

# **EC-Council Certified Ethical Hacker Version 6**

- **Course Number:** CEHv6
- **Course Length:** 5 Days

## **Course Overview**

This instructor-led course will immerse students in an interactive environment where they will learn how to scan, test, hack, and secure their own systems. The use of live demonstrations gives each student in-depth knowledge and practical experience with current and essential security systems. Students begin by understanding how perimeter defenses work and then are lead into scanning and attacking their own networks (this is, of course, for testing purposes only; no real network is harmed). The instructor then dives into how intruders escalate privileges and what steps should be taken to secure a system. All of this is followed with topics such as Intrusion Detection, DDoS Attacks, Buffer Overflows, Social Engineering, Policy Creation, Virus Creation, and much, much more. When the student completes this intensive class they will have the hands-on understanding and experience of a Certified Ethical Hacker.

## **Prerequisites**

Students must have at least 2 years experience in being a Network Administrator before attempting this course.

## **Audience**

This course is of significant benefit to Security Officers and Professionals, Site Administrators, Auditors, and anyone who is concerned about the integrity of their network infrastructure.

## **Certification Exam**

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

# Course Outline

## **Course Introduction**

4m

Course Introduction

## **Module 00 - Student Introduction**

9m

Student Introduction

Self Study Modules

EC-Council Certification Program

Certified Ethical Hacker Track

CEHv6 Exam Information

Lab Sessions

What does CEH teach you?

Remember This!

CEH Class Speed

Live Hacking Website

Student Introduction Review

## **Module 01 - Penetration Testing 101**

1h 59m

Penetration Testing 101

To Know more about Penetration Testing, Attend EC-Council's LPT Program

Introduction to PT

Hands-on: Module Overview - History of Hackers

Categories of Security Assessments

Vulnerability Assessment

Limitations of Vulnerability Assessment

Penetration Testing

Types of Penetration Testing

Risk Management

Hands-on: CIO View Self Assessment

Do-it-Yourself Testing

Hands-on: Security focus website

Outsourcing Penetration Testing Services

Terms of Engagement

Hands-on: NIST Methodology

Project Scope

Pentest Service Level Agreements

Testing Points

Hands-on: Zero-Day and Research

Testing Locations

Automated Testing

Manual Testing

Using DNS Domain Name and IP Address Information

Enumerating Information about Hosts on Publicly-Available Networks

Testing Network-Filtering Devices

Enumerating Devices

Denial of Service Emulation

Penetration Testing Tools

Evaluating Different Types of Pentest Tools  
Asset Audit  
Fault Trees and Attack Trees  
GAP Analysis  
Threats  
Threat  
Business Impact of Threat  
Internal Metrics Threat  
External Metrics Threat  
Calculating Relative Criticality  
Test Dependencies  
Other Tools Useful in Pen-Test  
Phases of Penetration Testing  
Pre-Attack Phase  
Best Practices  
Results that can be Expected  
Passive Reconnaissance  
Active Reconnaissance  
Attack Phase  
Activity: Perimeter Testing  
Activity: Web Application Testing - I  
Activity: Web Application Testing - II  
Activity: Web Application Testing - III  
Activity: Wireless Testing  
Activity: Acquiring Target  
Activity: Escalating Privileges  
Activity: Execute, Implant, and Retract  
Post-Attack Phase and Activities  
Penetration Testing Deliverables Templates  
Hands-on: BT4 VM Install 101  
Hands-on: Virtual Box  
Penetration Testing Review

## **Module 02 - Introduction to Ethical Hacking**

2h 34m

Introduction to Ethical Hacking  
Hands-on: VMware Basics Overview 01  
Hands-on: VMware Basics Overview 02  
Hands-on: Opening An Existing XP VMware System  
Hands-on: Opening VM Appliance  
Hands-on: Installing A New VM System  
Hands-on: Boot XP VM From Backtrack ISO  
Module Objective  
Module Flow  
Problem Definition - Why Security?  
Essential Terminologies  
Hands-on: Quantitative Threat Analysis  
Elements of Security  
Hands-on: Technology Evolution

The Security, Functionality, and Ease of Use Triangle  
Case Study

What Does a Malicious Hacker Do

Effect on Business

Phase 1 - Reconnaissance

Reconnaissance Types

Phase 2 - Scanning

Hands-on: Port Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Covering Tracks

Types of Hacker Attacks

1. Operating System Attacks

Hands-on: OS Attack

Security News: Default Installation

2. Application Level Attacks

Hands-on: Application Attacks

3. Shrink Wrap Code Attacks

4. Misconfiguration Attacks

Remember This Rule!

