow  
msw3prt.dll  
Oversized Print Requests  
Hacking Tool: Jill32  
Hacking Tool: IIS5-Koei  
Hacking Tool: IIS5Hack  
IPP Buffer Overflow Countermeasures  
ISAPI DLL Source Disclosure  
ISAPI.DLL Exploit  
Defacing Web Pages  
IIS Directory Traversal  
Unicode  
Directory Listing  
Clearing IIS Logs  
Network Tool: LogAnalyzer  
Attack Signature  
Creating Internet Explorer (IE) Trojan  
Hacking Tool: IISExploit  
Hacking Tool: UnicodeUploader.pl  
Hacking Tool: cmdasp.asp  
Escalating Privileges on IIS  
Hacking Tool: IISCrack.dll  
Hacking Tool: ispc.exe  
IIS WebDav Vulnerability  
Hacking Tool: WB  
RPC Exploit-GUI  
Hacking Tool: DComExpl\_UnixWin32  
Hacking Tool: Plonk  
Unspecified Executable Path Vulnerability  
Hacking Tool: CleanIISLog  
File System Traversal Countermeasures  
Microsoft HotFix Problems  
UpdateExpert  
Cacls utility  
Network Tool: Whisker  
N-Stealth Scanner  
Hacking Tool: WebInspect  
Network Tool: Shadow Security Scanner

## **Module 12: Web Application Vulnerabilities**

Documenting the Application Structure  
Manually Inspecting Applications  
Using Google to Inspect Applications  
Directory Structure  
Hacking Tool: Instant Source  
Java Classes and Applets  
Hacking Tool: Jad

HTML Comments and Contents  
Hacking Tool: Lynx  
Hacking Tool: Wget  
Hacking Tool: Black Widow  
Hacking Tool: WebSleuth  
Cross Side Scripting  
Session Hijacking using XSS  
Cookie Stealing  
Hacking Tool: IEEN  
Hacking Tool: IEflaw  
Exposing Sensitive Data with Google

### **Module 13: Web Based Password Cracking Techniques**

Basic Authentication  
Message Digest Authentication  
NTLM Authentication  
Certificate based Authentication  
Digital Certificates  
Microsoft Passport Authentication  
Forms based Authentication  
Creating Fake Certificates  
Hacking Tool: WinSSLMiM  
Password Guessing  
Default Account Database  
Hacking Tool: WebCracker  
Hacking Tool: Brutus  
Hacking Tool: ObiWan  
Hacking Tool: Munga Bunga  
Password dictionary Files  
Attack Time  
Hacking Tool: Variant  
Hacking Tool: PassList  
Query Strings  
Post data  
Hacking Tool: cURL  
Stealing Cookies  
Hacking Tool: CookieSpy  
Hacking Tool: ReadCookies  
Hacking Tool: SnadBoy

### **Module 14: SQL Injection**

What is SQL Injection Vulnerability?  
SQL Insertion Discovery  
Blank sa Password  
Simple Input Validation  
SQL Injection  
OLE DB Errors  
1=1  
blah' or 1=1  
Preventing SQL Injection  
Database Specific SQL Injection  
Hacking Tool: SQLDict  
Hacking Tool: SQLExec  
Hacking Tool: SQLbf  
Hacking Tool: SQLSmack  
Hacking Tool: SQL2.exe  
Hacking Tool: Oracle Password Buster

### **Module 15: Hacking Wireless Networks**

802.11 Standards  
What is WEP?  
Finding WLANs  
Cracking WEP keys  
Sniffing Traffic  
Wireless DoS Attacks

WLAN Scanners  
WLAN Sniffers  
MAC Sniffing  
Access Point Spoofing  
Securing Wireless Networks  
Hacking Tool: NetTumbler  
Hacking Tool: AirSnort  
Hacking Tool: AiroPeek  
Hacking Tool: WEP Cracker  
Hacking Tool: Kismet  
Hacking Tool: AirSnarf  
WIDZ- Wireless IDS

### **Module 16: Virus and Worms**

Cherobyl  
ExploreZip  
I Love You  
Melissa  
Pretty Park  
Code Red Worm  
W32/Klez  
BugBear  
W32/Opaserv Worm  
Nimda  
Code Red  
SQL Slammer  
Batch File Virus Creator  
How to write your own Virus?  
Worm Construction Kits

### **Module 17: Novell Hacking**

Common accounts and passwords  
Accessing password files  
Password crackers  
Netware Hacking Tools  
Chknull  
NOVELBFH  
NWPCRAK  
Bindery  
BinCrack  
SETPWD.NLM  
Kock  
userdump  
Burglar  
Getit  
Spooftlog  
Gobbler  
Novelffs  
Pandora

### **Module 18: Linux Hacking**

Why Linux ?  
Linux Basics  
Compiling Programs in Linux  
Scanning Networks  
Mapping Networks  
Password Cracking in Linux  
Linux Vulnerabilities  
SARA  
TARA  
Sniffing  
A Pinger in Disguise  
Session Hijacking  
Linux Rootkits  
Linux Security Countermeasures  
IPChains and IPTables

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

- Intrusion Detection System
- System Integrity Verifiers
- How are Intrusions Detected?
- Anomaly Detection
- Signature Recognition
- How does IDS match Signatures with Incoming Traffic?
- Protocol Stack Verification
- Application Protocol Verification
- What Happens after an IDS Detects an Attack?
- IDS Software Vendors
- SNORT
- Evading IDS (Techniques)
- Complex IDS Evasion
- Hacking Tool: fragrouter
- Hacking Tool: TCPReplay
- Hacking Tool: SideStep
- Hacking Tool: NIDSbench
- Hacking Tool: ADMutate
- IDS Detection
- Tools to Detect Packet Sniffers
- Tools to inject strangely formatted packets onto the wire
- Hacking Through Firewalls
- Placing Backdoors through Firewalls
- Hiding behind Covert Channels
- Hacking Tool: Ncovert
- What is a Honeypot?
- Honeypots Evasion
- Honeypots vendors
- Hacking Tool: Honeyd

## **Module 20: Buffer Overflows**

- What is a Buffer Overflow?
- Exploitation
- Assembly Language Basics
- How to Detect Buffer Overflows in a Program?
- Skills Required
- CPU/OS Dependency
- Understanding Stacks
- Stack Based Buffer Overflows
- Buffer Overflow Technical Implementation

- Writing your own Buffer Overflow Exploit in C
- Defense against Buffer Overflows
- Type Checking Tools for Compiling Programs
- StackGuard
- Immunix

## **Module 21: Cryptography**

- What is PKI?
- Digital Certificates
- RSA
- MD-5
- RC-5
- SHA
- SSL
- PGP
- SSH
- Encryption Cracking Techniques

## **Module 22: Penetration Testing Methodologies**

- Physical Security Testing
- Port Scanning Testing
- System Identification Testing
- Services Identification Testing
- Vulnerability Research and Verification Testing
- Application Testing and Source Code Review
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Domain Trusted Systems Testing
- Application Password Cracking Testing
- Denial of Service Testing
- Containment Measures Testing
- Information Security
- Document Grinding
- Gathering Competitive Intelligence
- Social Engineering Testing
- Wireless Networks Testing
- Cordless Communications Testing
- Infrared Systems Testing
- Modem Testing
- Writing Penetration Testing Reports