Ethical Hacking and Countermeasures

http://www.eccouncil.org

EC-Council

C|EH™

Certified Ethical Hacker

Hackers are here. Where are you?

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The definition of an Ethical Hacker is very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

Hackers Are Here. Where Are You?

Ethical Hacking and Countermeasures Training Program

Course DescriptionThis 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 certification exam 312-50 will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the 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 v5

Module: Introduction to Ethical Hacking

Module Objectives
Module Flow
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?
Phase1-Reconnaissaance
Reconnaissance Types
Phase2-Scanning
Phase3-Gaining Access
Phase4-Maintaining Access
Phase5-Covering Tracks
Types of Hacker Attacks
Operating System attacks
Application-level attacks
Shrink Wrap code attacks
Misconfiguration attacks
Remember this Rule!
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
Secunia (www.secunia.com)

Module: Footprinting

Module: Scanning

Scenario
Module Objectives
Module Flow
Scanning: Definition
Types of Scanning
Objectives of Scanning
CEH Scanning Methodology
Checking for live systems - ICMP Scanning
Angry IP
HPing2
Ping Sweep
Firewalk Tool
TCP Communication Flags
Syn Stealth/Half Open Scan
Stealth Scan
Xmas Scan
Fin Scan
Null Scan
Idle Scan
ICMP Echo Scanning/List Scan
TCP Connect/Full Open Scan
FTP Bounce Scan
Ftp Bounce Attack
SYN/FIN Scanning Using IP Fragments
UDP Scanning
Reverse Ident Scanning
RPC Scan
Window Scan
Blaster Scan
Portscan Plus, Strobe
Different Scanning tools
Nmap
IPSec Scan
Netscan Tools Pro 2003

WUPS – UDP Scanner
Superscan
IPScanner
Megaping
Global Network Inventory Scanner
Net Tools Suite Pack
Floppy Scan
War Dialer Technique
Phonesweep – War Dialing Tool
THC Scan
War Dialing Countermeasures: Sandtrap Tool
Banner Grabbing
OS Fingerprinting
Active Stack Fingerprinting
Passive Fingerprinting
Active Banner Grabbing Using Telnet
P0f – Banner Grabbing Tool
Httprint Banner Grabbing Tool
Tools for Active Stack Fingerprinting
Xprobe2
Ringv2
Netcraft
Vulnerability Scanning
Bidiblah Automated Scanner
Qualys Web Based Scanner
SAINT
ISS Security Scanner
Nessus
GFI Languard
Security Administrator's Tool for Analyzing Networks (SATAN)
Retina
NIKTO
SAFEsuite Internet Scanner, IdentTCPScan
Cheops
Friendly Pinger
Preparing Proxies
Proxy Servers

Module: Enumeration

Module: System Hacking

Module Flow

Scenario

Part 1- Cracking Password

CEH hacking Cycle

Password Types

Types of Password Attack

Passive Online-Wire Sniffing

Passive Online Attacks

Active Online- Password Guessing

Offline Attacks

Dictionary attacks

Hybrid attacks

Brute force Attack

Pre-computed Hashes

Non-Technical Attack

Password Mitigation

Permanent Account Lockout-Employee Privilege Abuse

Administrator Password Guessing

Manual Password cracking Algorithm

Automatic Password Cracking Algorithm

Performing Automated Password Guessing

Tool: NAT

Smbbf (SMB Passive Brute Force Tool)

SmbCrack Tool: Legion

Hacking Tool: LOphtcrack

Microsoft Authentication

LM, NTLMv1, and NTLMv2

NTLM And LM Authentication On The Wire

Kerberos Authentication

What is LAN Manager Hash?

LM “Hash” Generation

LM Hash

Salting

PWdump2 and Pwdump3

Tool: Rainbowcrack

Hacking Tool: KerbCrack

NetBIOS DoS Attack

Rootkit: Nuclear
Rootkit: Vanquish
Rootkit Countermeasures
Patchfinder2.0
RootkitRevealer
Creating Alternate Data Streams
How to Create NTFS Streams?
NTFS Stream Manipulation
NTFS Streams Countermeasures
NTFS Stream Detectors (ADS Spy and ADS Tools)
What is Steganography?
Tool: Merge Streams
Invisible Folders
Tool: Invisible Secrets 4
Tool : Image Hide
Tool: Stealth Files
Masker Steganography Tool
Hermetic Stego
DCPP – Hide an Operating System
Tool: Camera/Shy
www.spammimic.com
Tool: Mp3Stego
Tool: Snow.exe
Video Steganography
Steganography Detection
SIDS
Tool: dskprobe.exe
Part5-Covering Tracks
CEH Hacking Cycle
Covering Tracks
Disabling Auditing
Clearing the Event Log
Tool: elsave.exe
Hacking Tool: Winzapper
Evidence Eliminator
Tool: Traceless
Tool: Tracks Eraser Pro