Hactivism

Hacker Classes

Ethical Hacker Classes

What Do Ethical Hackers Do

Hands-on: Ethical Hacking Research

Can Hacking be Ethical

How to Become an Ethical Hacker

Skill Profile of an Ethical Hacker

What is Vulnerability Research

Why Hackers Need Vulnerability Research

Hands-on: Vulnerability Research Resources

Vulnerability Research Tools

Hands-on: Milw0rm Progenic Websites

How to Conduct Ethical Hacking

Hands-on: Pen-Test Templates and Methodologies

How Do They Go About It

Approaches to Ethical Hacking

Ethical Hacking Testing

Ethical Hacking Deliverables

Hands-on: Computer Crimes and Implications

Computer Crimes and Implications

What Happened Next

Hands-on: Module Summary Tips

Introduction to Ethical Hacking Review

## **Module 03 – Footprinting**

Footprinting

Module Objective

Module Flow

1h 47m

Revisiting Reconnaissance  
Defining Footprinting  
Why is Footprinting Necessary  
Areas and Information which Attackers Seek  
Information Gathering  
Information Gathering Methodology  
Unearthing Initial Information  
Hands-on: Sam Spade  
Finding a Company's URL  
Internal URL  
Extracting Archive of a Website  
Hands-on: Wayback Machine  
Google Search for Company's Info.  
People Search  
Satellite Picture of a Residence  
Footprinting Through Job Sites  
Passive Information Gathering  
Competitive Intelligence Gathering  
Why Do You Need Competitive Intelligence  
Competitive Intelligence Resource  
Hands-on: Competitive Intelligence Services  
Competitive Intelligence Tool: Web Investigator  
Reputica Dashboard  
MyReputation  
Public and Private Websites  
Footprinting Tools  
Whois Tools  
Hands-on: Wikto  
Hands-on: Whois Online And Backtrack  
Hands-on: CountryIP  
Hands-on: FireCat, Firefox Assessment Add Ons  
DNS Information Extraction Tools  
Tool: DNS Enumerator  
Hands-on: Nslookup  
Locating Network Range  
Hands-on: Networkblock And Traceroute  
Arin  
Traceroute  
Trace Route Analysis  
Hands-on: ICMP Traceroute Serversniff  
Hands-on: Visual IPtrace  
Tool: Maltego  
Hands-on: Kartoo / Maltego  
Hands-on: Maltego Info Gathering  
Layer Four Traceroute  
E-mail Spiders  
Hands-on: Email Spider  
Tool: 1st E-mail Address Spider

Hands-on: Core Impact Email Info Gathering  
Locating Network Activity  
Tool: GEOSpider  
Tool: Geowhere  
Hands-on: Google Earth, News Groups, Facebook  
Search Engines  
Kartoo Search Engine  
Dogpile (Meta Search Engine)  
robots.txt  
How to Fake Websites  
Faking Websites using Man-in-the-Middle Phishing Kit  
Steps to Perform Footprinting  
What Happened Next  
Hands-on: New Tool Bonus: Netifera  
Hands-on: New Tool Bonus: SEAT Search-Engine-Assessment-Tool  
Hands-on: Module Summary Tips  
Footprinting Review

