

EC-Council CEH v.7

Course Introduction

5m

Course Introduction

Module 00 - Student Introduction

5m

Student Introduction

Course Materials

CEHv7 Course Outline

EC-Council Certification Program

Certified Ethical Hacker Track

CEHv7 Exam Information

Lab Sessions

What Does CEH Teach You?

What CEH is NOT?

Remember This!

CEH Class Speed

Live Hacking Website

Let's Start Hacking!

Module 01 - Introduction to Ethical Hacking

1h

Module Flow: Info Security Overview

Security News

Case Study

Scenario: How Simple Things Can Get You into Trouble?

Internet Crime Current Report: IC3

Data Breach Investigations Report

Types of Data Stolen From the Organizations

Essential Terminologies

Elements of Information Security

Authenticity and Non-Repudiation

The Security, Functionality, and Usability Triangle

Security Challenges

Module Flow: Hacking Concepts

Effects of Hacking

Effects of Hacking on Business

Who is a Hacker?

Hacker Classes

Hacktivism

Module Flow: Hacking Phases

What Does a Hacker Do?

Phase 1 - Reconnaissance

Phase 2 - Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Covering Tracks

Module Flow: Types of Attacks

Types of Attacks on a System

Operating System Attacks

Application-Level Attacks

Shrink Wrap Code Attacks

Misconfiguration Attacks

Module Flow: Ethical Hacking

Why Ethical Hacking is Necessary?

Defense in Depth

Scope and Limitations of Ethical Hacking

What Do Ethical Hackers Do?

Skills of an Ethical Hacker

Module Flow: Vulnerability Research

Vulnerability Research

Vulnerability Research Websites

Demo - Vulnerability Research Website

What is Penetration Testing?

Why Penetration Testing?

Penetration Testing Methodology

Quotes

Module 01 Review

Module 02 - Footprinting and Reconnaissance

2h 23m

Module Flow: Footprinting Concepts

Security News

Footprinting Terminologies

What is Footprinting?

Objectives of Footprinting

Module Flow: Footprinting Threats

Footprinting Threats

Module Flow: Footprinting Methodology

Footprinting Methodology: Internet Footprinting

Finding a Company's URL

Locate Internal URLs

Public and Restricted Websites

Search for Company's Information

Tools to Extract Company's Data

Footprinting Through Search Engines

Demo - Footprinting Through Search Engines

Collect Location Information

Satellite Picture of a Residence

People Search

People Search Using <http://pipl.com>

People Search Online Services

Demo - People Search Using Online Services

People Search on Social Networking Services

Gather Information from Financial Services

Footprinting Through Job Sites

Monitoring Target Using Alerts

Footprinting Methodology: Competitive Intelligence

Competitive Intelligence Gathering

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

Competitive Intelligence - What are the Company's Plans?

Competitive Intelligence - What Expert Opinion Say About the Company?

Competitive Intelligence Tools

Competitive Intelligence Consulting Companies

Footprinting Methodology: WHOIS Footprinting

WHOIS Lookup

WHOIS Lookup Result Analysis

WHOIS Lookup Tools: SmartWhois

Demo - SmartWhois

WHOIS Lookup Tools

WHOIS Lookup Online Tools

Footprinting Methodology: DNS Footprinting

Extracting DNS Information

Demo - DNS Overview
DNS Interrogation Tools
DNS Interrogation Online Tools
Footprinting Methodology: Network Footprinting
Locate the Network Range
Traceroute
Traceroute Analysis
Traceroute Tool: 3D Traceroute
Traceroute Tool: LortotPro
Traceroute Tool: Path Analyzer Pro
Traceroute Tools
Footprinting Methodology: Website Footprinting
Mirroring Entire Website
Demo - HTTrack and Website Watcher
Website Mirroring Tools
Mirroring Entire Website Tools
Extract Website Information from <http://www.archive.org>
Monitoring Web Updates Using Website Watcher
Footprinting Methodology: E-mail Footprinting
Tracking Email Communications
Email Tracking Tools
Demo - Tracking Emails with ReadNotify
Footprinting Methodology: Google Hacking
Footprint Using Google Hacking Techniques
What a Hacker Can Do With Google Hacking?
Google Advance Search Operators
Finding Resources using Google Advance Operator
Demo - Google Hacking
Google Hacking Tool: Google Hacking Database (GHDB)
Google Hacking Tools
Module Flow: Footprinting Tools
Additional Footprinting Tools
Module Flow: Footprinting Countermeasures
Footprinting Countermeasures
Module Flow: Footprinting Pen Testing
Footprinting Pen Testing
Quotes
Module 02 Summary

Module 03 - Scanning Networks

1h 44m

Scanning Networks
Security News
Network Scanning
Types of Scanning
CEH Scanning Methodology: Check for Live System
Checking for Live Systems - ICMP Scanning
Ping Sweep
Ping Sweep Tools
Demo - Angry IP
CEH Scanning Methodology: Check for Open Ports
Three-Way Handshake
TCP Communication Flags
Create Custom Packet using TCP Flags
Hping2/Hping3
Hping3 Screenshot
Hping Commands

Scanning Techniques
TCP Connect/Full Open Scan
Stealth Scan (Half-open Scan)
Xmas Scan
FIN Scan
NULL Scan
IDLE Scan
IDLE Scan: Step 1
IDLE Scan: Step 2.1 (Open Port)
IDLE Scan: Step 2.2 (Closed Port)
IDLE Scan: Step 3
ICMP Echo Scanning/List Scan
SYN/FIN Scanning Using IP Fragments
UDP Scanning
Inverse TCP Flag Scanning
ACK Flag Scanning
Scanning: IDS Evasion Techniques
IP Fragmentation Tools
Scanning Tool: Nmap
Nmap
Demo - Nmap
Scanning Tool: NetScan Tools Pro
Scanning Tools
Do Not Scan These IP Addresses
Scanning Countermeasures
War Dialing
Why War Dialing?
War Dialing Tools
War Dialing Countermeasures
War Dialing Countermeasures: SandTrap Tool
CEH Scanning Methodology: Banner Grabbing
OS Fingerprinting
Active Banner Grabbing Using Telnet
Demo - Banner Grabbing Using Telnet
Banner Grabbing Tool: ID Serve
GET REQUESTS
Banner Grabbing Tool: Netcraft
Demo - Footprinting Webservers Using Netcraft
Banner Grabbing Tools
Banner Grabbing Countermeasures: Disabling or Changing Banner
Hiding File Extensions
Hiding File Extensions from Webpages
CEH Scanning Methodology: Scan for Vulnerability
Vulnerability Scanning
Nessus: Screenshot
Demo - Vulnerability Scanning with Nessus
Vulnerability Scanning Tool: SAINT
GFI LANGuard
Network Vulnerability Scanners
CEH Scanning Methodology: Draw Network Diagrams
LANsurveyor
LANsurveyor: Screenshot
Network Mappers
CEH Scanning Methodology: Prepare Proxies
Proxy Servers
Why Attackers Use Proxy Servers?