Trojans and Backdoors

Module: Sniffers

Ettercap
MAC Flooding
Tools for MAC Flooding
Linux Tool: Macof
Windows Tool: Etherflood
Threats of ARP Poisoning
Irs-Arp Attack Tool
ARPWorks Tool
Tool: Nemesis
Sniffers Hacking Tools
Linux tool: Arpspoof
Linux Tool: Dnssppoof
Linux Tool: Dsniff
Linux Tool: Filesnarf
Linux Tool: Mailsnarf
Linux Tool: Msgsnarf
Linux Tool: Sshmitm
Linux Tool: Tcpkill
Linux Tool: Tcpnice
Linux Tool: Urlsnarf
Linux Tool: Webspy
Linux Tool: Webmitm
DNS Poisoning
Intranet DNS Spoofing (Local Network)
Internet DNS Spoofing (Remote Network)
Proxy Server DNS Poisoning
DNS Cache Poisoning
Interactive TCP Relay
HTTP Sniffer: EffeTech
Ace Password Sniffer
MSN Sniffer
Smart Sniff
Session Capture Sniffer: Nwreader
Cain and Abel
Packet Crafter
SMAC
Netsetman Tool

Denial-of-Service

DoS Attack Classification
Smurf Attack
Buffer Overflow Attack
Ping of Death Attack
Teardrop Attack
SYN Attack
SYN Flooding
Tribal Flow Attack
DoS Attack Tools
Jolt2
Bubonic.c
Land and LaTierra
Targa
Blast2.0
Nemesys
Panthers2
Icmp Packet Sender
Some Trouble
UDP Flood
FSMax
Bot (Derived from the Word 'RoBot')
Botnets
Uses of botnets
Types of Bots
How do They Infect? Analysis of Agabot
Nuclear Bot
What is DDoS Attack?
DDoS Attack Characteristics
Agent Handler Model
DDoS IRC-based Model
DDoS Attack Taxonomy
Amplification Attack
DDoS Tools
Trinoo
Tribe Flood Network
TFN2K
Stacheldraht

Module: Social Engineering

Module: Session Hijacking

Module: Hacking Web Servers

IIS Components
IIS Directory Traversal (Unicode) Attack
Unicode
Unicode Directory Traversal Vulnerability
Hacking Tool: IISxploit.exe
Msw3prt IPP Vulnerability
WebDav/ntdll.dll Vulnerability
Real World Instance of WebDAV Exploit
RPC DCOM Vulnerability
ASN Exploits
ASP Trojan (cmd.asp)
IIS Logs
Network Tool: Log Analyzer
Hacking Tool: CleanIISLog
Unspecified Executable Path Vulnerability
Metasploit Framework
Scenario
Hotfixes and Patches
What is Patch Management?
Solution: UpdateExpert
Patch Management Tool: qfecheck
Patch Management Tool: HFNetChk
cacls.exe utility
cacls.exe utility
Vulnerability Scanners
Online Vulnerability Search Engine
Network Tool: Whisker
Network Tool: N-Stealth HTTP Vulnerability Scanner
Hacking Tool: WebInspect
Network Tool: Shadow Security Scanner
Secure IIS
Countermeasures
Increasing Web Server Security
Web Server Protection Checklist
Summary

Module: Web Application Vulnerabilities

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

Module: Web-Based Password Cracking Techniques

- Fingerprint-based Identification
- Hand Geometry- based Identification
- Retina Scanning
- Face Recognition
- How to Select a Good Password?
- Things to Avoid in Passwords
- Changing Your Password
- Protecting Your Password
- How Hackers Get Hold of Passwords?
- Microsoft Password Checker
- What is a Password Cracker
- Modus Operandi of an Attacker Using a Password Cracker
- How Does a Password Cracker Work?
- Attacks - Classification
- Password Guessing
- Query String
- Cookies
- Dictionary Maker
- Password Crackers Available
- L0phtCrack (LC4)
- John the Ripper
- Brutus
- ObiWaN
- Authforce
- Hydra
- Cain & Abel
- RAR
- Gammaprog
- WebCracker
- Munga Bunga
- PassList
- SnadBoy
- RockXP
- WinSSLMiM
- Countermeasures
- Summary