## **Module 04 - Google Hacking**

1h 5m

Google Hacking  
Module Flow  
What is Google Hacking  
What a Hacker Can do With Vulnerable Site  
Anonymity with Caches  
Hands-on: Google Hacking Overview  
Using Google as a Proxy Server  
Hands-on: Google As A Proxy Server  
Directory Listings  
Locating Directory Listings  
Hands-on: Google Directory Listings  
Hands-on: Google: Finding Specific Files  
Hands-on: Splunk  
Server Versioning  
Going Out on a Limb: Traversal Techniques  
Directory Traversal  
Incremental Substitution  
Extension Walking  
Google Advanced Operators  
Pre-Assessment  
intranet | help.desk  
Locating Exploits and Finding Targets  
Locating Public Exploit Sites  
Locating Vulnerable Targets  
"Powered by" Tags Are Common Query Fodder for Finding Web Applications  
Vulnerable Web Application Examples  
Locating Targets via CGI Scanning  
Web Server Software Error Messages  
Hands-on: Default Page Search: Tswab

Google Hacking Tools  
Hands-on: Metagoofil Search  
Hands-on: New Tool: SEAT  
Google Hacking Database (GHDB)  
SiteDigger Tool  
Gooscan  
Goolink Scanner  
Hands-on: Google Hack HoneyPot  
Hands-on: Goolag Wikto Automated  
Google Hack Honeypot  
Hands-on: Summary Google, Locating Live Cams  
Google Hacking Review

## **Module 05 – Scanning**

3h 56m

Scanning  
Module Objective  
Scanning - Definition  
Types of Scanning  
Objectives of Scanning  
CEH Scanning Methodology  
Checking for Live Systems  
Checking for Live Systems - ICMP Scanning  
Hands-on: NMAP is the Host IP  
Hands-on: NMAP Zenmap GUI Console  
Hands-on: Angry IP Scanner  
Firewalk Tool  
Hands-on: Tips and Installing ScanRand in Backtrack  
Checking for Open Ports  
Hands-on: Tip Video: TCPIP for Sec Pros  
Three Way Handshake  
Hands-on: techtionary.com Port Numbers  
Hands-on: techtionary.com TCP Handshake and Ack  
TCP Communication Flags  
Nmap  
Nmap: Scan Methods  
Hands-on: Basic Scan Techniques Using NMAP  
Hands-on: Launching a Scan from CentralOps Webserver  
Hands-on: NMAP Verbose  
NMAP Output Format  
Hands-on: LEO Tracking Your Results  
Hands-on: Tips and Saving Your Results with LEO  
Hands-on: NMAP Output for Reports  
Hands-on: Port Scan and Exploitation Using Core Impact  
HPING2  
Hands-on: HPING Basics  
ICMP Echo Scanning/List Scan

TCP Connect / Full Open Scan  
SYN/FIN Scanning Using IP Fragments  
UDP Scanning  
IPSecScan  
Hands-on: IPSec Scanner  
FloppyScan  
ike-scan  
Hands-on: ike-scan  
LANView  
Hands-on: Port Scanning with Look at LAN  
Hands-on: Unicorn Scanning to MySQL  
Colasoft MAC Scanner  
War Dialer Technique  
Why War Dialing?  
War Dialing Countermeasures SandTrap Tool  
Banner Grabbing  
OS Fingerprinting  
Active Stack Fingerprinting  
Hands-on: OS Fingerprinting Tool Examples  
Hands-on: NMAP OS Fingerprinting  
Hands-on: Scanning with AutoScan  
Passive Fingerprinting  
Active Banner Grabbing Using Telnet  
Hands-on: Banner Grabbing with Telnet  
Hands-on: HTTPrint Fingerprinting Webservers  
Tools for Active Stack Fingerprinting  
Disabling or Changing Banner  
IIS Lockdown Tool  
Hands-on: Nessus Client  
Vulnerability Scanning  
Hands-on: Vulnerability Research  
Hands-on: Nessus3 For Windows  
Qualys Web-based Scanner  
SAINT  
Nessus  
Hands-on: Installing Nessus in BackTrack  
Draw Network Diagrams of Vulnerable Hosts  
FriendlyPinger  
Hands-on: Spiceworks Network Mapping and Inventory  
Hands-on: Tip: Research Advice  
LANsurveyor  
Preparing Proxies  
Proxy Servers  
Use of Proxies for Attack  
SocksChain  
How Does MultiProxy Work  
TOR Proxy Chaining Software  
Hands-on: Janus TOR Proxy

