EC-Council Certified Ethical Hacker v.8

Course Overview

This course provides students with an introduction to ethical hacking. Students will also learn about footprinting and reconnaissance, scanning networks, enumeration, system hacking, trojans and backdoors, viruses and worms, sniffing, social engineering, denial of service, session hijacking, hacking webservers, hacking web applications, SQL injection, hacking wireless networks, hacking mobile platforms, evading IDS, firewalls, and honeypots, buffer overflow, cryptography, and penetration testing.

Course Introduction 3m

Course Introduction

Module 00 - Student Introduction 23m

Student Introduction
Course Materials
CEHv8 Course Outline
EC-Council Certification Program
Certified Ethical Hacker Track
CEHv8 Exam Information
Lab Sessions
What Does CEH Teach You?
What CEH is NOT?
Remember This!
CEH Class Speed
Live Hacking Website
Advanced Lab Environment
Student Computer Checklist
Launching Command Shell
Snapshots of Virtual Machines
AirPcap
Live Hack Website
Lets Start Hacking!

Module 01 - Introduction to Ethical Hacking 2h 4m

Module Flow: Info Security Overview
Security News
Internet Crime Current Report: IC3
Data Breach Investigations Report
Essential Terminology
Elements of Information Security
The Security, Functionality, and Usability Triangle
Module Flow: Information Security Threats and Attack Vectors
Top Information Security Attack Vectors

Motives, Goals, and Objectives of Information Security Attacks
Information Security Threats
Information Warfare
IPv6 Security Threats
Module Flow: Hacking Concepts
Hacking vs. Ethical Hacking
Effects of Hacking on Business
Who Is a Hacker?
Hacker Classes
Hacktivism
Module Flow: Hacking Phases
Hacking Phases
Module Flow: Types of Attacks
Types of Attacks on a System
Operating System Attacks
Misconfiguration Attacks
Application-Level Attacks
Examples of Application-Level Attacks
Shrink Wrap Code Attacks
Module Flow: Information Security Controls
Why Ethical Hacking is Necessary
Scope and Limitations of Ethical Hacking
Skills of an Ethical Hacker
Defense in Depth
Incident Management Process
Information Security Policies
Classification of Security Policies
Structure and Contents of Security Policies
Types of Security Policies
Steps to Create and Implement Security Policies
Examples of Security Policies
Vulnerability Research
Vulnerability Research Websites
Demo - Vulnerability Research Website
What is Penetration Testing?
Why Penetration Testing
Penetration Testing Methodology
Module 01 Review

Module 02 - Footprinting and Reconnaissance 2h 35m

Module Flow: Footprinting Concepts
Security News
Footprinting Terminology
What Is Footprinting?
Why Footprinting?
Objectives of Footprinting
Module Flow: Footprinting Threats
Footprinting Threats
Module Flow: Footprinting Methodology
Footprinting Methodology: Footprinting through Search Engines

Footprinting through Search Engines
Demo - Footprinting through Search Engines
Finding Company's External and Internal URLs
Public and Restricted Websites
Collect Location Information
People Search
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: Website Footprinting
Website Footprinting
Mirroring Entire Website
Website Mirroring Tools
Extract Website Information from http://www.archive.org
Monitoring Web Updates Using Website Watcher
Footprinting Methodology: Email Footprinting
Tracking Email Communications
Collecting Information from Email Header
Email Tracking Tools
Demo - Tracking Emails with ReadNotify
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 Opinions Say About the Company
Footprinting Methodology: Footprinting using Google
Footprint Using Google Hacking Techniques
What a Hacker can do with Google Hacking?
Google Advance Search Operators
Finding Resources using Google Advance Operator
Google Hacking Tool: Google Hacking Database (GHDB)
Google Hacking Tools
Demo - Google Hacking
Footprinting Methodology: WHOIS Footprinting
WHOIS Lookup
WHOIS Lookup Result Analysis
WHOIS Lookup Tool: SmartWhois
WHOIS Lookup Tools
WHOIS Lookup Online Tools
Demo - SmartWhois
Footprinting Methodology: DNS Footprinting
Extracting DNS Information
Demo - DNS Overview
DNS Interrogation Tools
Footprinting Methodology: Network Footprinting
Locate the Network Range
Determine the Operating System