Module: SQL Injection

Scenario
Module Objectives
Module Flow
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 if it is Vulnerable?
How Does It Work?
Executing Operating System Commands
How to get output of your SQL query?
How to get 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?
Absinthe Automated SQL Injection Tool
SQL Injection in Oracle
SQL Injection in MySql Database
Attacking SQL Servers
SQL Server Resolution Service (SSRS)
Osql -L Probing
SQL Injection Automated Tools
Hacking Tool: SQLDict
SQLExec
Tool: sqlbf
SQLSmack
SQL2.exe
SQL Injection Countermeasures
Preventive Measures

Module: Hacking Wireless Networks

Authentication Modes

Access Point Positioning

Rogue Access Points

Tools to Generate Rogue AP: Fake AP

NetStumbler

MiniStumbler

What is Wired Equivalent Privacy (WEP)?

XOR Encryption

Stream Cipher

PAD Collection Attacks

Cracking WEP

Weak keys

Problems with WEP's Key Stream and Reuse

Automated WEP Crackers

The Lightweight Extensible Authentication Protocol (LEAP)

LEAP Attacks

What is WPA?

WPA Vulnerabilities

Temporal Key Integrity Protocol (TKIP)

WEP, WPA and WPA2

Types of Attacks

Hacking

Steps for Hacking Wireless Networks

Step 1: Find Networks to Attack

Step2: Choose the Network to Attack

Step 3: Analyzing the Network

Step 4: Cracking the WEP Key

Step 5: Sniffing the Network

WEP Tool: Aircrack

AirSnort

WEPCrack

MAC Sniffing and AP Spoofing

Tool for Detecting MAC Spoofing: Wellenreiter v2

Denial-Of-Service (Dos) Attacks

Dos Attack Tool: Fatajack

Man-in-the-Middle Attack (MITM)

Scanning Tools

Redfang
Kismet
THC-wardrive
PrismStumbler
MacStumbler
Mognet V1.16
WaveStumbler
NetChaser v1.0 for Palm Tops
AP Scanner
Wavemon
Wireless Security Auditor (WSA)
AirTraf 1.0
Wifi Finder
Sniffing Tools
AiroPeek
NAI Wireless Sniffer
Ethereal
Aerosol v0.65
vxSniffer
EtherPEG
Driftnet
AirMagnet
WinDump
Ssidsniff
Multiuse Tool: THC-RUT
WinPcap
Auditing Tool: BSD-Airtools
AirDefense Guard
Wireless Intrusion Detection System (WIDZ)
PCR-PRO-1k Hardware Scanner
Securing Wireless Networks
Remote Authentication Dial-In User Service
Google Secure Access
Summary

Module: Virus and Worms

Case Study
Scenario
Module Objectives
Module Flow
Introduction
Virus History
Characteristics of Virus
Working of Virus
Infection Phase
    Attack Phase
Why people create Computer Viruses?
Symptoms of a Virus-like Attack
Virus Hoaxes
How is a Worm Different from a Virus?
Indications of a Virus Attack
Hardware Threats
Software Threats
Virus Damage
Mode of Virus Infection
Stages of Virus Life
Virus Classification
How Does a Virus Infect?
Storage Patterns of Virus
System Sector virus
Stealth Virus
Bootable CD-Rom Virus
Self -Modification
Encryption with a Variable Key
Polymorphic Code
Metamorphic Virus
Cavity Virus
Sparse Infector Virus
Companion Virus
File Extension Virus
Famous Virus/Worms – I Love You Virus
Famous Virus/Worms – Melissa

Module: Physical Security

Factors Affecting Physical Security
Physical Security Checklist
Physical Security Checklist -Company surroundings
Gates
Security Guards
Premises- Physical Security
CCTV Cameras
Reception
Server
Workstation Area
Wireless Access Point
Other Equipments
Access Control
Mantrap
Biometric Devices
Biometric Identification Techniques
Smart cards
Security Token
Computer Equipment Maintenance
Wiretapping
Remote Access
Locks
Lock Picking
Lock Picking Tools
Challenges in Ensuring Physical Security
Information Security
Wireless Security Countermeasures
EPS (Electronic Physical Security)
Spyware
Spying Devices
Lapse of Physical Security
Laptop Theft - Security Statistics
Laptop Theft
Laptop Theft: Data under loss
Laptop Security Tools
XTool® Computer Tracker
STOP Anti Theft Security Tags

