



ETHICAL HACKING AND COUNTERMEASURES

<http://www.eccouncil.org>

EC-Council

C | **E H** TM
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 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.

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-Reconnaissance

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!

Hactivism

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)

Hackerstorm Vulnerability Database Tool (www.hackerstrom.com)
HackerWatch (www.hackerwatch.org)
Web Page Defacement Reports (www.zone-h.org)
How to Conduct Ethical Hacking?
How Do They Go About It?
Approaches to Ethical Hacking
Ethical Hacking Testing
Ethical Hacking Deliverables
Computer Crimes and Implications
Legal Perspective (U.S. Federal Law)
Section 1029 and Penalties
Section 1030 and Penalties
Japan Cyber Laws
United Kingdom Cyber Laws
Australia Cyber Laws
Germany's Cyber Laws
Singapore's Cyber Laws
Summary

Module: Footprinting

Scenario
Module Objectives
Revisiting Reconnaissance
Defining Footprinting
Information Gathering Methodology
Unearthing Initial Information
Finding 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
Public and Private Websites

DNS Enumerator
SpiderFoot (<http://www.binarypool.com/spiderfoot/>)
Sensepost Footprint Tools (www.sensepost.com/research/bidiblah)
Wikito Footprinting Tool
Web Data Extractor Tool
Additional Footprinting Tools
Whois
Nslookup
Extract DNS Information
Types of DNS Records
Necrosoft Advanced DIG
Locate the Network Range
ARIN
Traceroute
Traceroute Analysis
3D Traceroute (<http://www.d3tr.de/>)
Tool: NeoTrace (Now McAfee Visual Trace)
GEOSpider (<http://www.delorme.com/professional/geospider/>)
Geowhere Footprinting Tool (<http://www.geowhere.net/>)
Google Earth
Tool: VisualRoute Trace
Kartoo Search Engine (www.kartoo.com)
Touchgraph Visual Browser (www.touchgraph.com)
Tool: SmartWhois
Tool: VisualRoute Mail Tracker
Tool: eMailTrackerPro
Tool: Read Notify (readnotify.com)
HTTrack Web Site Copier (www.httrack.com)
Web Ripper Tool
Robots.txt
Website Watcher
E-Mail Spiders
1st E-mail Address Spider
Powerful E-mail Collector Tool
Steps to Perform Foot Printing
Summary

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
Pof – Banner Grabbing Tool
Httpprint 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

Use of Proxies for Attacking
SocksChain
Proxy Workbench
Proxymanager Tool
Super Proxy Helper Tool
Happy Browser Tool (Proxy Based)
Multiproxy
Tor Proxy Chaining Software
Additional Proxy Tools
Anonymizers
Primediis Anonymizer
Google Cookies
G-Zapper
SSL Proxy Tool
HTTP Tunneling Techniques
HTTPPort
Spoofing IP Address
Spoofing IP Address Using Source Routing
Detection of IP Spoofing
Despoof Tool
Scanning Countermeasures
Summary

Module: Enumeration

Scenario
Module Objectives
Module Flow
Overview of System Hacking Cycle
What is Enumeration?
Techniques for Enumeration
NetBIOS Null Sessions
So What's the Big Deal?
DumpSec Tool
NetBIOS Enumeration
Nbtstat Enumeration Tool

SuperScan4 Tool
Enum Tool
Enumerating User Accounts
GetAcct
Null Session Countermeasure
PS Tools
PsExec
PsFile
PsGetSid
PsKill
PsInfo
PsList
PsLogged On
PsLogList
PsPasswd
PsService
PsShutdown
PsSuspend
Simple Network Management Protocol (SNMP) Enumeration
Management Information Base (MIB)
SNMPutil Example
SolarWinds
SNScan v1.05
UNIX Enumeration
SNMP UNIX Enumeration
SNMP Enumeration Countermeasures
Winfingerprint
Windows Active Directory Attack Tool
IP Tools Scanner
Enumerate Systems Using Default Password
Steps to Perform Enumeration
Summary

Module: System Hacking

Module Objectives

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: LOphtrcrack
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