Anonymizers  
Surfing Anonymously  
Psiphon  
Bloggers Write Text Backwards to Bypass Web Filters in China  
Hands-on: Jap Anonymous Web Surfing  
Hands-on: SecureStar SSH Tunnel Software  
Google Cookies  
Hands-on: HTTP Tunnels and Port Forwarding  
Hands-on: SSH SSL Tunnels and Port Forwarding  
Hands-on: SecureStar SSH  
Spoofing IP Address  
Detecting IP Spoofing  
Despoof Tool  
Scanning Countermeasures  
What Happened Next?  
Scanning Review

## **Module 06 – Enumeration**

1h 6m

Enumeration  
Module Flow  
Hands-on: Reconnaissance Refresher  
Overview of System Hacking Cycle  
What is Enumeration  
Techniques for Enumeration  
Netbios Null Sessions  
So What's the Big Deal  
Tool: DumpSec  
Hands-on: Null Session Tools  
NetBIOS Enumeration Using Netview  
Hands-on: SMB NAT Dictionary Attack  
Hands-on: Enumeration Banners  
Null Session Countermeasures  
Hands-on: Countermeasures  
PS Tools  
SNMP Enumeration  
Management Information Base  
SNMPutil Example  
Hands-on: SNMP Enumeration with BT  
Tool: Solarwinds  
UNIX Enumeration  
SNMP UNIX Enumeration  
SNMP Enumeration Countermeasures  
LDAP Enumeration  
Jxplorer  
NTP Enumeration  
SMTP Enumeration  
Hands-on: Injecting The Abel Service  
Web Enumeration

Asnumber  
Lynx  
Windows Active Directory Attack Tool  
How To Enumerate Web Application Directories in IIS Using Directory Services  
Enumerate Systems Using Default Passwords  
Terminal Service Agent  
Tool: TXDNS  
Hands-on: NSLookup DNS Zone Transfer  
What Happened Next  
Enumeration Review

## **Module 07 - System Hacking**

2h 43m

System Hacking  
Module Flow  
Hands-on: AFX Rootkit  
CEH Hacking Cycle 01  
Password Types  
Types of Password Attacks  
Hands-on: Monitoring User Login  
Passive Online Attack: Wire Sniffing  
Passive Online Attack: Man-in-the-Middle and Replay Attacks  
Hands-on: SSL MITM  
Active Online Attack: Password Guessing  
Offline Attacks  
Hands-on: Cain and Abel Dictionary Attack  
Offline Attack: Brute-force Attack  
Offline Attack: Pre-Computed Hashes  
Hands-on: Local Password Reset  
Hands-on: Backtrack: Local XP Password Attack  
Syllable Attack/Rule-based Attack/Hybrid Attack  
Distributed Network Attack  
Hands-on: Rainbow Table Cracking  
Non-Technical Attacks  
PDF Password Cracker  
Hands-on: Removing A PDF Password  
Password Mitigation  
Permanent Account Lockout - Employee Privilege Abuse  
Administrator Password Guessing  
Manual Password Cracking Algorithm  
Automatic Password Cracking Algorithm  
Microsoft Authentication  
LM, NTLMv1, and NTLMv2  
NTLM and LM Authentication on the Wire  
Kerberos Authentication  
What is LAN Manager Hash  
Salting  
Hands-on: TS Grinder  
Hands-on: Cracking Your Local XP 64bit Password with Ophcrack

Password Cracking Countermeasures  
Do Not Store LAN Manager Hash in SAM Database  
LM Hash Backward Compatibility  
Escalating Privileges  
Privilege Escalation  
Hands-on: Privilege Escalation  
Executing Applications  
Actual Spy  
Hands-on: Hardware Keystroke Loggers  
Wiretap Professional  
Keylogger Countermeasures  
Anti-Keylogger  
Hiding Files 01  
CEH Hacking Cycle 02  
Hiding Files 02  
Rootkits  
Why Rootkits  
Rootkits in Linux  
Detecting Rootkits  
Steps for Detecting Rootkits  
Sony Rootkit Case Study  
Hands-on: Dreampak PL Rootkit  
Rootkit Countermeasures  
Creating Alternate Data Streams  
Hands-on: Alternate Data Streams  
NTFS Streams Countermeasures  
Hacking Tool: USB Dumper  
Steganography  
Hands-on: Steganography  
Least Significant Bit Insertion in Image Files  
Steganography Tools  
Steganography Detection  
Steganalysis  
Steganalysis Methods/Attacks on Steganography  
Steganalysis Tools  
Stegdetect  
Covering Tracks  
Hands-on: Darins Boot and Nuke  
Disabling Auditing  
Clearing the Event Log  
What Happened Next  
System Hacking Review