Physical Security: Lock Down USB Ports
Tool: Device Lock
Track Stick GPS Tracking Device
Summary

Module: Linux Hacking

Scenario
Module Objectives
Module Flow
Why Linux?
Linux Distributions
Linux Live CD-ROMs
Linux Basic Commands
Linux File Structure
Linux Networking Commands
Directories in Linux
Compiling the Linux control
How to install a kernel patch
Compiling Programs in Linux
GCC commands
Make Files
Make Install Command
Linux Vulnerabilities
Chrooting
Why is Linux Hacked?
Linux Vulnerabilities in 2005
How to apply patches to vulnerable programs
Scanning Networks
Nmap in Linux
Nessus
Cheops
Port Scan Detection Tools
Password Cracking in Linux
Firewall in Linux: IPTables
Basic Linux Operating System Defense

Module: Evading IDS, Firewalls and Detecting Honey Pots

Module Objectives
Module Flow
Introduction
Terminology
Intrusion Detection System (IDS)
IDS Placement
Ways to Detect an Intrusion
Types of Instruction Detection Technique
System Integrity Verifiers (SIVS)
Tripwire
Cisco Security Agent (CSA)
Signature Analysis
General Indication of Intrusion: System Indications
General Indication of Intrusion: File System Indications
General Indication of Intrusion: Network Indications
Intrusion Detection Tools
Snort 2.x
Using EventTriggers.exe for Eventlog Notifications
SnortSam
Steps to Perform after an IDS detects an attack
Evading IDS Systems
Ways to Evade IDS
Tools to Evade IDS: SideStep
ADMutate
Packet Generators
What is a Firewall?
What Does a Firewall Do?
Packet Filtering
What can’t a firewall do?
How does a Firewall work?
Firewall Operations
Hardware Firewall
Software Firewall
Types of Firewall
Packet Filtering Firewall
Circuit-Level Gateway
Application Level Firewall

Module: Buffer Overflows

Buffer Overflows
Reasons for Buffer Overflow attacks
Knowledge Required to Write Buffer Overflow Exploits
Stack-based Buffer Overflow
Understanding Assembly Language
Understanding Stacks
A Normal Stack
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
Once the Stack is Smashed
Defense against Buffer Overflows
Tool to Defend Buffer Overflow:Return Address Defender (RAD)
StackGuard
Immunix System
Vulnerability Search – ICAT
Summary

Module: Cryptography

Module Objectives
Module Flow
Public Key Cryptography
Working of Encryption
Digital Signature
RSA (Rivest, Shamir, and Adleman)
RC4, RC5, RC6, Blowfish
Algorithms and Security
Brute-Force Attack
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
Hacking Tool: PGPCrack
Magic Lantern
WEPCrack
Cracking S/MIME Encryption using idle CPU Time
CypherCalc
Command Line Scriptor
CryptoHeaven
Summary

Module: Penetration Testing

Introduction to Penetration Testing (PT)
Categories of security assessments
Vulnerability Assessment
Limitations of Vulnerability Assessment
Penetration Testing
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

Pentest using Appscan

HackerShield

Pen-Test Using Cerberus Internet Scanner:

Pen-Test Using Cybercop Scanner:

Pen-Test Using FoundScan Hardware Appliances

Pen-Test Using Nessus

Pen-Test Using NetRecon

Pen-Test Using SAINT

Pen-Test Using SecureNet Pro

Pen-Test Using SecureScan

Pen-Test Using SATAN, SARA and Security Analyzer

Pen-Test Using STAT Analyzer

VigiLENT

WebInspect

Evaluating Different Types of Pen-Test Tools

Asset Audit

Fault Tree 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
Pre-attack Phase
Best Practices
Results that can be Expected
Passive Reconnaissance
Active Reconnaissance
Attack Phase
Activity: Perimeter Testing
Activity: Web Application Testing - I
Activity: Web Application Testing - II
Activity: Wireless Testing
Activity: Acquiring Target
Activity: Escalating Privileges
Activity: Execute, Implant and Retract
Post Attack Phase and Activities

For Training Requirements, Please Contact EC-Council ATC.

EC-Council

http://www.eccouncil.org
info@eccouncil.org