

Certified Ethical Hacker

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.

Prerequisites: 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.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Understand how intruders escalate privileges and what steps can be taken to secure a system.
- Understand Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Understand Ethical Hacking.

Course Outline:

Introduction to Ethical Hacking

Why Security?
Essential Terminologies
Elements of Security
The Security, Functionality, and Ease of Use Triangle
What Does a Malicious Hacker Do?
Types of Hacker Attacks
Operating System attacks
Application-level attacks
Shrink Wrap code attacks
Misconfiguration attacks
Hacktivism
Hacker Classes
Hacker Classes and Ethical Hacking
What Do Ethical Hackers Do?
Can Hacking be Ethical?
How to Become an Ethical Hacker?
Skill Profile of an Ethical Hacker
What is Vulnerability Research?
Why Hackers Need Vulnerability Research?
Vulnerability Research Tools
Vulnerability Research Websites
How to Conduct Ethical Hacking?
Approaches to Ethical Hacking
Ethical Hacking Testing
Ethical Hacking Deliverables
Computer Crimes and Implications
Legal Perspective

Footprinting

Revisiting Reconnaissance
Defining of Footprinting
Information Gathering Methodology
Unearthing Initial Information
Finding a Company's URL
Internal URL
Extracting Archive Of a Website
Google Search for Company's Info.
People Search
Footprinting Through Job Sites
Passive Information Gathering
Competitive Intelligence Gathering
Why Do You Need Competitive Intelligence?
Companies Providing Competitive Intelligence Services
Competitive Intelligence
Public and Private Websites
Tools
Whois
Nslookup
Necrosoft
ARIN
Traceroute
Neo Trace
GEOSpider
Geowhere
GoogleEarth

VisualRoute Trace
Kartoo Search Engine
Touchgraph Visual Browser
SmartWhois
VisualRoute Mail Tracker
eMailTrackerPro
Read Notify
HTTrack Web Site Copier
Web Ripper
robots.txt
Website watcher
E-mail Spider
Power E-mail Collector Tool
Steps to Perform Footprinting

Scanning

Definition of Scanning
Types of Scanning
Port Scanning
Network Scanning
Vulnerability Scanning
Objectives of Scanning
CEH Scanning Methodology

Enumeration

Overview of System Hacking Cycle
What is Enumeration?
Techniques for Enumeration
Netbios Null Sessions
Tools
DumpSec
NetBIOS Enumeration Using Netview
Nbtstat
SuperScan4
Enum
sid2user
user2sid
GetAcct
Null Session Countermeasures
PSTools
SNMP Enumeration
Management Information Base
Tools
UNIX Enumeration
SNMP UNIX Enumeration
SNMP Enumeration
Countermeasures
Tools
Steps to Perform Enumeration

System Hacking

Cracking Passwords
Password Types
Types of Password Attacks
Passive Online – Wire Sniffing
Passive Online Attacks
Active Online – Password Guessing
Offline Attacks
Non-Technical Attacks
Password Mitigation
Permanent Account Lockout –

Employee Privilege Abuse
Administrator Password Guessing
Manual Password Cracking Algorithm
Automatic Password Cracking

Algorithm
Performing Automated Password Guessing

Tools
Microsoft Authentication - LM, NTLMv1, and NTLMv2
Kerberos Authentication
What is LAN Manager Hash?
Salting
Tools
Password Sniffing
How to Sniff SMB Credentials?
Sniffing Hashes Using LophCrack
Tools
SMBRelay Weaknesses & Countermeasures
Password Cracking Countermeasures
LM Hash Backward Compatibility
How to Disable LM HASH?
Tools
Escalating Privileges
Privilege Escalation
Cracking NT/2000 Passwords
Active@ Password Changer
Change Recovery Console Password
Privilege Escalation Tool: x.exe
Executing applications
What is Spyware?