## **Module 08 - Trojans and Backdoors**

52m

Trojans and Backdoors  
Introduction  
What is a Trojan  
Overt and Covert Channels  
Working of Trojans

Different Types of Trojans  
What Do Trojan Creators Look For  
Different Ways a Trojan Can Get into a System  
Indications of a Trojan Attack  
Ports Used by Trojans  
How to Determine which Ports are "Listening"  
Hands-on: Determining What Ports are Listening  
Wrappers  
Hands-on: Wrapping Tool: EliteWrap  
Hands-on: IronGeek Splice  
RemoteByMail  
HTTP Trojans  
ICMP Tunneling  
Trojan: Netcat  
Hands-on: Using Netcat for Basic Exploits  
Hands-on: Netcat 101  
Hands-on: Netcat Banner Dump  
Hacking Tools  
Trojan Detecting Tools  
How to Detect Trojans  
Hands-on: Malware Detection  
Delete Suspicious Device Drivers  
Check for Running Processes: What's on My Computer  
Super System Helper Tool  
Tool: MSConfig  
Hands-on: Keeping Up-To-Date for Malware  
Anti-Trojan Software  
TrojanHunter  
Backdoor Countermeasures  
Tool: Tripwire  
Hands-on: System File Verification  
System File Verification  
How to Avoid a Trojan Infection  
What happened next  
Trojans and Backdoors Review

## **Module 09 - Viruses and Worms**

50m

Viruses and Worms  
Introduction to Virus  
Virus History  
Characteristics of a Virus  
Working of Virus  
Why People Create Computer Viruses  
Symptoms of Virus-Like Attack  
Virus Hoaxes  
Worms  
How is a Worm different from a Virus  
Indications of a Virus Attack  
Hardware Threats

Software Threats  
Stages of Virus Life  
Types of Viruses  
Virus Classification  
How does a Virus Infect  
Storage Patterns of a Virus  
System Sector Viruses  
Stealth Virus  
Bootable CD-ROM Virus  
Self-Modification  
Encryption with a Variable Key  
Polymorphic Code  
Metamorphic Virus  
Cavity Virus  
Sparse Infector Virus  
Companion Virus  
File Extension Virus  
Famous Viruses and Worms  
Famous Viruses/Worms: I Love You Virus  
Zombies and DoS  
Spread of Slammer Worm - 30 min  
Latest Viruses  
Disk Killer  
Writing Virus Programs  
Writing a Simple Virus Program  
Virus Construction Kits  
Examples of Virus Construction Kits  
Hands-on: Stealth Toolv2: Hide Viruses and Malware  
Virus Detection Methods  
Virus Incident Response  
What is Sheep Dip  
Virus Analysis - IDA Pro Tool  
Hands-on: Beast Remote Trojan  
Prevention is Better than Cure  
Anti-Virus Software  
Viruses and Worms Review

## **Module 10 – Sniffers**

1h 4m

Sniffers  
Definition: Sniffing  
Protocols Vulnerable to Sniffing  
Types of Sniffing  
Passive Sniffing  
Active Sniffing  
Hands-on: Engard Packet Builder  
What is Address Resolution Protocol (ARP)  
Hands-on: Sniffers and ARP  
Tool: Network View - Scans the Network for Devices  
Hands-on: Basic Sniffers