Traceroute
Traceroute Analysis
Traceroute Tools
Footprinting Methodology: Footprinting through Social Engineering
Footprinting through Social Engineering
Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
Footprinting Methodology: Footprinting through Social Networking Sites
Collect Information through Social Engineering on Social Networking Sites
Information Available on Social Networking Sites
Collecting Facebook Information
Collecting Twitter Information
Collecting Linkedin Information
Collecting Youtube Information
Tracking Users on Social Networking Sites
Module Flow: Footprinting Tools
Footprinting Tool: Maltego
Footprinting Tool: Domain Name Analyzer Pro
Footprinting Tool: Web Data Extractor
Additional Footprinting Tools
Module Flow: Footprinting Countermeasures
Footprinting Countermeasures
Module Flow: Footprinting Penetration Testing
Footprinting Pen Testing
Footprinting Pen Testing Report Templates
Demo - HTTrack and Website Watcher
Module 02 Review

Module 03 - Scanning Networks 1h 59m

Scanning Networks
Security News
Overview of Network Scanning
CEH Scanning Methodology: Check for Live Systems
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
Scanning IPv6 Network
Scanning Tool: Nmap
Demo - Nmap
Hping2 / Hping3
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 and 3
ICMP Echo Scanning/List Scan
UDP Scanning
Inverse TCP Flag Scanning
ACK Flag Scanning
Scanning Tool: NetScan Tools Pro
Scanning Tools
Do Not Scan These IP Addresses
Port Scanning Countermeasures
CEH Scanning Methodology: Scanning Beyond IDS
IDS Evasion Techniques
SYN/FIN Scanning Using IP Fragments
CEH Scanning Methodology: Banner Grabbing
Banner Grabbing
Banner Grabbing Tools
Demo - Banner Grabbing Using Telnet
Demo - Footprinting Webservers Using Netcraft
Banner Grabbing Countermeasures: Disabling or Changing Banner
Hiding File Extensions from Web Pages
CEH Scanning Methodology: Scan for Vulnerability
Vulnerability Scanning
Vulnerability Scanning Tool: Nessus
Demo - Vulnerability Scanning with Nessus
Vulnerability Scanning Tool: GFI LanGuard
Vulnerability Scanning Tool: SAINT
Network Vulnerability Scanners
CEH Scanning Methodology: Draw Network Diagrams
Drawing Network Diagrams
Network Discovery Tool: LANsurveyor
Network Discovery Tool: OpManager
Network Discovery Tool: NetworkView
Network Discovery Tool: The Dude
Network Discovery and Mapping Tools
CEH Scanning Methodology: Prepare Proxies
Proxy Servers
Why Attackers Use Proxy Servers?
Use of Proxies for Attack
Proxy Chaining
Proxy Tool: Proxy Workbench
Proxy Tool: Proxifier
Proxy Tool: Proxy Switcher
Proxy Tool: SocksChain
Proxy Tool: TOR (The Onion Routing)
Proxy Tools
Free Proxy Servers
HTTP Tunneling Techniques

Why do I Need HTTP Tunneling
HTTP Tunneling Tool: Super Network Tunnel
HTTP Tunneling Tool: HTTP-Tunnel
SSH Tunneling
SSH Tunneling Tool: Bitvise
Anonymizers
Case: Bloggers Write Text Backwards to Bypass Web Filters in China
Censorship Circumvention Tool: Psiphon
Censorship Circumvention Tool: Your-Freedom
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
CEH Scanning Methodology: Scanning Pen Testing
Scanning Pen Testing
Module 03 Review

