CEH - Certified Ethical Hacker

Course Outline: CEH - Certified Ethical Hacker

Learning Method: Instructor Led

Duration: 5 Days

Overview:
This class immerses students in an interactive environment where they will learn how to scan, test, hack, and secure their own systems. Students then learn how intruders escalate privileges and what steps can be taken to secure a system.

Target Audience:
This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Skills Gained:
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 led 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, Open Source Intelligence, Incident Handling and Log Interpretation.

Pre-requisites:
At least two years of IT security experience
Strong working knowledge of TCP/IP
Basic familiarity with Linux/UNIX
Essentials of Network Security is highly recommended.

Outline:
Module 1: 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

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

Module 2: Footprinting

Revisiting Reconnaissance

Defining of Footprinting

Information Gathering Methodology

Unearthing Initial Information

Finding a Companys URL

Internal URL

Extracting Archive 0f a Website

Google Search for Companys 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

Steps to Perform Footprinting

Module 3: Scanning

Definition of Scanning

Types of Scanning

Objectives of Scanning

CEH Scanning Methodology

Check for live sytems

Check for open ports

Banner grabbing/OS Fingerprinting

Identify Service

Scan for Vulnerability

Draw network diagrams of Vulnerable hosts

Prepare proxies

Anonymizers

SSL Proxy Tool

HTTP Tunneling Techniques

HTTPort

Spoofing IP Address - Source Routing

Detecting IP Spoofing

Despoof Tool

Scanning Countermeasures

Tool: SentryPC

Module 4: Enumeration

Overview of System Hacking Cycle

What is Enumeration?

Techniques for Enumeration

Netbios Null Sessions

Tools

Null Session Countermeasures

PSTools

SNMP Enumeration

Management Information Base

Tools

UNIX Enumeration

SNMP UNIX Enumeration

SNMP Enumeration Countermeasures

Tools

Steps to Perform Enumeration

Module 5: System Hacking

Cracking Passwords

Escalating Privileges

Executing applications

Hiding Files

Covering tracks

Module 6: 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

Wrappers

Wrapper Covert Program

Wrapping 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

How to Avoid a Trojan Infection?

Module 7: 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?

Module 8: 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

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

Module 9: 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

Karens URL Discombobulator

HTML Image Mapping Techniques

Fake Browser Address Bars

Fake Toolbars

Fake Status Bar

DNS Cache Poisoning Attack

Module 10: 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

Msw3prt 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

SecureIIS

Countermeasures

File System Traversal Countermeasures

Increasing Web Server Security

Web Server Protection Checklist

Module 12: Web Application Vulnerabilities

Web Application Setup

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

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

Hacking Tools

Module 13: 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

Countermeasures

Module 14: 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)

Osql L- Probing

SQL Injection Automated Tools

SQL Injection Countermeasures

Preventing SQL Injection Attacks

SQL Injection Blocking Tool: SQLBlock

Acunetix Web Vulnerability Scanner

Module 15: 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 WEPs 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
Scanning Tools
Sniffing Tools
Multiuse 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

Module 16: 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

Socketshield

Popular Anti-Virus Packages

Virus Databases

Module 17: 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

Module 18: 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

Module 19: Evading IDS, Firewalls, and Honeypots

Introduction to Intrusion Detection Systems

Terminologies

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?

Module 20: 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

Stack-based Buffer Overflow

Heap/BSS-based Buffer Overflow

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

Module 21: 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

Module 22: 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

Blueprint Software Web Scripting Editor

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

Insider attacks

What is covert channel?

Security Breach

Why Do You Want to Use Covert Channel?