Hands-on: TCP Dump  
Wiretap  
RF Transmitter Wiretaps  
Infinity Transmitter  
Slave Parallel Wiretaps  
Switched Port Analyzer (SPAN)  
Lawful Intercept  
Benefits of Lawful Intercept  
Network Components Used for Lawful Intercept  
ARP Spoofing Attack  
How Does ARP Spoofing Work  
Hands-on: ARP Poisoning With Cain  
Hands-on: Cain DNS Spoofing  
Hands-on: SSL MITM  
Hands-on: Cain VoIP  
Mac Duplicating  
Mac Duplicating Attack  
ARP Spoofing Tools  
MAC Flooding Tools  
Threats of ARP Poisoning  
Hands-on: Engage Packet Builder  
IP-based Sniffing  
Linux Sniffing Tools  
DNS Poisoning Techniques  
1. Intranet DNS Spoofing (Local Network)  
2. Internet DNS Spoofing (Remote Network)  
3. Proxy Server DNS Poisoning  
4. DNS Cache Poisoning  
Interactive TCP Relay  
Raw Sniffing Tools  
Features of Raw Sniffing Tools  
Detecting Sniffing  
How to Detect Sniffing  
Countermeasures  
Hands-on: SecureNNTP Tunnel  
Sniffers Review

## **Module 11 - Social Engineering**

1h 3m

Social Engineering  
There is No Patch to Human Stupidity  
What is Social Engineering  
Human Weakness  
"Rebecca" and "Jessica"  
Office Workers  
Types of Social Engineering  
Human-Based Social Engineering  
Human-Based Social Engineering: Eavesdropping  
Human-Based Social Engineering: Shoulder Surfing  
Human-Based Social Engineering: Dumpster Diving

Dumpster Diving Example  
Human-Based Social Engineering (cont'd)  
Movies to Watch for Reverse Engineering Examples: The Italian Job and Catch Me If You Can  
Computer-Based Social Engineering  
Hands-on: Hotmail Social Engineering  
Insider Attack  
Disgruntled Employee  
Preventing Insider Threat  
Common Targets of Social Engineering  
Social Engineering Threats and Defenses  
Online Threats  
Telephone-Based Threats  
Personal Approaches  
Defenses Against Social Engineering Threats  
Factors that make Companies Vulnerable to Attacks  
Why is Social Engineering Effective  
Warning Signs of an Attack  
Tool: Netcraft Anti-Phishing Toolbar  
Phases in a Social Engineering Attack  
Behaviors Vulnerable to Attacks  
Impact on the Organization  
Countermeasures  
Policies and Procedures  
Impersonating on Facebook  
Identity Theft  
Hands-on: Social Engineering Example  
Social Engineering Review

## **Module 12 – Phishing**

21m

Phishing  
Introduction  
Reasons for Successful Phishing  
Phishing Methods  
Process of Phishing  
Types of Phishing Attacks  
Man-in-the-Middle Attacks  
URL Obfuscation Attacks  
Cross-site Scripting Attacks  
Hidden Attacks  
Client-side Vulnerabilities  
Deceptive Phishing  
Malware-Based Phishing  
DNS-Based Phishing  
Content-Injection Phishing  
Search Engine Phishing  
Anti-Phishing  
Hands-on: Phishing Video  
Phishing Review

## **Module 13 - Hacking Email Accounts**

11m

Hacking Email Accounts  
Introduction  
Ways for Getting Email Account Information  
Stealing Cookies  
Social Engineering  
Password Phishing  
Fraudulent e-mail Messages  
Vulnerabilities  
Vulnerabilities: Web Email  
Email Hacking Tools  
Securing Email Accounts  
Creating Strong Passwords  
Sign-in Seal  
Alternate Email Address  
Keep Me Signed In/Remember Me  
Hands-on: Hacking Email Accounts  
Hacking Email Accounts Review