Use of Proxies for Attack
How Does MultiProxy Work?
Free Proxy Servers
Proxy Workbench
Proxifier Tool: Create Chain of Proxy Servers
SocksChain
TOR (The Onion Routing)
TOR Proxy Chaining Software
HTTP Tunneling Techniques
Why do I Need HTTP Tunneling?
Super Network Tunnel Tool
Httpunnel for Windows
Additional HTTP Tunneling Tools
SSH Tunneling
SSL Proxy Tool
How to Run SSL Proxy?
Proxy Tools
Anonymizers
Types of Anonymizers
Case: Bloggers Write Text Backwards to Bypass Web Filters in China
Text Conversion to Avoid Filters
Censorship Circumvention Tool: Psiphon
How Psiphon Works?
Psiphon: Screenshot
How to Check if Your Website is Blocked in China or Not?
G-Zapper
Anonymizers (Cont.)
Spoofing IP Address
IP Spoofing Detection Techniques: Direct TTL Probes
IP Spoofing Detection Techniques: IP Identification Number
IP Spoofing Detection Techniques: TCP Flow Control Method
IP Spoofing Countermeasures
Scanning Penetration Testing
Scanning Pen Testing
Quotes
Module 03 Review

Module 04 - Enumeration

48m

Module Flow: Enumeration Concepts

Security News
What is Enumeration?
Techniques of Enumeration

Module Flow: NetBIOS Enumeration

Netbios Enumeration
NetBIOS Enumeration Tool: SuperScan
Demo - Enumerating Users Using Null Sessions
NetBIOS Enumeration Tool: NetBIOS Enumerator
Enumerating User Accounts
Enumerate Systems Using Default Passwords

Module Flow: SNMP Enumeration

SNMP (Simple Network Management Protocol) Enumeration
Management Information Base (MIB)
SNMP Enumeration Tool: OpUtils Network Monitoring Toolset
SNMP Enumeration Tool: SolarWinds
Demo - SNMP Enumeration with Solar Winds
SNMP Enumeration Tools

Module Flow: UNIX/Linux Enumeration

UNIX/Linux Enumeration

Linux Enumeration Tool: Enum4linux

Module Flow: LDAP Enumeration

LDAP Enumeration

LDAP Enumeration Tool: JXplorer

LDAP Enumeration Tool

Module Flow: NTP Enumeration

NTP Enumeration

NTP Server Discovery Tool: NTP Server Scanner

NTP Server: Presentense Time Server

NTP Enumeration Tools

Module Flow: SMTP Enumeration

SMTP Enumeration

SMTP Enumeration Tool: NetScanTools Pro

Module Flow: DNS Enumeration

DNS Zone Transfer Enumeration Using nslookup

Demo - Enumerating DNS Using nslookup

DNS Analyzing and Enumeration Tool: The Men & Mice Suite

Module Flow: Enumeration Countermeasures

Enumeration Countermeasures

SMB Enumeration Countermeasures

Module Flow: Enumeration Pen Testing

Enumeration Pen Testing

Quotes

Module 04 Review

Module 05 - System Hacking

2h 40m

System Hacking

Security News

Information at Hand Before System Hacking Stage

System Hacking: Goals

CEH Hacking Methodology (CHM)

CEH System Hacking Steps: Cracking Passwords

Password Cracking

Password Complexity

Password Cracking Techniques

Demo - Password Cracking with Cain

Types of Password Attacks

Passive Online Attacks: Wire Sniffing

Password Sniffing

Passive Online Attack: Man-in-the-Middle and Replay Attack

Active Online Attack: Password Guessing

Active Online Attack: Trojan/Spyware/Keylogger

Active Online Attack: Hash Injection Attack

Rainbow Attacks: Pre-Computed Hash

Distributed Network Attack

Elcomsoft Distributed Password Recovery

Demo - Distributed Password Cracking with Elcomsoft

Non-Electronic Attacks

Demo - Spytector

Default Passwords

Manual Password Cracking (Guessing)

Automatic Password Cracking Algorithm

Stealing Passwords Using USB Drive

Microsoft Authentication

How Hash Passwords are Stored in Windows SAM?
What is LAN Manager Hash?
LM "Hash" Generation
LM, NTLMv1, and NTLMv2
NTLM Authentication Process
Kerberos Authentication
Salting
PWdump7 and Fgdump
L0phtCrack
Ophcrack
Cain & Abel
RainbowCrack
Password Cracking Tools
LM Hash Backward Compatibility
How to Disable LM HASH?
How to Defend against Password Cracking?
Implement and Enforce Strong Security Policy
CEH System Hacking Steps: Escalating Privileges
Privilege Escalation
Escalation of Privileges
Active@Password Changer
Privilege Escalation Tools
How to Defend against Privilege Escalation?
CEH System Hacking Steps: Executing Applications
Executing Applications
Alchemy Remote Executor
RemoteExec
Execute This!
Keylogger
Types of Keystroke Loggers
Acoustic/CAM Keylogger
Keylogger: Advanced Keylogger
Keylogger: Spytech SpyAgent
Keylogger: Perfect Keylogger
Keylogger: Powered Keylogger
Keylogger for Mac: Aobo Mac OS X KeyLogger
Keylogger for Mac: Perfect Keylogger for Mac
Hardware Keylogger: KeyGhost
Keyloggers
Spyware
What Does the Spyware Do?
Types of Spywares
Desktop Spyware
Desktop Spyware: Activity Monitor
Desktop Spyware (Cont.)
Email and Internet Spyware
Email and Internet Spyware: eBLASTER
Internet and E-mail Spyware
Child Monitoring Spyware
Child Monitoring Spyware: Advanced Parental Control
Child Monitoring Spyware (Cont.)
Screen Capturing Spyware
Screen Capturing Spyware: Spector Pro
Screen Capturing Spyware (Cont.)
USB Spyware
USB Spyware: USBDumper

USB Spyware (Cont.)
Audio Spyware
Audio Spyware: RoboNanny, Stealth Recorder Pro and Spy Voice Recorder
Video Spyware
Video Spyware: Net Video Spy
Video Spyware (Cont.)
Print Spyware
Print Spyware: Printer Activity Monitor
Print Spyware (Cont.)
Telephone/Cellphone Spyware
Cellphone Spyware: Mobile Spy
Telephone/Cellphone Spyware (Cont.)
GPS Spyware
GPS Spyware: GPS TrackMaker
GPS Spyware (Cont.)
How to Defend against Keyloggers?
Anti-Keylogger
Anti-Keylogger: Zemana AntiLogger
Anti-Keyloggers
How to Defend against Spyware?
Anti-Spyware: Spyware Doctor
Anti-Spywares
CEH System Hacking Steps: Hiding Files
Rootkits
Types of Rootkits
How Rootkit Works?
Rootkit: Fu
Demo - Fu Rootkit
Detecting Rootkits
Steps for Detecting Rootkits
How to Defend against Rootkits?
Anti-Rootkit: RootkitRevealer and McAfee Rootkit Detective
Anti-Rootkits
NTFS Data Stream
How to Create NTFS Streams?
NTFS Stream Manipulation
How to Defend against NTFS Streams?
Demo - Creating Alternate Data Streams
NTFS Stream Detector: ADS Scan Engine
NTFS Stream Detectors
What is Steganography?
Steganography Techniques
How Steganography Works?
Types of Steganography
Whitespace Steganography Tool: SNOW
Image Steganography
Image Steganography: Hermetic Stego
Image Steganography Tools
Document Steganography: wbStego
Document Steganography Tools
Video Steganography: Our Secret
Video Steganography Tools
Audio Steganography: Mp3stegz
Audio Steganography Tools
Folder Steganography: Invisible Secrets 4
Demo - Steganography