Motivation of a Firewall Bypass

Covert Channels Scope

Covert Channel: Attack Techniques

Simple Covert Attacks

Advanced Covert Attacks

Reverse Connecting Agents

Covert Channel Attack Tools

Writing Virus Codes

Introduction of Virus

Types of Viruses

Symptoms of a Virus Attack

Prerequisites for Writing Viruses

Required Tools and Utilities

Virus Infection Flow Chart

Components of Viruses

Functioning of Replicator part

Diagrammatical representation

Writing Replicator

Writing Concealer

Dispatcher

Writing Bomb/Payload

Trigger Mechanism

Brute Force Logic Bombs

Testing Virus Codes

Tips for Better Virus Writing

Assembly Language Tutorial

Number System

Base 10 System

Base 2 System

Decimal 0 to 15 in Binary

Binary Addition (C stands for Canary)

Hexadecimal Number

Hex Example

Hex Conversion

nibble

Computer memory

Characters Coding

ASCII and UNICODE

CPU

Machine Language

Compilers

Clock Cycle

Original Registers

Instruction Pointer

Pentium Processor

Interrupts

Interrupt handler

External interrupts and Internal interrupts

Handlers

Machine Language

Assembly Language

Assembler

Assembly Language Vs High-level Language

Assembly Language Compilers

Instruction operands

MOV instruction

ADD instruction

SUB instruction

INC and DEC instructions

Directive

preprocessor

equ directive

%define directive

Data directives

Labels

Input and output

C Interface

Call

Creating a Program

Why should anyone learn assembly at all?

Assembling the code

Compiling the C code

Linking the object files

Understanding an assembly listing file

Big and Little Endian Representation

Skeleton File

Working with Integers

Signed integers

Signed Magnitude

Twos Compliment

If statements

Do while loops

Indirect addressing

Subprogram

The Stack

The SS segment

ESP

The Stack Usage

The CALL and RET Instructions

General subprogram form

Local variables on the stack

General subprogram form with local variables

Multi-module program

Saving registers

Labels of functions

Calculating addresses of local variables

Exploit Writing

Exploits Overview

Prerequisites for Writing Exploits and Shellcodes

Purpose of Exploit Writing

Types of Exploits

The Proof-of-Concept and Commercial Grade Exploit

Converting a Proof of Concept Exploit to Commercial Grade Exploit

Attack Methodologies

Socket Binding Exploits

Tools for Exploit Writing

Steps for Writing an Exploit

Differences Between Windows and Linux Exploits

Shellcodes

Tools Used for Shellcode Development

Steps for Writing a Shellcode

Issues Involved With Shellcode Writing

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
execve()
exit.c
The code in Assembly
JMP
Code using indexed addressing
Offset calculation
shellcodeasm.c
testsc.c
Compile the code
NULL byte
shellcodeasm2.c
testsc2.c
Writing an Exploit
overflow1.c
Compiling the code
sp.c
vulnerable.c

NOPs

Windows Based Buffer Overflow Exploit Writing

Buffer Overflow

Stack overflow

Writing Windows Based Exploits

Exploiting stack based buffer overflow

OpenDataSource Buffer Overflow Vulnerability Details

Simple Proof of Concept

Windbg.exe

Analysis

EIP Register

Execution Flow

But where can we jump to?

Offset Address

The Query

Finding jmp esp

Debug.exe

listdlls.exe

Msvcrt.dll

Out.sql

The payload

ESP

Limited Space

Getting Windows API/function absolute address

Memory Address

Other Addresses

Compile the program

Final Code

Reverse Engineering

Positive Applications of Reverse Engineering

Ethical Reverse Engineering

World War Case Study

DMCA Act

What is Disassembler?

Why do you need to decompile?

Professional Disassembler Tools

Tool: IDA Pro

Convert Machine Code to Assembly Code

Decompilers

Program Obfuscation

Convert Assembly Code to C++ code

Machine Decompilers

Tool: dcc

Machine Code of compute.exe Prorgam

Assembly Code of compute.exe Program

Code Produced by the dcc Decompiler in C

Tool: Boomerang

What Boomerang Can Do?

Andromeda Decompiler

Tool: REC Decompiler

Tool: EXE To C Decompiler

Delphi Decompilers

Tools for Decompiling .NET Applications

Salamander .NET Decompiler

Tool: LSW DotNet-Reflection-Browser

Tool: Reflector

Tool: Spices NET.Decompiler

Tool: Decompilers.NET

NET Obfuscator and .NET Obfuscation

Java Bytecode Decompilers

Tool: JODE Java Decompiler

Tool: JREVERSEPRO

Tool: SourceAgain

Tool: ClassCracker

Python Decompilers

Reverse Engineering Tutorial

OllyDbg Debugger

How Does OllyDbg Work?

Debugging a Simple Console Application