Module 04 - Enumeration 57m

Module Flow: Enumeration Concepts
Security News
What Is Enumeration?
Techniques for Enumeration
Services and Ports to Enumerate
Module Flow: NetBIOS Enumeration
NetBIOS Enumeration
NetBIOS Enumeration Tool: SuperScan
Demo - Enumerating Users Using Null Sessions
NetBIOS Enumeration Tool: Hyena
NetBIOS Enumeration Tool: Winfingerprint
NetBIOS Enumeration Tool: NetBIOS Enumerator
Enumerating User Accounts
Enumerate Systems Using Default Passwords
Module Flow: SNMP Enumeration
SNMP (Simple Network Management Protocol) Enumeration
Working of SNMP
Management Information Base (MIB)
SNMP Enumeration Tool: OpUtils
SNMP Enumeration Tool: SolarWind's IP Network Browser
Demo - SNMP Enumeration with Solar Winds
SNMP Enumeration Tools
Module Flow: UNIX/Linux Enumeration
UNIX/Linux Enumeration Commands
Linux Enumeration Tool: Enum4linux
Module Flow: LDAP Enumeration
LDAP Enumeration
LDAP Enumeration Tool: Softerra LDAP Administrator

LDAP Enumeration Tools
Module Flow: NTP Enumeration
NTP Enumeration
NTP Enumeration Commands
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
Module Flow: Enumeration Countermeasures
Enumeration Countermeasures
SMB Enumeration Countermeasures
Module Flow: Enumeration Pen Testing
Enumeration Pen Testing
Module 04 Review

Module 05 - System Hacking 3h 24m
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 Attack: Wire Sniffing
Passive Online Attacks: Man-in-the-Middle and Replay Attack
Active Online Attack: Password Guessing
Active Online Attack: Trojan/Spyware/Keylogger
Active Online Attack: Hash Injection Attack
Offline Attack: Rainbow Attacks
Tools to Create Rainbow Tables: Winrtgen and rtgen
Demo - Making Rainbow Tables
Demo - Using Rainbow Tables
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
Stealing Passwords Using Keyloggers
Microsoft Authentication
How Hash Passwords Are Stored in Windows SAM?

Screen Capturing Spyware
Screen Capturing Spyware: SoftActivity TS Monitor
Screen Capturing Spyware (Cont.)
USB Spyware
USB Spyware: USBSpy
USB Spyware (Cont.)
Audio Spyware
Audio Spyware: Spy Voice Recorder and Sound Snooper
Video Spyware
Video Spyware: WebCam Recorder
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: SPYPhone
GPS Spyware (Cont.)
How to Defend Against Keyloggers
Anti-Keylogger
Anti-Keylogger: Zemana AntiLogger
Anti-Keylogger (Cont.)
How to Defend Against Spyware
Anti-Spyware: PC Tools Spyware Doctor
Anti-Spywares
CEH System Hacking Steps: Hiding Files
Rootkits
Types of Rootkits
How Rootkit Works
Rootkit: Fu
Demo - Fu Rootkit
Rootkit: KBeast
Rootkit: Hacker Defender HxDef Rootkit
Detecting Rootkits
Steps for Detecting Rootkits
How to Defend against Rootkits
Anti-Rootkit: Stinger
Anti-Rootkit: UnHackMe
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: StreamArmor
NTFS Stream Detectors
What Is Steganography?
Application of Steganography

Module 06 - Trojans and Backdoors	1h 53m

Module Flow: Trojan Concepts
Security News
What Is a Trojan?
Communication Paths: 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 and NetBot Attacker
Proxy Server Trojans
Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
FTP Trojans
VNC Trojans
VNC Trojans: WinVNC and VNC Stealer
HTTP/HTTPS Trojans
HTTP Trojan: HTTP RAT
Shttpd Trojan - HTTPS (SSL)
ICMP Tunneling
Remote Access Trojans
Demo - Beast
Remote Access Trojan: RAT DarkComet and Apocalypse
Covert Channel Trojan: CCTT
E-banking Trojans
Banking Trojan Analysis
E-banking Trojan: ZeuS and SpyEye
Destructive Trojans: M4sT3r Trojan
Notification Trojans
Credit Card Trojans
Data Hiding Trojans (Encrypted Trojans)