Folder Steganography Tools
Spam/Email Steganography: Spam Mimic
Natural Text Steganography: Sams Big G Play Maker
Steganalysis
Steganalysis Methods/Attacks on Steganography
Steganography Detection Tool: Stegdetect
Steganography Detection Tools
CEH System Hacking Steps: Covering Tracks
Why Cover Tracks?
Covering Tracks
Ways to Clear Online Tracks
Disabling Auditing: Auditpol
Covering Tracks Tool: Window Washer
Covering Tracks Tool: Tracks Eraser Pro
Track Covering Tools
CEH System Hacking Steps: Penetration Testing
Password Cracking (Cont.)
Privilege Escalation (Cont.)
Executing Applications (Cont.)
Hiding Files
Covering Tracks (Cont.)
Quotes
Module 05 Review

Module 06 - Trojans and Backdoors

1h 16m

Module Flow: Trojan Concepts

Security News
What is a Trojan?
Overt and Covert Channels
Purpose of Trojans
What Do Trojan Creators Look For?
Indications of a Trojan Attack
Common Ports used by Trojans

Module Flow: Trojan Infection

How to Infect Systems Using a Trojan?
Wrappers
Wrapper Covert Programs
Different Ways a Trojan can Get into a System
How to Deploy a Trojan?
Evading Anti-Virus Techniques

Module Flow: Types of Trojans

Types of Trojans
Command Shell Trojans
Command Shell Trojan: Netcat
Demo - Netcat
GUI Trojan: MoSucker
GUI Trojan: Jumper and Biodox
Document Trojans
E-mail Trojans
E-mail Trojans: RemoteByMail
Defacement Trojans
Defacement Trojans: Restorator
Botnet Trojans
Botnet Trojan: Illusion Bot
Botnet Trojan: NetBot Attacker
Proxy Server Trojans

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

FTP Trojans

FTP Trojan: TinyFTPD

VNC Trojans

HTTP/HTTPS Trojans

HTTP Trojan: HTTP RAT

Sshcp Trojan - HTTPS (SSL)

ICMP Tunneling

ICMP Trojan: icmpsend

Remote Access Trojans

Demo - Beast

Remote Access Trojan: RAT DarkComet

Remote Access Trojan: Apocalypse

Covert Channel Trojan: CCTT

E-banking Trojans

Banking Trojan Analysis

E-banking Trojan: ZeuS

Destructive Trojans

Notification Trojans

Credit Card Trojans

Data Hiding Trojans (Encrypted Trojans)

BlackBerry Trojan: PhoneSnoop

MAC OS X Trojan: DNSChanger

Mac OS X Trojan: Hell Raiser

Module Flow: Trojan Detection

How to Detect Trojans?

Scanning for Suspicious Ports

Port Monitoring Tool: IceSword

Port Monitoring Tools: CurrPorts and TCPView

Scanning for Suspicious Processes

Process Monitoring Tool: What's Running

Process Monitoring Tools

Scanning for Suspicious Registry Entries

Registry Entry Monitoring Tools

Scanning for Suspicious Device Drivers

Device Drivers Monitoring Tools: DriverView

Device Drivers Monitoring Tools

Scanning for Suspicious Windows Services

Windows Services Monitoring Tools: Windows Service Manager (SrvMan)

Windows Services Monitoring Tools

Scanning for Suspicious Startup Programs

Windows7 Startup Registry Entries

Startup Programs Monitoring Tools: Starter

Startup Programs Monitoring Tools: Security AutoRun

Startup Programs Monitoring Tools

Demo - What's Running?

Scanning for Suspicious Files and Folders

Files and Folder Integrity Checker: FastSum and WinMD5

Files and Folder Integrity Checker

Scanning for Suspicious Network Activities

Detecting Trojans and Worms with Capsa Network Analyzer

Module Flow: Countermeasures

Trojan Countermeasures

Backdoor Countermeasures

Trojan Horse Construction Kit

Module Flow: Anti-Trojan Software

Anti-Trojan Software: TrojanHunter
Anti-Trojan Software: Emsisoft Anti-Malware
Anti-Trojan Softwares
Module Flow: Penetration Testing
Pen Testing for Trojans and Backdoors
Quotes
Module 06 Review

Module 07 - Viruses and Worms

40m

Module Flow: Virus and Worms Concepts

Security News
Introduction to Viruses
Virus and Worm Statistics 2010
Stages of Virus Life
Working of Viruses: Infection Phase
Working of Viruses: Attack Phase
Why Do People Create Computer Viruses?
Indications of Virus Attack
How does a Computer get Infected by Viruses?
Virus Hoaxes
Virus Analysis: W32/Sality.AA
Virus Analysis: W32/Toal-A
Virus Analysis: W32/Virut
Virus Analysis: Klez

Module Flow: Types of Viruses

Types of Viruses
System or Boot Sector Viruses
File and Multipartite Viruses
Macro Viruses
Cluster Viruses
Stealth/Tunneling Viruses
Encryption Viruses
Polymorphic Code
Metamorphic Viruses
File Overwriting or Cavity Viruses
Sparse Infector Viruses
Companion/Camouflage Viruses
Shell Viruses
File Extension Viruses
Add-on and Intrusive Viruses
Transient and Terminate and Stay Resident Viruses
Writing a Simple Virus Program
Terabit Virus Maker
JPS Virus Maker
Demo - JPS Virus Maker Tool
DELmE's Batch Virus Maker

Module Flow: Computer Worms

Computer Worms
How is a Worm Different from a Virus?
Example of Worm Infection: Conficker Worm
What does the Conficker Worm do?
How does the Conficker Worm Work?
Worm Analysis: W32/Netsky
Worm Analysis: W32/Bagle.GE
Worm Maker: Internet Worm Maker Thing

Module Flow: Malware Analysis

What is Sheep Dip Computer?
Anti-Virus Sensors Systems
Malware Analysis Procedure: Preparing Testbed
Malware Analysis Procedure
String Extracting Tool: Bintext
Compression and Decompression Tool: UPX
Process Monitoring Tools: Process Monitor
Log Packet Content Monitoring Tools: NetResident
Debugging Tool: Ollydbg
Virus Analysis Tool: IDA Pro
Online Malware Testing: Sunbelt CWSandbox
Online Malware Testing: VirusTotal
Online Malware Analysis Services
Module Flow: Countermeasures
Virus Detection Methods
Virus and Worms Countermeasures
Companion Antivirus: Immundet Protect
Anti-virus Tools
Module Flow: Penetration Testing
Penetration Testing for Virus
Quotes
Module 07 Review

Module 08 - Sniffers

1h 32m

Module Flow: Sniffing Concepts

Security News
Lawful Intercept
Benefits of Lawful Intercept
Network Components Used for Lawful Intercept
Wiretapping
Sniffing Threats
How a Sniffer Works?
Hacker Attacking a Switch
Types of Sniffing: Passive Sniffing
Types of Sniffing: Active Sniffing
Protocols Vulnerable to Sniffing
Tie to Data Link Layer in OSI Model
Hardware Protocol Analyzers
SPAN Port

Module Flow: MAC Attacks

MAC Flooding
MAC Address/CAM Table
How CAM Works?
What Happens When CAM Table is Full?
Mac Flooding Switches with macof
MAC Flooding Tool: Yersinia
How to Defend against MAC Attacks?