Tools
Keylogger Countermeasures
Anti-Keylogger
PrivacyKeyboard
Hiding Files
Hacking Tool: RootKit
Why Rootkits?
Rootkits in Linux
Detecting Rootkits
Rootkit Detection Tools
Sony Rootkit Case Study
Planting the NT/2000 Rootkit
Rootkits
Rootkit Countermeasures
Patchfinder2.0
RootkitRevealer
Creating Alternate Data Streams
How to Create NTFS Streams?
NTFS Stream Manipulation
NTFS Streams Countermeasures
NTFS Stream Detectors
What is Steganography?
Tools
Video Steganography
Steganography Detection
SIDS (Siego intrusion detection system)
High-Level View
Tool: dskprobe.exe

Covering tracks
Disabling Auditing
Clearing the Event Log
Tools

Trojans and Backdoors

Introduction
Effect on Business
What is a Trojan?
Overt and Covert Channels
Working of Trojans
Different Types of Trojans
What Do Trojan Creators Look For?
Different Ways a Trojan Can Get into a System
Indications of a Trojan Attack
Ports Used by Trojans
How to Determine which Ports are "Listening"?
Classic Trojans Found in the Wild
Trojans
Tini
iCmd
NetBus
Netcat
Beast
MoSucker
Proxy Server
SARS Trojan Notification
Wrappers
Wrapper Covert Program
Wrapping Tools
One file EXE Maker
Yet Another Binder
Pretator Wrapper
Packaging Tool: WordPad
RemoteByMail
Tool: Icon Plus
Defacing Application: Restorator
HTTP Trojans
Trojan Attack through Http
HTTP Trojan (HTTP RAT)
Shttpd Trojan - HTTP Server
Reverse Connecting Trojans
Nuclear RAT Trojan (Reverse Connecting)
Tool: BadLuck Destructive Trojan
ICMP Tunneling
ScreenSaver Password Hack Tool – Dummylock
Trojan
Hacking Tool: Loki
Atelier Web Remote Commander
Trojan Horse Construction Kit
How to Detect Trojans?
Tools
Delete Suspicious Device Drivers
Inzider - Tracks Processes and Ports
Tools
Anti-Trojan Software
Evading Anti-Virus Techniques

Evading Anti-Trojan/Anti-Virus Using
Stealth Tools v2.0
Backdoor Countermeasures
Tools
Tripwire
System File Verification
MD5sum.exe
Microsoft Windows Defender
How to Avoid a Trojan Infection?

Sniffers

Definition of Sniffing
Protocols Vulnerable to Sniffing
Types of Sniffing
ARP - What is Address Resolution Protocol?
ARP Spoofing Attack
Tools for ARP Spoofing
MAC Flooding
Tools for MAC Flooding
Threats of ARP Poisoning
IRS – ARP Attack Tool
ARPWorks Tool
Tool: Nemesis
Sniffer Hacking Tools (dsniff package)
DNS Poisoning Techniques
Types of DNS Poisoning:
Interactive TCP Relay
Sniffers
Tools
How to Detect Sniffing?
AntiSniff Tool
ArpWatch Tool
Countermeasures

Denial of Service

What are Denial of Service Attacks?
Goal of DoS
Impact and the Modes of Attack
Types of Attacks
DoS Attack Classification
DoS Attack Tools
Botnets
Uses of botnets
Types of Bots
Tool: Nuclear Bot
What is DDoS Attack?
Characteristics of DDoS Attacks
DDoS Unstoppable
Agent Handler Model
DDoS IRC based Model
DDoS Attack Taxonomy
Amplification Attack
Reflective DNS Attacks
Reflective DNS Attacks Tool:
ihateperl.pl
DDoS Tools
Worms
Slammer Worm
Spread of Slammer Worm – 30 min
MyDoom.B

SCO Against MyDoom Worm
How to Conduct a DDoS Attack
The Reflected DoS Attacks
Reflection of the Exploit
Countermeasures for Reflected DoS
DDoS Countermeasures
Taxonomy of DDoS Countermeasures
Preventing Secondary Victims
Detect and Neutralize Handlers
Detect Potential Attacks
Mitigate or Stop the Effects of DDoS Attacks
Deflect Attacks
Post-attack Forensics
Packet Traceback