OS X Trojan: Crisis
MAC OS X Trojan: DNSChanger
Mac OS X Trojan: Hell Raiser
Trojan Analysis: Flame
Flame C&C Server Analysis
Trojan Analysis: SpyEye
Trojan Analysis: ZeroAccess
Trojan Analysis: Duqu
Trojan Analysis: Duqu Framework
Trojan Analysis: Event Driven Framework
Module Flow: Trojan Detection
How to Detect Trojans
Scanning for Suspicious Ports
Port Monitoring Tools: TCPView and CurrPorts
Scanning for Suspicious Processes
Process Monitoring Tool: What's Running
Process Monitoring Tools
Scanning for Suspicious Registry Entries
Registry Entry Monitoring Tool: PC Tools Registry Mechanic
Registry Entry Monitoring Tools
Scanning for Suspicious Device Drivers
Device Drivers Monitoring Tool: DriverView
Device Drivers Monitoring Tools
Scanning for Suspicious Windows Services
Windows Services Monitoring Tool: Windows Service Manager (SrvMan)
Windows Services Monitoring Tools
Scanning for Suspicious Startup Programs
Windows8 Startup Registry Entries
Startup Programs Monitoring Tool: Starter
Startup Programs Monitoring Tool: 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
Module 06 Review

Module 07 - Viruses and Worms 46m

Module Flow: Virus and Worms Concepts

Security News

Introduction to Viruses

Virus and Worm Statistics

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

Common Techniques Used to Distribute Malware on the Web

Virus Hoaxes and Fake Antiviruses

Virus Analysis: DNSChanger

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 and DELmE's Batch Virus Maker

Demo - JPS Virus Maker Tool

Module Flow: Computer Worms

Computer Worms

How Is a Worm Different from a Virus?

Worm Analysis: Stuxnet

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

Virus Analysis Tool: IDA Pro

Online Malware Testing: VirusTotal

Online Malware Analysis Services

Module Flow: Countermeasures

Virus Detection Methods

Virus and Worms Countermeasures
Companion Antivirus: Immunet
Anti-virus Tools
Module Flow: Penetration Testing
Penetration Testing for Virus
Module 07 Review

Module 08 - Sniffing 2h 24m
Module Flow: Sniffing Concepts
Security News
Wiretapping
Lawful Interception
Packet Sniffing
Sniffing Threats
How a Sniffer Works
Types of Sniffing Attacks
Types of Sniffing: Passive Sniffing
Types of Sniffing: Active Sniffing
Protocols Vulnerable to Sniffing
Tie to Data Link Layer in OSI Model
IPv6 Addresses
IPv4 and IPv6 Header Comparison
Hardware Protocol Analyzers
SPAN Port
Module Flow: MAC Attacks
MAC Address/CAM Table
How CAM Works
What Happens When CAM Table Is Full?
MAC Flooding
Demo - Port Security
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
DHCP Starvation Attack Tools
Rogue DHCP Server Attack
Demo - Rogue DHCP Server
How to Defend Against DHCP Starvation and Rogue Server Attack
Module Flow: ARP Poisoning
What Is Address Resolution Protocol (ARP)?
ARP Spoofing Techniques
ARP Spoofing Attack
How Does ARP Spoofing Work
Threats of ARP Poisoning
ARP Poisoning Tool: Cain & Abel
Demo - Active Sniffing with Cain

Demo - Actively Sniffing a Switched Network with Cain
Demo - MITM
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
ARP Spoofing Detection: XArp
Module Flow: Spoofing Attack
MAC Spoofing/Duplicating
MAC Spoofing Technique: Windows
MAC Spoofing Tool: SMAC
Demo - Spoofing the MAC Address
IRDP Spoofing
How to Defend Against MAC Spoofing
Module Flow: DNS Poisoning
DNS Poisoning Techniques
Intranet DNS Spoofing
Internet 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: Cascade Pilot
Sniffing Tool: Tcpdump/Windump
Packet Sniffing Tool: Capsa Network Analyzer
Network Packet Analyzer: OmniPeek Network Analyzer
Network Packet Analyzer: Observer
Network Packet Analyzer: Sniff-O-Matic
Network Packet Analyzer: JitBit Network Sniffer
Chat Message Sniffer: MSN Sniffer 2
TCP/IP Packet Crafter: Colasoft Packet Builder
Additional Sniffing Tools
How an Attacker Hacks the Network Using Sniffers
Module Flow: Countermeasures
How to Defend Against Sniffing
How to Detect Sniffing
Sniffer Detection Technique: Ping Method
Sniffer Detection Technique: ARP Method
Sniffer Detection Technique: DNS Method
Promiscuous Detection Tool: PromqryUI
Module Flow: Sniffing Pen Testing
Sniffing Pen Testing
Module 08 Review