Module Flow: DHCP Attacks

How DHCP Works?
DHCP Request/Reply Messages
IPv4 DHCP Packet Format
DHCP Starvation Attack
Rogue DHCP Server Attack
DHCP Starvation Attack Tool: Gobbler
How to Defend Against DHCP Starvation and Rogue Server Attack?

Module Flow: ARP Poisoning Attacks

What is Address Resolution Protocol (ARP)?
ARP Spoofing Attack
How Does ARP Spoofing Work?
Threats of ARP Poisoning
ARP Poisoning Tool: Cain and Abel
Demo - Active Sniffing with Cain
Demo - Actively Sniffing a Switched Network with Cain
ARP Poisoning Tool: WinArpAttacker
ARP Poisoning Tool: Ufasoft Snif
How to Defend Against ARP Poisoning?
Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

Module Flow: Spoofing Attack

MAC Spoofing/Duplicating
Spoofing Attack Threats
MAC Spoofing Tool: SMAC
Demo - Spoofing the MAC Address
How to Defend Against MAC Spoofing?

Module Flow: DNS Poisoning

DNS Poisoning Techniques
Intranet DNS Spoofing
Proxy Server DNS Poisoning
DNS Cache Poisoning
How to Defend Against DNS Spoofing?

Module Flow: Sniffing Tools

Sniffing Tool: Wireshark
Demo - Packet Capturing with Wireshark
Follow TCP Stream in Wireshark
Display Filters in Wireshark
Additional Wireshark Filters
Sniffing Tool: CACE Pilot
Sniffing Tool: Tcpdump/Windump
Discovery Tool: NetworkView
Discovery Tool: The Dude Sniffer
Password Sniffing Tool: Ace
Packet Sniffing Tool: Capsa Network Analyzer
OmniPeek Network Analyzer
Network Packet Analyzer: Observer
Session Capture Sniffer: NetWitness
Email Message Sniffer: Big-Mother
TCP/IP Packet Crafter: Packet Builder
Additional Sniffing Tools
How an Attacker Hacks the Network Using Sniffers?

Module Flow: Countermeasures

How to Defend Against Sniffing?
Sniffing Prevention Techniques
How to Detect Sniffing?
Promiscuous Detection Tool: PromqryUI
Promiscuous Detection Tool: PromiScan
Quotes
Module 08 Review

Module 09 - Social Engineering

Module Flow: Social Engineering Concepts

Security News
What is Social Engineering?

48m

Behaviors Vulnerable to Attacks
Factors that Make Companies Vulnerable to Attacks
Why is Social Engineering Effective?
Warning Signs of an Attack
Phases in a Social Engineering Attack
Impact on the Organization
Command Injection Attacks
"Rebecca" and "Jessica"
Common Targets of Social Engineering
Common Targets of Social Engineering: Office Workers

Module Flow: Social Engineering Techniques

Types of Social Engineering
Human-Based Social Engineering
Technical Support Example
Authority Support Example
Human-Based Social Engineering (Cont.)
Human-Based Social Engineering: Dumpster Diving
Human-Based Social Engineering (Cont..)
Watch these Movies
Watch this Movie
Computer-Based Social Engineering
Computer-Based Social Engineering: Pop-Ups
Computer-Based Social Engineering: Phishing
Social Engineering Using SMS
Social Engineering by a "Fake SMS Spying Tool"
Insider Attack
Disgruntled Employee
Preventing Insider Threats
Common Intrusion Tactics and Strategies for Prevention

Module Flow: Impersonation on Social Networking Sites

Social Engineering Through Impersonation on Social Networking Sites
Social Engineering Example: LinkedIn Profile
Social Engineering on Facebook
Social Engineering on Twitter
Social Engineering on Orkut
Social Engineering on MySpace
Risks of Social Networking to Corporate Networks

Module Flow: Identity Theft

Identity Theft Statistics 2010
Identity Theft
How to Steal an Identity?
Step 1
Step 2
Comparison
Step 3
Real Steven Gets Huge Credit Card Statement
Identity Theft - Serious Problem

Module Flow: Social Engineering Countermeasures

Social Engineering Countermeasures: Policies
Social Engineering Countermeasures
How to Detect Phishing Emails?
Anti-Phishing Toolbar: Netcraft
Demo - Netcraft Anti-Phishing Toolbar
Anti-Phishing Toolbar: PhishTank
Identity Theft Countermeasures

Module Flow: Penetration Testing

Social Engineering Pen Testing
Social Engineering Pen Testing: Using Emails
Social Engineering Pen Testing: Using Phone
Social Engineering Pen Testing: In Person
Quotes
Module 09 Review

Module 10 - Denial of Service

30m

Module Flow: DoS/DDoS Concepts

Security News
What is a Denial of Service Attack?
What are Distributed Denial of Service Attacks?
How Distributed Denial of Service Attacks Work?
Symptoms of a DoS Attack
Cyber Criminals
Organized Cyber Crime: Organizational Chart
Internet Chat Query (ICQ)
Internet Relay Chat (IRC)

Module Flow: DoS/DDoS Attack Techniques

DoS Attack Techniques
Bandwidth Attacks
Service Request Floods
SYN Attack
Demo - SynFlooding with hping2
SYN Flooding
ICMP Flood Attack
Peer-to-Peer Attacks
Permanent Denial-of-Service Attack
Application Level Flood Attacks

Module Flow: Botnets

Botnet
Botnet Propagation Technique
Botnet Ecosystem
Botnet Trojan: Shark
Poison Ivy: Botnet Command Control Center
Botnet Trojan: PlugBot

Module Flow: DDoS Case Study

Wikileaks
DDoS Attack
DDoS Attack Tool: LOIC
Denial of Service Attack Against MasterCard, Visa, and Swiss Banks
Hackers Advertise Links to Download Botnet