Social Engineering

What is Social Engineering?
Human Weakness
"Rebecca" and "Jessica"
Office Workers
Types of Social Engineering
Preventing Insider Threat
Common Targets of Social Engineering
Factors that make Companies Vulnerable to Attacks
Why is Social Engineering Effective?
Warning Signs of an Attack
Tool: Netcraft Anti-Phishing Toolbar
Phases in a Social Engineering Attack
Behaviors Vulnerable to Attacks
Impact on the Organization
Countermeasures
Policies and Procedures
Security Policies - Checklist
Phishing Attacks and Identity Theft
What is Phishing?
Phishing Report
Attacks
Hidden Frames
URL Obfuscation
URL Encoding Techniques
IP Address to Base 10 Formula
Karen's URL Discombobulator
HTML Image Mapping Techniques
Fake Toolbars
Fake Status Bar
DNS Cache Poisoning Attack

Session Hijacking

What is Session Hijacking?
Spoofing vs. Hijacking
Steps in Session Hijacking
Types of Session Hijacking
The 3-Way Handshake
TCP Concepts 3-Way Handshake
Sequence Number Prediction
TCP/IP Hijacking
RST Hijacking

RST Hijacking Tool: hijack_rst.sh
Programs that Perform Session Hijacking
Hacking Tools
Remote TCP Session Reset Utility
Dangers Posed by Hijacking
Protecting against Session Hijacking
Countermeasure: IP Security
IP-SEC
Module 11: Hacking Web Servers
How Web Servers Work
How are Web Servers Compromised?
How are Web Servers Defaced?
Apache Vulnerability
Attacks Against IIS
Unicode
Hacking Tool: IISxploit.exe
Msv3prt IPP Vulnerability
WebDAV / ntdll.dll Vulnerability
RPC DCOM Vulnerability
ASN Exploits
ASP Trojan (cmd.asp)
IIS Logs
Network Tool: Log Analyzer
Hacking Tool: CleanIISLog
Unspecified Executable Path Vulnerability
Metasploit Framework
Immunity CANVAS Professional
Core Impact
Hotfixes and Patches
What is Patch Management?
Solution: UpdateExpert
Patch Management Tool
cacls.exe Utility
Vulnerability Scanners
Online Vulnerability Search Engine
Network Tools
Hacking Tool: WebInspect
Network Tool: Shadow Security Scanner
SecurEIS
Countermeasures
File System Traversal
Countermeasures
Increasing Web Server Security
Web Server Protection Checklist

Web Application Vulnerabilities

Web Application Setup
Web Application Hacking
Anatomy of an Attack
Web Application Threats
Cross-Site Scripting/XSS Flaws
Countermeasures
SQL Injection
Command Injection Flaws
Cookie/Session Poisoning
Parameter/Form Tampering
Buffer Overflow
Directory Traversal/Forceful Browsing
Cryptographic Interception
Cookie Snooping
Authentication Hijacking
Log Tampering
Error Message Interception
Attack Obfuscation
Platform Exploits
DMZ Protocol Attacks
Security Management Exploits
Web Services Attacks
Zero-Day Attacks
Network Access Attacks
TCP Fragmentation
Hacking Tools

Web-based Password Cracking Techniques

Definition of Authentication
Authentication Mechanisms
How to Select a Good Password?
Things to Avoid in Passwords
Changing Your Password
Protecting Your Password
How Hackers get hold of Passwords?
Windows XP: Remove Saved Passwords
Microsoft Password Checker
What is a Password Cracker?
Modus Operandi of an Attacker Using Password Cracker
How does a Password Cracker Work?
Classification of Attacks
Password Guessing
Query String
Cookies
Dictionary Maker
Available Password Crackers
Hacking Tools
Countermeasures

SQL Injection

Introducing SQL injection
Exploiting Web Applications
SQL Injection Steps
SQL Injection Techniques

How to Test for SQL Injection Vulnerability?
How does it Work?
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?
Automated SQL Injection Tool
SQL Injection in Oracle
SQL Injection in MySQL Database
Attack against SQL Servers
SQL Server Resolution Service (SSRS)
Osqli - Probing
SQL Injection Automated Tools
SQL Injection Countermeasures
Preventing SQL Injection Attacks
SQL Injection Blocking Tools:
SQLBlock
Acunetix Web Vulnerability Scanner