Module 09 - Social Engineering 56m

Module Flow: Social Engineering Concepts
Security News
There is No Patch to Human Stupidity
What Is Social Engineering?
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
"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: Eavesdropping and Shoulder Surfing
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
Computer-based Social Engineering: Spear Phishing
Mobile-based Social Engineering: Publishing Malicious Apps
Mobile-based Social Engineering: Repackaging Legitimate Apps
Mobile-based Social Engineering: Fake Security Applications
Mobile-based Social Engineering: Using SMS
Insider Attack
Disgruntled Employee
Preventing Insider Threats
Common Social Engineering Targets and Defense Strategies
Module Flow: Impersonation on Social Networking Sites
Social Engineering Through Impersonation on Social Networking Sites
Social Engineering on Facebook
Social Engineering Example: LinkedIn Profile
Social Engineering on Twitter
Risks of Social Networking to Corporate Networks
Module Flow: Identity Theft
Identity Theft Statistics 2011
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
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
Social Engineering Pen Testing: Social Engineering Toolkit (SET)
Module 09 Review

Module 10 - Denial of Service 33m

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
Module Flow: DoS/DDoS Attack Techniques
DoS Attack Techniques
Bandwidth Attacks
Service Request Floods
SYN Attack
SYN Flooding
Demo - SYN Flooding with Hping2
ICMP Flood Attack
Peer-to-Peer Attacks
Permanent Denial-of-Service Attack
Application Level Flood Attacks
Module Flow: Botnets
Organized Crime Syndicates
Organized Cyber Crime: Organizational Chart
Botnet
Botnet Propagation Technique
Botnet Ecosystem
Botnet Trojan: Shark
Poison Ivy: Botnet Command Control Center
Botnet Trojan: PlugBot
Botnet Trojan: Illusion Bot and NetBot Attacker
Module Flow: DDoS Case Study
DDoS Attack
DDoS Attack Tool: LOIC
Hackers Advertise Links to Download Botnet
Module Flow: DoS/DDoS Attack Tools

DoS Attack Tools
Module Flow: Countermeasures
Detection Techniques
Activity Profiling
Wavelet-based Signal Analysis
Sequential Change-Point Detection
DoS/DDoS Countermeasure Strategies
DDoS Attack Countermeasures
DoS/DDoS Countermeasures: Protect 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 Appliances
Module Flow: DoS/DDoS Protection Tools
DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall
DoS/DDoS Protection Tools
Module Flow: DoS/DDoS Penetration Testing
Denial-of-Service (DoS) Attack Penetration Testing
Module 10 Review

Module 11 - Session Hijacking 45m

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 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 Numbers 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: Zaproxy
Session Hijacking Tool: Burp Suite
Demo - Session Hijacking with Burp
Session Hijacking Tool: JHijack
Session Hijacking Tools
Module Flow: 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
IPSec
Modes of IPsec
IPsec Architecture
IPsec Authentication and Confidentiality
Components of IPsec
IPsec Implementation
Module Flow: Penetration Testing
Session Hijacking Pen Testing
Module 11 Review

Module 12 - Hacking Webservers 1h 10m

Module Flow: Webserver Concepts
Security News
Webserver Market Shares
Open Source Webserver Architecture
IIS Web Server Architecture
Website Defacement
Why Web Servers Are Compromised
Impact of Webserver Attacks
Module Flow: Webserver Attacks
Web Server Misconfiguration
Web Server 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
Web Password Cracking Tool: Internet Password Recovery Toolbox
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: Syhunt Dynamic
Web Application Security Scanner: N-Stalker Web Application Security Scanner
Web Server Security Scanner: Wikto
Web Server Security Scanner: Acunetix Web Vulnerability Scanner
Web Server Malware Infection Monitoring Tool: HackAlert
Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection
Webserver Security Tools
Module Flow: Webserver Pen Testing