Hacking Tool: John the Ripper
Password Sniffing
How to Sniff SMB Credentials?
Sniffing Hashes Using LophtCrack
Tool: ScoopLM
Hacking Tool: SMBRelay
SMBRelay Man-In-The-Middle Scenario
Redirecting SMB Logon to the Attacker
SMB Replay Attacks
Replay Attack Tool : SMBProxy
Hacking Tool: SMB Grind
Hacking Tool: SMBDie
SMBRelay Weakness & Countermeasures
SMB Signing
Password Cracking Countermeasures
Do Not Store LAN Manager Hash in SAM Database
LM Hash Backward Compatibility
How to Disable LM HASH?
Password Brute Force Estimate Tool
Syskey Utility
Scenario
Part2-Escalating Privileges
CEH Hacking Cycle
Privilege Escalation
Cracking NT/2000 passwords
Active@ Password Changer
Change Recovery Console Password - Method 1
Change Recovery Console Password - Method 2
Privilege Escalation Tool: x.exe
Part3-Executing applications
CEH Hacking Cycle
Tool: psexec
Tool: remoexec
Tool: Alchemy Remote Executor
Keystroke Loggers
E-mail Keylogger
SpyToctor FTP Keylogger

IKS Software Keylogger
Ghost Keylogger
Hacking Tool: Hardware Key Logger
What is Spyware?
Spyware: Spector
Remote Spy
eBlaster
Stealth Voice Recorder
Stealth Keylogger
Stealth Website Logger
Digi Watcher Video Surveillance
Desktop Spy Screen Capture Program
Telephone Spy
Print Monitor Spy Tool
Perfect Keylogger
Stealth E-Mail Redirector
Spy Software: Wiretap Professional
Spy Software: FlexiSpy
PC PhoneHome
Keylogger Countermeasures
Anti Keylogger
Privacy Keyboard
Scenario
Part4-Hiding files
 CEH Hacking Cycle
 Hiding Files
Hacking Tool: RootKit
Why rootkits?
Rootkits
Rootkits in Linux
Detecting Rootkits
Steps for Detecting Rootkits
Rootkit detection tools
Sony Rootkit Case Study
Planting the NT/2000 Rootkit
Rootkit: Fu
AFX Rootkit 2005

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

Tool: ZeroTracks

Summary

Trojans and Backdoors

Scenario

Module Objectives

Module Flow

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

Some Famous Trojans and Ports They Use

How to Determine which Ports are Listening

Different Trojans in the Wild

Trojan: Tini

Trojan: icmd

Trojan: NetBus

Netcat

Beast

MoSucker Trojan

Proxy Server Trojan

SARS Trojan Notification

Wrappers

Graffiti.exe

Wrapping Tools

Packaging Tool: WordPad

RemoteByMail

Icon Plus

Restorator

Tetris

HTTP Trojans
HTTP RAT
Reverse Connecting Trojans
BadLuck Destructive Trojan
ICMP Tunneling
ICMP Backdoor Trojan
ScreenSaver Password Hack Tool
Phatbot
Amitis
Senna Spy
QAZ
Case Study: Microsoft Network Hacked by QAZ Trojan
Back Orifice
Back Orifice 2000
Back Orifice Plug-ins
SubSeven
CyberSpy Telnet Program
Subroot Telnet Trojan
Let Me Rule! 2.0 BETA 9
Donald Dick
RECUB
Loki
Loki Countermeasures
Atelier Web Remote Commander
Trojan Horse Construction Kit
How to Detect Trojans?
Netstat
fPort
TCPView
CurrPorts Tool
Process Viewer
Delete Suspicious Device Drivers
What's on My Computer?
Super System Helper Tool
Inzider-Tracks Processes and Ports
What's Running on My Computer?
MS Configuration Utility

Registry- What's Running
Autoruns
Hijack This (System Checker)
Startup List
Anti-Trojan Software
Evading Anti-Virus Techniques
Evading Anti-Trojan/Anti-Virus using Stealth Tools v 2.0
Backdoor Countermeasures
Tripwire
System File Verification
MD5 Checksum
Microsoft Windows Defender
How to Avoid a Trojan Infection?
Summary