Hacking Wireless Networks

Introduction to Wireless Networking
Wired Network vs. Wireless Network
Effects of Wireless Attacks on Business
Types of Wireless Networks
Advantages and Disadvantages of a Wireless Network
Wireless Standards
Related Technology and Carrier Networks
Antennas
Cantenna
Wireless Access Points
SSID
Beacon Frames
Is the SSID a Secret?
Setting Up a WLAN
Detecting a Wireless Network
How to Access a WLAN
Terminologies
Authentication and Association
Authentication Modes
Authentication and (Dis)Association Attacks
Rogue Access Points
Tools to Generate Rogue Access Points: Fake AP
Tools to Detect Rogue Access Points: Netstumbler
Tools to Detect Rogue Access Points: MiniStumbler
Wired Equivalent Privacy (WEP)
What is WPA?
WPA Vulnerabilities
WEP, WPA, and WPA2
Steps for Hacking Wireless Networks
Cracking WEP
Weak Keys (a.k.a. Weak IVs)
Problems with WEP's Key Stream and Reuse
Automated WEP Crackers
Pad-Collection Attacks
XOR Encryption
Stream Cipher
WEP Tools
Temporal Key Integrity Protocol (TKIP)
LEAP: The Lightweight Extensible Authentication Protocol
LEAP Attacks
MAC Sniffing and AP Spoofing
Tool to Detect MAC Address Spoofing: Wellenreiter V2
Man-in-the-Middle Attack (MITM)
Denial-of-Service Attacks
Dos Attack Tool: Fatajack
Phone Jammers
Sniffing Tools
Sniffing Tools
Multisite Tool: THC-RUT
PCR-PRO-1k Hardware Scanner
Tools
Securing Wireless Networks
Auditing Tool: BSD-Airtools
AirDefense Guard
WIDZ: Wireless Intrusion Detection System
Radius: Used as Additional Layer in Security
Google Secure Access

Virus and Worms

Introduction to Virus
Virus History
Characteristics of a Virus
Working of Virus
Why People create computer viruses?
Symptoms of Virus-Like Attack

Virus Hoaxes
Chain Letters
How is a Worm different from a Virus?
Indications of Virus Attack
Hardware Threats
Software Threats
Virus Damage
Modes of Virus Infection
Stages of Virus Life
Virus Classification
How does a Virus Infect?
Storage Patterns of a Virus
System Sector Viruses
Stealth Virus
Bootable CD-ROM Virus
Self-Modification
Encryption with a Variable Key
Polymorphic Code
Viruses
Famous Virus/Worms – JS.Spth
Klez Virus Analysis
Writing a Simple Virus Program
Virus Construction Kits
Virus Detection Methods
Virus Incident Response
What is Sheep Dip?
Sheep Dip Computer
Virus Analysis - IDA Pro Tool
Prevention is Better than Cure
Latest Viruses
Top 10 Viruses- 2006
Anti-Virus Software
SocketsShield
Popular Anti-Virus Packages
Virus Databases

Physical Security

Security Statistics
Physical Security Breach Incidents
Understanding Physical Security
What Is the Need for Physical Security?
Who Is Accountable for Physical Security?
Factors Affecting Physical Security
Physical Security Checklist
Information Security
EPS (Electronic Physical Security)
Wireless Security
Laptop Theft: Security Statistics
Laptop Theft
Laptop Security Tools
Laptop Tracker - XTool Computer Tracker
Tools to Locate Stolen Laptops
Stop's Unique, Tamper-proof Patented Plate
Tool: TrueCrypt
Laptop Security Countermeasures
Mantrap
TEMPEST
Challenges in Ensuring Physical Security
Spyware Technologies
Spying Devices
Physical Security: Lock Down USB Ports
Tool: DeviceLock
Blocking the Use of USB Storage Devices
Track Stick GPS Tracking Device

Linux Hacking

Why Linux?
Linux Distributions
Linux – Basics
Linux Live CD-ROMs
Basic Commands of Linux
Linux File Structure
Linux Networking Commands
Directories in Linux
Compiling the Linux Kernel
How to Install a Kernel Patch?
Compiling Programs in Linux
GCC Commands
Make Install Command
Linux Vulnerabilities
Chrooting
Why is Linux Hacked?
Linux Vulnerabilities in 2005
How to Apply Patches to Vulnerable Programs?
Scanning Networks
Tools
Password Cracking in Linux
Firewall in Linux: IPTables
Basic Linux Operating System Defense
SARA (Security Auditor's Research Assistant)
Linux Tool
Linux Loadable Kernel Modules
Hacking Tool: Linux Rootkits
Rootkits
Rootkit Countermeasures
Linux Tools: Application Security
Advanced Intrusion Detection