Module Flow: DoS/DDoS Attack Tools

DoS Attack Tools

Module Flow: Countermeasures

Detection Techniques
Activity Profiling
Wavelet Analysis
Sequential Change-Point Detection
DoS/DDoS Countermeasure Strategies
DDoS Attack Countermeasures
DoS/DDoS Countermeasures: Project Secondary Victims
DoS/DDoS Countermeasures: Detect and Neutralize Handlers
DoS/DDoS Countermeasures: Detect Potential Attacks
DoS/DDoS Countermeasures: Deflect Attacks
DoS/DDoS Countermeasures: Mitigate Attacks

Post-Attack Forensics
Techniques to Defend against Botnets
DoS/DDoS Countermeasures
DoS/DDoS Protection at ISP Level
Enabling TCP Intercept on Cisco IOS Software
Advanced DDoS Protection: IntelliGuard DDoS Protection System (DPS)

Module Flow: DoS/DDoS Protection Tools

DoS/DDoS Protection Tool: NetFlow Analyzer
DoS/DDoS Protection Tools

Module Flow: DoS/DDoS Penetration Testing

Denial of Service (DoS) Attack Penetration Testing
Denial of Service (DoS) Attack Pen Testing
Quotes
Module 10 Review

Module 11 - Session Hijacking

32m

Module Flow: Session Hijacking Concepts

Security News
What is Session Hijacking?
Dangers Posed by Hijacking
Why Session Hijacking is Successful?
Key Session Hijacking Techniques
Brute Forcing
Brute Forcing Attack
HTTP Referrer Attack
Spoofing vs. Hijacking
Session Hijacking Process
Packet Analysis of a Local Session Hijack
Types of Session Hijacking
Session Hijacking in OSI Model

Module Flow: Application Level Session Hijacking

Application Level Session Hijacking
Session Sniffing
Predictable Session Token
How to Predict a Session Token?
Man-in-the-Middle Attack
Man-in-the-Browser Attack
Steps to Perform Man-in-the-Browser Attack
Client-side Attacks
Cross-site Script Attack
Session Fixation
Session Fixation Attack

Module Flow: Network Level Session Hijacking

Network Level Session Hijacking
The 3-Way Handshake
Sequence Numbers
Sequence Number Prediction
TCP/IP Hijacking
IP Spoofing: Source Routed Packets
RST Hijacking
Blind Hijacking
Man-in-the-Middle Attack using Packet Sniffer
UDP Hijacking

Module Flow: Session Hijacking Tools

Session Hijacking Tool: Paros
Session Hijacking Tool: Burp Suite

Demo - Session Hijacking with Burp

Session Hijacking Tool: Firesheep

Session Hijacking Tools

Module Flow: Countermeasures

Countermeasures

Protecting against Session Hijacking

Methods to Prevent Session Hijacking: To be Followed by Web Developers

Methods to Prevent Session Hijacking: To be Followed by Web Users

Defending against Session Hijack Attacks

Session Hijacking Remediation

IPSec

Modes of IPSec

IPSec Architecture

IPSec Authentication and Confidentiality

Components of IPSec

IPSec Implementation

Module Flow: Penetration Testing

Session Hijacking Pen Testing

Quotes

Module 11 Review

Module 12 - Hacking Webservers

1h 5m

Module Flow: Webserver Concepts

Security News

Webserver Market Shares

Open Source Webserver Architecture

IIS Webserver Architecture

Website Defacement

Case Study

Why Web Servers are Compromised?

Impact of Webserver Attacks

Module Flow: Webserver Threats

Webserver Misconfiguration

Example

Directory Traversal Attacks

Demo - Performing a Directory Traversal Attack

HTTP Response Splitting Attack

Web Cache Poisoning Attack

HTTP Response Hijacking

SSH Bruteforce Attack

Man-in-the-Middle Attack

Webserver Password Cracking

Webserver Password Cracking Techniques

Web Application Attacks

Module Flow: Attack Methodology

Webserver Attack Methodology

Webserver Attack Methodology: Information Gathering

Demo - Fingerprinting Webserver with HTTPRecon

Webserver Attack Methodology: Webserver Footprinting

Webserver Footprinting Tools

Webserver Attack Methodology: Mirroring a Website

Webserver Attack Methodology: Vulnerability Scanning

Webserver Attack Methodology: Session Hijacking

Webserver Attack Methodology: Hacking Web Passwords

Module Flow: Webserver Attack Tools

Webserver Attack Tools: Metasploit

Metasploit Architecture
Metasploit Exploit Module
Metasploit Payload Module
Metasploit Auxiliary Module
Metasploit NOPS Module
Webserver Attack Tools: Wfetch
Web Password Cracking Tool: Brutus
Web Password Cracking Tool: THC-Hydra
Module Flow: Countermeasures
Countermeasures: Patches and Updates
Countermeasures: Protocols
Demo - Web-based Password Cracking with Brutus
Countermeasures: Accounts
Countermeasures: Files and Directories
How to Defend Against Web Server Attacks?
How to Defend against HTTP Response Splitting and Web Cache Poisoning
Module Flow: Patch Management
Patches and Hotfixes
What is Patch Management?
Identifying Appropriate Sources for Updates and Patches
Installation of a Patch
Implementation and Verification of a Security Patch or Upgrade
Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)
Patch Management Tools
Module Flow: Webserver Security Tools
Web Application Security Scanner: Sandcat
Web Server Security Scanner: Wikto
Webserver Malware Infection Monitoring Tool: HackAlert
Webserver Security Tools
Module Flow: Webserver Pen Testing
Webserver Pen Testing
Web Server Penetration Testing
Quotes
Module 12 Review

Module 13 - Hacking Web Applications

1h 50m

Module Flow: Web App Concepts

Security News
Web Application Security Statistics
Introduction to Web Applications
Web Application Components
How Web Applications Work?
Web Application Architecture
Web 2.0 Applications
Vulnerability Stack
Web Attack Vectors

Module Flow: Web App Threats

Web Application Threats - 1
Web Application Threats - 2
Unvalidated Input
Parameter/Form Tampering
Directory Traversal
Security Misconfiguration
Injection Flaws
SQL Injection Attacks
Command Injection Attacks

Demo - Web Vulnerability Scanning with Acunetix
Command Injection Example
File Injection Attack
What is LDAP Injection?
How LDAP Injection Works?
Hidden Field Manipulation Attack
Cross-Site Scripting (XSS) Attacks
How XSS Attacks Work?
Cross-Site Scripting Attack Scenario: Attack via Email
XSS Example: Attack via Email
XSS Example: Stealing Users' Cookies
XSS Example: Sending as Unauthorized Request
XSS Attack in Blog Posting
XSS Attack in Comment Field
XSS Cheat Sheet
Cross-Site Request Forgery (CSRF) Attack
How CSRF Attacks Work?
Web Application Denial-of-Service (DoS) Attack
Denial of Service (DoS) Examples
Buffer Overflow Attacks
Cookie/Session Poisoning
How Cookie Poisoning Works?
Session Fixation Attack
Insufficient Transport Layer Protection
Improper Error Handling
Insecure Cryptographic Storage
Broken Authentication and Session Management
Unvalidated Redirects and Forwards
Web Services Architecture
Web Services Attack
Web Services Footprinting Attack
Web Services XML Poisoning
Module Flow: Hacking Methodology
Web App Hacking Methodology: Footprint Web Infrastructure
Footprint Web Infrastructure
Footprint Web Infrastructure: Server Discovery
Footprint Web Infrastructure: Service Discovery
Footprint Web Infrastructure: Server Identification/Banner Grabbing
Footprint Web Infrastructure: Hidden Content Discovery
Web Spidering Using Burp Suite
Web App Hacking Methodology: Attack Web Servers
Hacking Web Servers
Web Server Hacking Tool: WebInspect
Web App Hacking Methodology: Analyze Web Applications
Analyze Web Applications
Analyze Web Applications: Identify Entry Points for User Input
Analyze Web Applications: Identify Server-Side Technologies
Analyze Web Applications: Identify Server-Side Functionality
Analyze Web Applications: Map the Attack Surface
Web App Hacking Methodology: Attack Authentication Mechanism
Attack Authentication Mechanism
Username Enumeration
Password Attacks: Password Functionality Exploits
Password Attacks: Password Guessing
Password Attacks: Brute-forcing
Session Attacks: Session ID Prediction/Brute-forcing