Web Server Pen Testing Tool: CORE Impact Pro
Web Server Pen Testing Tool: Immunity CANVAS
Web Server Pen Testing
Web Server Penetration Testing
Module 12 Review

Module 13 - Hacking Web Applications 1h 52m

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 an 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 Spidering Using Mozenda Web Agent Builder
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
User Name 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 Tool: CookieDigger

Web Application Hacking Tool: 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: Watcher Web Security Tool

Web Application Security Scanner: Netsparker

Web Application Security Tool: N-Stalker Web Application Security Scanner

Web Application Security Tool: VampireScan

Web Application Security Tools

Web Application Firewall: dotDefender

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

Module 13 Review

Module 14 - SQL Injection 1h 7m

Module Flow: SQL Injection Concepts
Security News
SQL Injection
Scenario
SQL Injection Is the Most Prevalent Vulnerability in 2012
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 File System
Network Reconnaissance Using SQL Injection
Network Reconnaissance Full Query
Module Flow: SQL Injection Tools
SQL Injection Tool: BSQLHacker
SQL Injection Tool: Marathon Tool
SQL Injection Tool: SQL Power Injector
SQL Injection Tool: 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 Filter
SQL Injection Detection Tool: dotDefender
SQL Injection Detection Tool: IBM Security AppScan
SQL Injection Detection Tool: WebCruiser
Snort Rule to Detect SQL Injection Attacks
SQL Injection Detection Tools
Module 14 Review

<u>Module 15 - Hacking Wireless Networks</u> 2h 8m

Module Flow: Wireless Concepts
Security News
Wireless Networks
2010 vs. 2011 Wi-Fi Data Usage Comparison
Wi-Fi Networks at Home and Public Places
Types of Wireless Networks
Wireless Standards
Service Set Identifier (SSID)

Wi-Fi Authentication Modes
Wi-Fi Authentication Process Using a Centralized Authentication Server
Wireless Terminologies
Wi-Fi Chalking
Wi-Fi Chalking Symbols
Types of Wireless Antennas
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 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
Footprint the Wireless Network
Attackers Scanning for Wi-Fi Networks
Find Wi-Fi Networks to Attack
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
Mobile-based Wi-Fi Discovery Tool
Wi-Fi Discovery Tools
Wireless Hacking Methodology: GPS Mapping

GPS Mapping
GPS Mapping Tool: WIGLE
GPS Mapping Tool: Skyhook
Wi-Fi Hotspot Finder: jiWire
Wi-Fi Hotspot Finder: WeFi
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: Cascade Pilot
Wi-Fi Packet Sniffer: OmniPeek
Wi-Fi Packet Sniffer: CommView for Wi-Fi
What Is Spectrum Analysis?
Wi-Fi Packet Sniffers
Wireless Hacking Methodology: Launch Wireless Attacks
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 Traffic Analyzer Tools
Wi-Fi Raw Packet Capturing and 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
Module 15 Review

Module 16 - Hacking Mobile Platforms 1h 13m

Module Flow: Mobile Platform Attack Vectors
Security News
Mobile Threat Report Q2 2012
Terminology
Mobile Attack Vectors
Mobile Platform Vulnerabilities and Risks
Security Issues Arising from App Stores
Threats of Mobile Malware
App Sandboxing Issues
Module Flow: Hacking Android OS
Android OS
Android OS Architecture
Android Device Administration API
Android Rooting
Rooting Android Phones using SuperOneClick
Rooting Android Phones Using Superboot
Android Rooting Tools
Session Hijacking Using DroidSheep
Android-based Sniffer: FaceNiff