Environment (AIDE)
Linux Tools
Linux Security Countermeasures
Steps for Hardening Linux

Evading IDS, Firewalls, and Honeypots

Introduction to Intrusion Detection Systems
Terminologies
Intrusion Detection System (IDS)
Firewall
Firewall Identification
Firewalking
Banner Grabbing
Breaching Firewalls
Bypassing a Firewall Using HTTP Tunnel
Placing Backdoors Through Firewalls
Hiding behind a Covert Channel: LOKI
ACK Tunneling
Tools to Breach Firewalls
Common Tool for Testing Firewall & IDS
Honeypot
What is a Honeypot?
The Honeynet Project
Types of Honeypots
Advantages and Disadvantages of a Honeypot
Where to Place a Honeypot?
Honeypots
Physical and Virtual Honeypots
Tools to Detect Honeypots
What to do When Hacked?

Buffer Overflows

Why are Programs/Applications Vulnerable?
Buffer Overflows
Reasons for Buffer Overflow Attacks
Knowledge Required to Program Buffer Overflow Exploits
Types of Buffer Overflows
How to Detect Buffer Overflows in a Program
Attacking a Real Program
NOPS
How to Mutate a Buffer Overflow Exploit
Defense Against Buffer Overflows
Tool to Defend Buffer Overflow
Vulnerability Search – ICAT
Simple Buffer Overflow in C
Code Analysis

Cryptography

Public-key Cryptography
Working of Encryption
Digital Signature
RSA (Rivest Shamir Adleman)
RC4, RC5, RC6, Blowfish
Algorithms and Security
Brute-Force Attack
RSA Attacks
Message Digest Functions
One-way Bash Functions
MD5
SHA (Secure Hash Algorithm)
SSL (Secure Sockets Layer)
RC5
What is SSH?
SSH (Secure Shell)
Government Access to Keys (GAK)
RSA Challenge
distributed.net
Cleversafe Grid Builder
PGP (Pretty Good Privacy)
Code Breaking: Methodologies
Cryptography Attacks
Disk Encryption
Hacking Tool

Penetration Testing

Introduction to Penetration Testing
Categories of Security Assessments
Vulnerability Assessment
Limitations of Vulnerability Assessment
Types of Penetration Testing
Risk Management
Do-it-Yourself Testing
Outsourcing Penetration Testing Services
Terms of Engagement
Project Scope
Pentest Service Level Agreements
Testing Points
Testing Locations
Automated Testing
Manual Testing
Using DNS Domain Name and IP Address Information
Enumerating Information about Hosts on Publicly-Available Networks
Testing Network-Filtering Devices

Enumerating Devices
Denial of Service Emulation Tools
Evaluating Different Types of Pentest Tools
Asset Audit
Fault Trees and Attack Trees
GAP Analysis
Threat
Business Impact of Threat
Internal Metrics Threat
External Metrics Threat
Calculating Relative Criticality
Test Dependencies
Defect Tracking Tools
Disk Replication Tools
DNS Zone Transfer Testing Tools
Network Auditing Tools
Trace Route Tools and Services
Network Sniffing Tools
Denial-of-Service Emulation Tools
Traditional Load Testing Tools
System Software Assessment Tools
Operating System Protection Tools
Fingerprinting Tools
Port Scanning Tools
Directory and File Access Control Tools
File Share Scanning Tools
Password Directories
Password Guessing Tools
Link Checking Tools
Web Testing-based Scripting Tools
Buffer Overflow Protection Tools
File Encryption Tools
Database Assessment Tools
Keyboard Logging and Screen Reordering Tools
System Event Logging and Reviewing Tools
Tripwire and Checksum Tools
Mobile-Code Scanning Tools
Centralized Security Monitoring Tools
Web Log Analysis Tools
Forensic Data and Collection Tools
Security Assessment Tools
Multiple OS Management Tools
Phases of Penetration Testing
Penetration Testing Deliverables Templates

Self-Study Modules

Covert Hacking
Writing Virus Codes
Assembly Language Tutorial
Exploit Writing
Smashing the Stack for Fun and Profit
Windows Based Buffer Overflow Exploit Writing
Reverse Engineering