Cookie Exploitation: Cookie Poisoning
Web App Hacking Methodology: Attack Authorization Schemes
Authorization Attack
HTTP Request Tampering
Authorization Attack: Cookie Parameter Tampering
Web App Hacking Methodology: Attack Session Management Mechanism
Session Management Attack
Attacking Session Token Generation Mechanism
Attacking Session Tokens Handling Mechanism: Session Token Sniffing
Web App Hacking Methodology: Perform Injection Attacks
Injection Attacks
Web App Hacking Methodology: Attack Data Connectivity
Attack Data Connectivity
Connection String Injection
Connection String Parameter Pollution (CSPP) Attacks
Connection Pool DoS
Web App Hacking Methodology: Attack Web Client
Attack Web App Client
Web App Hacking Methodology: Attack Web Services
Attack Web Services
Web Services Probing Attacks
Web Service Attacks: SOAP Injection
Web Service Attacks: XML Injection
Web Services Parsing Attacks
Web Service Attack Tool: soapUI
Web Service Attack Tool: XMLSpy

Module Flow: Web Application Hacking Tools

Web Application Hacking Tool: Burp Suite Professional
Web Application Hacking Tools: CookieDigger
Web Application Hacking Tools: WebScarab
Web Application Hacking Tools

Module Flow: Countermeasures

Encoding Schemes
How to Defend Against SQL Injection Attacks?
How to Defend Against Command Injection Flaws?
How to Defend Against XSS Attacks?
How to Defend Against DoS Attacks?
How to Defend Against Web Services Attack?
Web Application Countermeasures
How to Defend Against Web Application Attacks?

Module Flow: Security Tools

Web Application Security Tool: Acunetix Web Vulnerability Scanner
Web Application Security Tool: Falcove Web Vulnerability Scanner
Web Application Security Scanner: Netsparker
Web Application Security Tool: N-Stalker Web Application Security Scanner
Web Application Security Tools
Web Application Firewall: dotDefender
Web Application Firewall: IBM AppScan
Web Application Firewall: ServerDefenderVP
Web Application Firewall

Module Flow: Web App Pen Testing

Web Application Pen Testing
Information Gathering
Configuration Management Testing
Authentication Testing
Session Management Testing

Authorization Testing
Data Validation Testing
Denial of Service Testing
Web Services Testing
AJAX Testing
Quotes
Module 13 Review

Module 14 - SQL Injection

58m

Module Flow: SQL Injection Concepts

Security News
SQL Injection is the Most Prevalent Vulnerability in 2010
SQL Injection Threats
What is SQL Injection?
SQL Injection Attacks
How Web Applications Work?
Server Side Technologies
HTTP Post Request
Example 1: Normal SQL Query
Example 1: SQL Injection Query
Example 1: Code Analysis
Example 2: BadProductList.aspx
Example 2: Attack Analysis
Example 3: Updating Table
Example 4: Adding New Records
Example 5: Identifying the Table Name
Example 6: Deleting a Table

Module Flow: Testing for SQL Injection

SQL Injection Detection
SQL Injection Error Messages
SQL Injection Attack Characters
Additional Methods to Detect SQL Injection
SQL Injection Black Box Pen Testing
Testing for SQL Injection

Module Flow: Types of SQL Injection

Types of SQL Injection
Simple SQL Injection Attack
Union SQL Injection Example
SQL Injection Error Based

Module Flow: Blind SQL Injection

What is Blind SQL Injection?
No Error Messages Returned
Blind SQL Injection: WAITFOR DELAY YES or NO Response
Blind SQL Injection - Exploitation (MySQL)
Blind SQL Injection - Extract Database User
Blind SQL Injection - Extract Database Name
Blind SQL Injection - Extract Column Name
Blind SQL Injection - Extract Data from ROWS

Module Flow: SQL Injection Methodology

SQL Injection Methodology

Module Flow: Advanced SQL Injection

Information Gathering
Extracting Information through Error Messages
Understanding SQL Query
Bypass Website Logins Using SQL Injection
Database, Table, and Column Enumeration

Demo - SQL Injection Techniques
Advanced Enumeration
Features of Different DBMSs
Creating Database Accounts
Password Grabbing
Grabbing SQL Server Hashes
Extracting SQL Hashes (In a Single Statement)
Transfer Database to Attacker's Machine
Interacting with the Operating System
Interacting with the FileSystem
Network Reconnaissance Full Query
Module Flow: SQL Injection Tools
SQL Injection Tools: BSQLHacker
SQL Injection Tools: Marathon Tool
SQL Injection Tools: SQL Power Injector
SQL Injection Tools: Havij
SQL Injection Tools
Module Flow: Evasion Techniques
Evading IDS
Types of Signature Evasion Techniques
Evasion Technique: Sophisticated Matches
Evasion Technique: Hex Encoding
Evasion Technique: Manipulating White Spaces
Evasion Technique: In-line Comment
Evasion Technique: Char Encoding
Evasion Technique: String Concatenation
Evasion Technique: Obfuscated Codes
Module Flow: Countermeasures
How to Defend Against SQL Injection Attacks?
How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters
How to Defend Against SQL Injection Attacks? (Cont.)
SQL Injection Detection Tool: Microsoft Source Code Analyzer
SQL Injection Detection Tool: Microsoft UrlScan
SQL Injection Detection Tool: dotDefender
SQL Injection Detection Tool: IBM AppScan
Snort Rule to Detect SQL Injection Attacks
SQL Injection Detection Tools
Quotes
Module 14 Review

Module 15 - Hacking Wireless Networks

1h 56m

Module Flow: Wireless Concepts

Security News
Wireless Networks
Wi-Fi Usage Statistics in the US
Wi-Fi Hotspots at Public Places
Wi-Fi Networks at Home
Types of Wireless Networks
Wireless Standards
Service Set Identifier (SSID)
Wi-Fi Authentication Modes
Wi-Fi Authentication Process Using a Centralized Authentication Server
Wi-Fi Authentication Process
Wireless Terminologies
Wi-Fi Chalking
Wi-Fi Chalking Symbols

Wi-Fi Hotspot Finder: jewire.com

Wi-Fi Hotspot Finder: WeFi.com

Types of Wireless Antenna

Parabolic Grid Antenna

Module Flow: Wireless Encryption

Types of Wireless Encryption

WEP Encryption

How WEP Works?