Android Trojan: ZitMo (ZeuS-in-the-Mobile)
Android Trojan: GingerBreak
Android Trojan: AcnetSteal and Cawitt
Android Trojan: Frogonal and Gamex
Android Trojan: KabStamper and Mania
Android Trojan: PremiumSMS and SmsSpy
Android Trojan: DroidLive SMS and UpdtKiller
Android Trojan: FakeToken
Securing Android Devices
Google Apps Device Policy
Remote Wipe Service: Remote Wipe
Android Security Tool: DroidSheep Guard
Android Vulnerability Scanner: X-Ray
Android Penetration Testing Tool: Android Network Toolkit - Anti
Android Device Tracking Tools
Module Flow: Hacking iOS
Security News
Apple iOS
Jailbreaking iOS
Types of Jailbreaking
Jailbreaking Techniques
App Platform for Jailbroken Devices: Cydia
Jailbreaking Tools: Redsn0w and Absinthe
Tethered Jailbreaking of iOS 6 Using RedSn0w
Jailbreaking Tools: Sn0wbreeze and PwnageTool
Jailbreaking Tools: LimeRaln and Jailbreakme
Jailbreaking Tools: Blackraln and Spirit
Guidelines for Securing iOS Devices
iOS Device Tracking Tools
Module Flow: Hacking Windows Phone OS
Windows Phone 8
Windows Phone 8 Architecture
Secure Boot Process
Guidelines for Securing Windows OS Devices
Module Flow: Hacking BlackBerry
BlackBerry Operating System
BlackBerry Enterprise Solution Architecture
Blackberry Attack Vectors
Malicious Code Signing
JAD File Exploits and Memory/Processes Manipulations
Short Message Service (SMS) Exploits
Email Exploits
PIM Data Attacks and TCP/IP Connections Vulnerabilities
BlackBerry Spyware: FinSpy Mobile
Guidelines for Securing BlackBerry Devices
Module Flow: Mobile Device Management
Mobile Device Management (MDM)
MDM Logical Architecture
MDM Solution: MaaS360 Mobile Device Management (MDM)
MDM Solutions

Module Flow: Mobile Security Guidelines and Tools
General Guidelines for Mobile Platform Security
Mobile Device Security Guidelines for Administrator
Mobile Protection Tool: BullGuard Mobile Security
Mobile Protection Tool: Lookout
Mobile Protection Tool: WISeID
Mobile Protection Tools
Module Flow: Mobile Pen Testing
Android Phone Pen Testing
iPhone Pen Testing
Windows Phone Pen Testing
BlackBerry Pen Testing
Module 16 Review

Module 17 - Evading IDS, Firewalls, and Honeypots 1h 42m

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
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: ZoneAlarm PRO 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
Source Routing
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
Module 17 Review

Module 18 - Buffer Overflow 36m

Module Flow: Buffer Overflow Concepts
Security News
Buffer Overflows
Why Are Programs and Applications Vulnerable to Buffer Overflows?
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
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
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 Tool: Immunity CANVAS
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 Settings
Module Flow: Buffer Overflow Security Tools
/GS
BoF Security Tool: BufferShield
BoF Security Tools
Module Flow: Buffer Overflow Pen Testing
Buffer Overflow Penetration Testing

Module 18 Review

Module 19 - Cryptography 55m

Module Flow: Cryptography Concepts
Security News
Cryptography
Types of Cryptography
Government Access to Keys (GAK)
Module Flow: Encryption Algorithms
Ciphers
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
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 Tool: BCTextEncoder
Cryptography Tools
Module Flow: Public Key Infrastructure (PKI)
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 Tool: GiliSoft Full Disk Encryption
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 Tools
Module 19 Review

Module 20 - Penetration Testing 1h 20m

Module Flow: Pen Testing Concepts
Security News
Security Assessments
Security Audit
Vulnerability Assessment
Limitations of Vulnerability Assessment
Introduction to Penetration Testing
Penetration Testing
Why Penetration Testing
Comparing Security Audit, Vulnerability Assessment, and 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: Define Rules of Engagement (ROE)
Pre-Attack Phase: Understand Customer Requirements
Pre-Attack Phase: Create a Checklist of the Testing Requirements
Pre-Attack Phase: Define the Pen-Testing Scope
Pre-Attack Phase: Sign Penetration Testing Contract
Pre-Attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements
Pre-Attack Phase: Information Gathering
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 Simulation
Module Flow: Outsourcing Pen Testing Services
Outsourcing Penetration Testing Services
Demo - Rapid Penetration Testing with Core Impact
Terms of Engagement
Project Scope
Pen Test Service Level Agreements
Penetration Testing Consultants
Module 20 Review
Course Closure

Total Duration: 30h 38m