## **Module 14 - Denial of Service**

38m

Denial of Service  
Terminologies  
Goal of DoS  
Impact and the Modes of Attack  
Types of Attacks  
DoS Attack Classification  
Smurf Attack  
Buffer Overflow Attack  
Ping of Death Attack  
Hands-on: Ping of Death and Nemesy  
Teardrop Attack  
SYN Attack  
SYN Flooding  
DoS Attack Tools  
Bot (Derived from the Word RoBOT)  
Botnets  
Uses of Botnets  
Types of Bots  
How Do They Infect? Analysis Of Agabot  
DDoS Unstoppable  
DDoS Attack Taxonomy  
Reflective DNS Attacks  
DDoS Tools  
How to Conduct a DDoS Attack  
Reflection of the Exploit  
Countermeasures for Reflected DoS  
Taxonomy of DDoS Countermeasures  
Preventing Secondary Victims  
Detect and Neutralize Handlers  
Mitigate or Stop the Effects of DDoS Attacks

Post-attack Forensics  
Denial of Service Review

## **Module 15 - Session Hijacking**

32m

Session Hijacking  
What is Session Hijacking  
Understanding Session Hijacking  
Spoofing vs. Hijacking  
Steps in Session Hijacking  
Types of Session Hijacking  
Session Hijacking Levels  
Network Level 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: Packet Sniffer  
UDP Hijacking  
Application Level Hijacking  
Session Hijacking Tools  
Programs that Perform Session Hijacking  
Dangers Posed by Hijacking  
Countermeasures  
Protecting against Session Hijacking  
Countermeasure: IP Security  
What Happened Next  
Hands-on: Tsight Session Hijack  
Session Hijacking Review

## **Module 16 - Hacking Web Servers**

2h 39m

Hacking Web Servers  
How are Web Servers Compromised  
Web Server Defacement  
How are Web Servers Defaced  
Attacks Against IIS  
IIS 7 Components  
IIS Directory Traversal (Unicode) Attack  
ServerMask ip100  
Unicode  
Hands-on: Input Injection Attack  
Hands-on: Viewing Website with Telnet  
Core Impact Professional 101  
Core Impact Professional  
Networking Attack Vector  
Client Side Application Testing  
Web Application Testing

Core Impact Professional 101 Review  
Patch Management  
Hotfixes and Patches  
What is Patch Management  
Vulnerability Scanners  
Hands-on: Spider  
Countermeasures  
File System Traversal Countermeasures  
Increasing Web Server Security  
Hacking Web Servers Review

## **Module 17 - Web Application Vulnerabilities**

1h 42m

Web Application Vulnerabilities  
Web Application Setup  
Web Application Hacking  
Anatomy of an Attack  
Web Application Threats  
Cross-Site Scripting/XSS Flaws  
Countermeasures 01  
SQL Injection  
Command Injection Flaws  
Countermeasures 02  
Cookie/Session Poisoning  
Countermeasures 03  
Parameter/Form Tampering  
Buffer Overflow  
Countermeasures 04  
Directory Traversal/Forceful Browsing  
Countermeasures 05  
Cryptographic Interception  
Cookie Snooping  
Authentication Hijacking  
Countermeasures 06  
Log Tampering  
Error Message Interception  
Attack Obfuscation  
Platform Exploits  
DMZ Protocol Attacks  
Countermeasures 07  
Security Management Exploits  
Web Services Attacks  
Zero-Day Attacks  
Network Access Attacks  
Hands-on: WebGoat  
Hands-on: NTO Spider  
Web Application Vulnerabilities Review

## **Module 18 - Web-Based Password Cracking Techniques**

41m

Web-Based Password Cracking Techniques

- Authentication
  - Authentication - Definition
  - Authentication Mechanisms
  - HTTP Authentication
  - Basic Authentication
  - Digest Authentication
  - Integrated Windows (NTLM) Authentication
  - Negotiate Authentication
  - Certificate-based Authentication
  - Forms-based Authentication
  - RSA SecurID Token
  - Biometrics Authentication
    - Types of Biometrics Authentication
    - Fingerprint-based Identification
    - Hand Geometry-based Identification
    - Retina Scanning
    - Afghan Woman Recognized After 17 Years
    - Face Recognition
    - Face Code: WebCam Based Biometrics Authentication System
- Password Cracking
  - How to Select a Good Password
  - Things to Avoid in Passwords
  - Changing Your Password
  - Windows XP: Remove Saved Passwords
  - What is a Password Cracker
  - Modus Operandi of an Attacker Using Password Cracker
  - How does a Password Cracker Work
  - Attacks - Classification
  - Password Guessing
  - Query String
  - Cookies
  - Dictionary Maker
  - Password Cracking Tools
  - Security Tools
  - Password Administrator
  - Countermeasures
  - Hands-on: Cracking Passwords with Xhydra
- Web-Based Password Cracking Techniques Review