What is WPA?

How WPA Works?

Temporal Keys

What is WPA2?

How WPA2 Works?

WEP vs. WPA vs. WPA2

WEP Issues

Weak Initialization Vectors (IV)

How to Break WEP Encryption?

How to Break WPA/WPA2 Encryption?

How to Defend Against WPA Cracking?

Module Flow: Wireless Threats

Wireless Threats: Access Control Attacks

Wireless Threats: Integrity Attacks

Wireless Threats: Confidentiality Attacks

Wireless Threats: Availability Attacks

Wireless Threats: Authentication Attacks

Rogue Access Point Attack

Client Mis-association

Misconfigured Access Point Attack

Unauthorized Association

Ad Hoc Connection Attack

HoneySpot Access Point Attack

AP MAC Spoofing

Denial-of-Service Attack

Jamming Signal Attack

Wi-Fi Jamming Devices

Module Flow: Wireless Hacking Methodology

Wireless Hacking Methodology: Wi-Fi Discovery

Find Wi-Fi Networks to Attack

Attackers Scanning for Wi-Fi Networks

Footprint the Wireless Network

Wi-Fi Discovery Tool: inSSIDer

Wi-Fi Discovery Tool: NetSurveyor

Wi-Fi Discovery Tool: NetStumbler

Wi-Fi Discovery Tool: Vistumbler

Wi-Fi Discovery Tool: WirelessMon

Wi-Fi Discovery Tools

Wireless Hacking Methodology: GPS Mapping

GPS Mapping

GPS Mapping Tool: WIGLE

GPS Mapping Tool: Skyhook

How to Discover Wi-Fi Network Using Wardriving?

Wireless Hacking Methodology: Wireless Traffic Analysis

Wireless Traffic Analysis

Wireless Cards and Chipsets

Wi-Fi USB Dongle: AirPcap

Wi-Fi Packet Sniffer: Wireshark with AirPcap

Wi-Fi Packet Sniffer: Wi-Fi Pilot
Wi-Fi Packet Sniffer: OmniPeek
Wi-Fi Packet Sniffer: CommView for Wi-Fi
What is Spectrum Analysis?
Wireless Sniffers
Wireless Hacking Methodology: Launch Wireless Attack
Aircrack-ng Suite
How to Reveal Hidden SSIDs
Demo - Cracking WEP with BackTrack 4
Fragmentation Attack
How to Launch MAC Spoofing Attack?
Denial of Service: Deauthentication and Disassociation Attacks
Man-in-the-Middle Attack
MITM Attack Using Aircrack-ng
Wireless ARP Poisoning Attack
Rogue Access Point
Evil Twin
How to Set Up a Fake Hotspot (Evil Twin)?
Wireless Hacking Methodology: Crack Wi-Fi Encryption
How to Crack WEP Using Aircrack?
How to Crack WEP Using Aircrack? Screenshot 1/2
How to Crack WEP Using Aircrack? Screenshot 2/2
How to Crack WPA-PSK Using Aircrack?
WPA Cracking Tool: KisMAC
WEP Cracking Using Cain & Abel
Demo - Cracking WEP with Cain
WPA Brute Forcing Using Cain & Abel
WPA Cracking Tool: Elcomsoft Wireless Security Auditor
WEP/WPA Cracking Tools
Module Flow: Wireless Hacking Tools
Wi-Fi Sniffer: Kismet
Wardriving Tools
RF Monitoring Tools
Wi-Fi Connection Manager Tools
Wi-Fi Traffic Analyzer Tools
Wi-Fi Raw Packet Capturing Tools/Spectrum Analyzing Tools
Module Flow: Bluetooth Hacking
Bluetooth Hacking
Bluetooth Stack
Bluetooth Threats
How to BlueJack a Victim?
Bluetooth Hacking Tool: Super Bluetooth Hack
Bluetooth Hacking Tool: PhoneSnoop
Bluetooth Hacking Tool: BlueScanner
Bluetooth Hacking Tools
Module Flow: Countermeasures
How to Defend Against Bluetooth Hacking?
How to Detect and Block Rogue AP?
Wireless Security Layers
How to Defend Against Wireless Attacks?
Module Flow: Wireless Security Tools
Wireless Intrusion Prevention Systems
Wireless IPS Deployment
Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
Wi-Fi Security Auditing Tool: AirDefense
Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

Wi-Fi Security Auditing Tool: Aruba RFProtect WIPS
Wi-Fi Intrusion Prevention System
Wi-Fi Predictive Planning Tools
Wi-Fi Vulnerability Scanning Tools
Module Flow: Wi-Fi Penetration Testing
Wireless Penetration Testing
Wireless Penetration Testing Framework
Wi-Fi Pen Testing Framework
Pen Testing LEAP Encrypted WLAN
Pen Testing WPA/WPA2 Encrypted WLAN
Pen Testing WEP Encrypted WLAN
Pen Testing Unencrypted WLAN
Quotes
Module 15 Review

Module 16 - Evading IDS, Firewalls and Honeypots

1h 17m

Module Flow: IDS Firewall and Honeypot Concepts

Security News
Intrusion Detection Systems (IDS) and their Placement
How IDS Works?
Ways to Detect an Intrusion
Types of Intrusion Detection Systems
System Integrity Verifiers (SIV)
General Indications of Intrusions
General Indications of System Intrusions
Firewall
Firewall Architecture
DeMilitarized Zone (DMZ)
Types of Firewall
Packet Filtering Firewall
Circuit-Level Gateway Firewall
Application-Level Firewall
Stateful Multilayer Inspection Firewall
Firewall Identification: Port Scanning
Firewall Identification: Firewalking
Firewall Identification: Banner Grabbing
Honeypot
Types of Honeypots
How to Set Up a Honeypot?