Module: Sniffers

Scenario
Module Objectives
Module Flow
Definition - Sniffing
Protocols Vulnerable to Sniffing
Tool: Network View – Scans the Network for Devices
Ethereal
Displaying Filters in Ethereal
Following the TCP Stream in Ethereal
tcpdump
Types of Sniffing
Passive Sniffing
Active Sniffing
What is ARP?
ARP Spoofing Attack
How does ARP Spoofing Work?
ARP Poisoning
MAC Duplicating
Tools for ARP Spoofing

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: Dnssppooof
Linux Tool: Dsniff
Linux Tool: Filesnarf
Linux Tool: Mailsnarf
Linux Tool: Msgsnarf
Linux Tool: Sshmitm
Linux Tool: Tcpcill
Linux Tool: Tcpcnice
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

Raw Sniffing Tools and features

Sniffit

Aldebaran

Hunt

NGSSniff

Ntop

Pf

Iptraf

Etherape

Netfilter

Network Probe

Maatec Network Analyzer

Snort

Windump

Etherpeek

Mac Changer

Iris

Netintercept

Windnsspoof

How to Detect Sniffing?

Antisniff Tool

Arpwatch Tool

Scenario

Countermeasures

Summary

Denial-of-Service

Scenario

Module Objectives

Module Flow

Real World Scenario of DoS Attacks

What are Denial-of-Service Attacks?

Goal of DoS

Impact and the Modes of Attack

Types of Attacks

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

Shaft
Trinity
Knight and Kaiten
MStream
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
Worms
Slammer Worm
Spread of Slammer Worm – 30 Min
MyDoom.B
How to Conduct DDoS Attack?
Summary

Module: Social Engineering

Module Objectives
Module Flow
What is Social Engineering?
Security 5 Program
Common Types of Social Engineering
Human-Based Social Engineering
Human-based Impersonation
Technical Support Example
More Social Engineering Example
Dumpster Diving Example
Shoulder Surfing

Computer Based Social Engineering
Insider Attack
Disgruntled Employee
Preventing Insider Threat
 Reverse Social Engineering
Common Targets of Social Engineering
Factors that make Companies Vulnerable to Attack
Why is Social Engineering Effective?
Warning Signs of an Attack
Computer Based Social Engineering
Computer Based Social Engineering: Phishing
Netcraft Anti-Phishing Toolbar
Phases in Social Engineering Attack
Behaviors Vulnerable to Attacks
Impact on the Organization
Countermeasures
Scenario
Policies and Procedures
Security Policies - Checklist
Summary
Phishing Attacks and Identity Theft
What is Phishing?
Phishing Reports
Hidden Frames
URL obfuscation
URL Encoding Techniques
IP Address to Base 10 Formula
HTML Image Mapping Techniques
DNS Cache Poisoning Attack
Identity Theft
How to steal Identity?
Countermeasures

Module: Session Hijacking

Scenario

Module Objectives
Module Flow
What is Session Hijacking?
Spoofing v Hijacking
Steps in Session Hijacking
Types of Session Hijacking
TCP Three-way Handshake
Sequence Numbers
Sequence Number Prediction
TCP/IP hijacking
RST Hijacking
RST Hijacking Tool: `hijack_rst.sh`
Programs that Performs Session Hacking
Juggernaut
Hunt
TTY-Watcher
IP watcher
T-sight
Remote TCP Session Reset Utility (SOLARWINDS)
Paros HTTP Session Hijacking Tool
Dangers that hijacking Pose
Protecting against Session Hijacking
Countermeasures: IPSec
Summary

Module: Hacking Web Servers

Scenario
Module Objectives
Module Flow
How Web Servers Work?
How are Web Servers Compromised?
Web Server Defacement
How are Servers Defaced?
Apache Vulnerability
Attacks against IIS

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

Instant Source
Wget
WebSleuth
BlackWidow
SiteScope Tool
WSDigger Tool – Web Services Testing Tool
CookieDigger Tool
SSLDigger Tool
SiteDigger Tool
Hacking Tool: WindowBomb
Burp
Hacking Tool: cURL
dotDefender
Google Hacking
Google Hacking Database (GHDB)
Acunetix Web Scanner
AppScan-Web Application Scanner
Summary