Module Flow: IDS Firewall and Honeypot System

Intrusion Detection Tool: Snort
How Snort Works?
Snort Rules
Snort Rules: Rule Actions and IP Protocols
Snort Rules: The Direction Operator and IP Addresses
Snort Rules: Port Numbers
Demo - Introduction to Snort
Intrusion Detection System: Tipping Point
Intrusion Detection Tools
Firewall: Sunbelt Personal Firewall
Firewalls
Honeypot Tool: KFSensor
Honeypot Tool: SPECTER
Honeypot Tools
Module Flow: Evading IDS
Insertion Attack

Evasion
Denial-of-Service Attack (DoS)
Obfuscating
False Positive Generation
Session Splicing
Unicode Evasion Technique
Fragmentation Attack
Overlapping Fragments
Time-To-Live Attacks
Invalid RST Packets
Urgency Flag
Polymorphic Shellcode
ASCII Shellcode
Application-Layer Attacks
Desynchronization-Pre Connection SYN
Desynchronization-Post Connection SYN
Other Types of Evasion

Module Flow: Evading Firewalls

IP Address Spoofing
Attacking Session Token Generation Mechanism
Tiny Fragments
Bypass Blocked Sites Using IP Address in Place of URL
Bypass Blocked Sites Using Anonymous Website Surfing Sites
Bypass a Firewall using Proxy Server
Bypassing Firewall through ICMP Tunneling Method
Bypassing Firewall through ACK Tunneling Method
Bypassing Firewall through HTTP Tunneling Method
Bypassing Firewall through External Systems
Bypassing Firewall through MITM Attack

Module Flow: Detecting Honeypots

Detecting Honeypots
Honeypot Detecting Tool: Send-Safe Honeypot Hunter

Module Flow: Firewall Evading Tools

Firewall Evasion Tool: Traffic IQ Professional
Firewall Evasion Tool: tcp-over-dns
Firewall Evasion Tools
Packet Fragment Generators

Module Flow: Countermeasures

Countermeasures
Module Flow: Penetration Testing
Firewall/IDS Penetration Testing
Firewall Penetration Testing
IDS Penetration Testing
Quotes
Module 16 Review

Module 17 - Buffer Overflow

30m

Module Flow: Buffer Overflow Concepts

Security News
Buffer Overflows
Why are Programs And Applications Vulnerable?
Understanding Stacks
Stack-Based Buffer Overflow
Understanding Heap
Heap-Based Buffer Overflow
Stack Operations

Shellcode

No Operations (NOPs)

Module Flow: Buffer Overflow Methodology

Knowledge Required to Program Buffer Overflow Exploits

Buffer Overflow Steps

Attacking a Real Program

Format String Problem

Overflow using Format String

Smashing the Stack

Once the Stack is Smashed ...

Module Flow: Buffer Overflow Examples

Simple Uncontrolled Overflow

Simple Buffer Overflow in C

Demo - Simple Buffer Overflow in C

Code Analysis

Exploiting Semantic Comments in C (Annotations)

How to Mutate a Buffer Overflow Exploit

Module Flow: Buffer Overflow Detection

Identifying Buffer Overflows

How to Detect Buffer Overflows in a Program?

BOU (Buffer Overflow Utility)

Testing for Heap Overflow Conditions: heap.exe

Steps for Testing for Stack Overflow in OllyDbg Debugger

Testing for Stack Overflow in OllyDbg Debugger

Testing for Format String Conditions using IDA Pro

BoF Detection Tools

Module Flow: Buffer Overflow Countermeasures

Defense Against Buffer Overflows

Preventing BoF Attacks

Programming Countermeasures

Data Execution Prevention (DEP)

Enhanced Mitigation Experience Toolkit (EMET)

EMET System Configuration Settings

EMET Application Configuration Window

Module Flow: Buffer Overflow Security Tools

/GS

BoF Security Tool: BufferShield

BoF Security Tools

Module Flow: Buffer Overflow Pen Testing

Buffer Overflow Penetration Testing

Quotes

Module 17 Review

Module 18 - Cryptography

39m

Module Flow: Cryptography Concepts

Security News

Cryptography

Types of Cryptography

Government Access to Keys (GAK)

Module Flow: Encryption Algorithms

Ciphers

Advanced Encryption Standard (AES)

Data Encryption Standard (DES)

RC4, RC5, RC6 Algorithms

The DSA and Related Signature Schemes

RSA (Rivest Shamir Adleman)

Example of RSA Algorithm
The RSA Signature Scheme
Message Digest (One-way Hash) Functions
Message Digest Function: MD5
Secure Hashing Algorithm (SHA)
What is SSH (Secure Shell)?
Module Flow: Cryptography Tools
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
Cryptography Tool: Advanced Encryption Package
Cryptography Tools
Module Flow: Public Key Infrastructure
Public Key Infrastructure (PKI)
Certification Authorities
Module Flow: Email Encryption
Digital Signature
SSL (Secure Sockets Layer)
Transport Layer Security (TLS)
Module Flow: Disk Encryption
Disk Encryption
Disk Encryption Tool: TrueCrypt
Disk Encryption Tools
Module Flow: Cryptography Attacks
Cryptography Attacks
Code Breaking Methodologies
Brute-Force Attack
Meet-in-the-Middle Attack on Digital Signature Schemes
Module Flow: Cryptanalysis Tools
Cryptanalysis Tool: CrypTool
Demo - Cryptanalysis Tool: CrypTool
Cryptanalysis Tools
Online MD5 Decryption Tool
Quotes
Module 18 Review

Module 19 - Penetration Testing

1h 6m

Module Flow: Pen Testing Concepts
Security News
Introduction to Penetration Testing
Security Assessments
Vulnerability Assessment
Limitations of Vulnerability Assessment
Penetration Testing
Why Penetration Testing?
What Should be Tested?
What Makes a Good Penetration Test?
ROI on Penetration Testing
Testing Points
Testing Locations
Module Flow: Types of Pen Testing
Types of Penetration Testing
External Penetration Testing
Internal Security Assessment
Black-box Penetration Testing
Grey-box Penetration Testing
White-box Penetration Testing
Announced/Unannounced Testing

Automated Testing
Manual Testing
Module Flow: Pen Testing Techniques
Common Penetration Testing Techniques
Using DNS Domain Name and IP Address Information
Enumerating Information about Hosts on Publicly Available Networks
Module Flow: Pen Testing Phases
Phases of Penetration Testing
Pre-Attack Phase
Attack Phase
Activity: Perimeter Testing
Enumerating Devices
Activity: Acquiring Target
Activity: Escalating Privileges
Activity: Execute, Implant and Retract
Post-Attack Phase and Activities
Penetration Testing Deliverable Templates
Module Flow: Pen Testing Roadmap
Penetration Testing Methodology
Application Security Assessment
Web Application Testing - I
Web Application Testing - II
Web Application Testing - III
Network Security Assessment
Wireless/Remote Access Assessment
Wireless Testing
Telephony Security Assessment
Social Engineering
Testing Network-Filtering Devices
Denial of Service Emulation
Module Flow: Outsourcing Pen Testing Services
Outsourcing Penetration Testing Services
Terms of Engagement
Project Scope
Pentest Service Level Agreements
Penetration Testing Consultants
Module Flow: Pen Testing Tools
Evaluating Different Types of Pentest Tools
Application Security Assessment Tool: WebScarab
Application Security Assessment Tools
Network Security Assessment Tool: Angry IP scanner
Network Security Assessment Tool: GFI LANguard
Network Security Assessment Tools
Wireless/Remote Access Assessment Tool: Kismet
Wireless/Remote Access Assessment Tools
Telephony Security Assessment Tool: Omnippeek
Telephony Security Assessment Tools
Testing Network-Filtering Device Tool: Traffic IQ Professional
Demo - Rapid Penetration Testing with Core Impact
Quotes
Module 19 Review
Course Closure

Total Duration: 23hrs 24m