Module: Web-Based Password Cracking Techniques

Scenario
Module Objectives
Module Flow
Authentication - Definition
Authentication Mechanisms
HTTP Authentication
Basic Authentication
Digest Authentication
Integrated Windows (NTLM) Authentication
Negotiate Authentication
Certificate-based Authentication
Forms-based Authentication
RSA SecurID Token
Biometrics Authentication
Types of Biometrics Authentication

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
Gammalog
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)

Osqli -L Probing

SQL Injection Automated Tools

Hacking Tool: SQLDict

SQLExec

Tool: sqlbf

SQLSmack

SQL2.exe

SQL Injection Countermeasures

Preventive Measures

Preventing SQL Injection Attacks
SQL Injection Blocking Tool: SQL Block
Acunetix Web Vulnerability Scanner
Summary

Module: Hacking Wireless Networks

Scenario
Module Objectives
Module Flow
Introduction to Wireless Networking
Business and Wireless Attacks
Basics
Related Technology and Carrier Networks
802.11a
802.11b – “WiFi”
802.11g
802.11i
802.11n
Availability
Wired vs. Wireless
Terminology
StumbVerter
Types of Wireless Network
Setting up a WLAN
Detecting a Wireless Network
How to Access a WLAN
Advantages
Advantages and Disadvantage of a Wireless Network
Antennas
Cantenna – www.cantenna.com
SSID
Beacon Frames
Is the SSID a Secret?
Authentication and Association
Authentication and (Dis) Association

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

Famous Virus/Worms – JS/Spth

Klez Virus Analysis - 1

Klez Virus Analysis - 2

Klez Virus Analysis - 3

Klez Virus Analysis - 4

Klez Virus Analysis - 5

Writing a Simple Virus Program

Virus Construction Kits

Virus Detection Methods

Virus Incident Response

What is Sheep Dip?

Virus Analysis – IDA Pro Tool

Prevention is better than Cure

Latest viruses

Top 10 Viruses- 2006

Anti-Virus Software

AVG Antivirus

Norton Antivirus

McAfee

Socketsheild

Popular Anti-Virus Packages

Virus Databases

Jason Springfield Methodology

Summary

Module: Physical Security

Real World Scenario

Module Objectives

Module Flow

Security Statistics

Physical Security Breach Incidents

Understanding Physical Security

Physical Security

Why Physical Security is Needed?

Who is Accountable?

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

SARA (Security Auditor's Research Assistant)

Linux Tool: Netcat

Linux Tool: tcpdump

Linux Tool: Snort

LINUX TOOL: SAINT

Linux tool: Ethereal

Linux tool: Abacus Portentry

Dsniff collection

Linux tool:Hping2

Linux tool: Sniffit

Linux tool: Nemesis

Linux Tool:LSOF

Linux tool:IPTraF

Linux tool: LIDS

Hacking tool:Hunt

TCP Wrappers

Linux Loadable Kernel Modules

Linux Rootkits

Rootkits: Knark and Torn

Tuxit, Adore, Ramen

Beastkit

Rootkit Countermeasures

chkrootkit Detects the Following Rootkits

Linux Tool : Application Security : Whisker

Advanced Intrusion Detection Environment (AIDE)

Linux Tool: Security Testing Tools

Tool: Encryption

Log and Traffic Monitors

Linux Security Auditing Tool (LSAT)

Linux Security Countermeasures

Steps for Hardening Linux

Summary

Module: Evading IDS, Firewalls and Detecting Honey Pots

Scenario

Module Objectives
Module Flow
Introduction
Terminology
Intrusion Detection System (IDS)
IDS Placement
Ways to Detect an Intrusion
Types of Intrusion 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

Stateful Multilayer Inspection 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 and IDS
IDS testing tool: IDS Informer
IDS Testing Tool: Evasion Gateway
IDS testing tool: Firewall Informer
What is Honeybot?
The Honeybot Project
Types of Honeybots
Advantages of Honeybots
Where to place Honeybots?
Honeybots
Honeybot-Specter
Honeybot – Honeyd
Honeybot – KFSensor
Sebek
Physical and Virtual Honeybots
Tools to Detect Honeybots
What to do when hacked?
Summary

Module: Buffer Overflows

Module Objectives
Module Flow
Introduction
Why are Programs/Applications Vulnerable?

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