## **Module 19 - SQL Injection**

38m

SQL Injection

- What is SQL Injection
- Exploiting Web Applications
- SQL Injection Steps
- What Should You Look For
- What If It Doesn't Take Input
- OLE DB Errors
- SQL Injection Techniques

How to Test for SQL Injection Vulnerability  
How Does it Work  
BadLogin.aspx.cs  
Executing Operating System Commands  
Getting Output of SQL Query  
Getting Data from the Database Using ODBC Error Message  
SQL Injection in Oracle  
SQL Injection in MySQL Database  
Attack Against SQL Servers  
SQL Server Resolution Service (SSRS)  
Osql L-Probing  
SQL Injection Tools  
SQL Injection Automated Tools  
Blind SQL Injection  
Blind SQL Injection: Countermeasures  
SQL Injection Countermeasures  
Preventing SQL Injection Attacks  
Hands-on: SQL Injection  
Hands-on: SQL with Lee Lawson  
SQL Injection Review

## **Module 20 - Hacking Wireless Networks**

2h 46m

Hacking Wireless Networks  
Introduction to Wireless Networking  
Wired Network vs. Wireless Network  
Effects of Wireless Attacks on Business  
Types of Wireless Network  
Hands-on: Techtionary Website  
Advantages and Disadvantages of a Wireless Network  
Wireless Standards  
Wireless Standard: 802.11a  
Wireless Standard: 802.11b - "WiFi"  
Wireless Standard: 802.11g  
Wireless Standard: 802.11i  
Wireless Standard: 802.11n  
Related Technology and Carrier Networks  
Antennas  
Hands-on: Resources for Antennas  
Cantenna  
Wireless Access Points  
Hands-on: Linksys AP Config SSID  
Hands-on: Asus WL530G Config SSID  
SSID  
Beacon Frames  
Is the SSID a Secret  
Setting up a WLAN  
Authentication and Association  
Authentication Modes  
Hands-on: Authentication Settings

The 802.1X Authentication Process  
Wired Equivalent Privacy (WEP)  
Hands-on: WEP Setup Security  
WEP Issues  
What is WPA  
WPA  
WPA Vulnerabilities  
WEP, WPA, and WPA2  
WPA2 Wi-Fi Protected Access 2  
Attacks and Hacking Tools  
Terminologies  
Authentication and (Dis)Association Attacks  
WEP Attack  
Cracking WEP  
Hands-on: Hacking WEP Encryption  
Weak Keys (a.k.a. Weak IVs)  
Problems with WEP's Key Stream and Reuse  
Automated WEP Crackers  
Attacking WPA Encrypted Networks  
Hands-on: Cracking WPA with Cain and Abel  
Evil Twin: Attack  
Rogue Access Points  
Hands-on: Tool: NetStumbler  
Cloaked Access Point  
Temporal Key Integrity Protocol (TKIP)  
Hands-on: WEP Cracking with Cain and Abel  
Hands-on: MAC SSID Security  
Phone Jammers  
Phone Jammer: Mobile Blocker  
2.4Ghz Wi-Fi & Wireless Camera Jammer  
3 Watt Digital Cell Phone Jammer  
3 Watt Quad Band Digital Cellular Mobile Phone Jammer  
Detecting a Wireless Network  
Scanning Tools  
Hands-on: Tool: Kismet in Linux  
Hands-on: Alternate War Driving  
Sniffing Tools  
Hands-on: Wireless Sniffing with Omni-Peek  
Hands-on: Airmagnet Laptop Analyzer  
Hacking Wireless Networks 02  
Step 1: Find Networks to Attack  
Step 2: Choose the Networks to Attack  
Step 3: Analyzing the Network  
Step 4: Cracking the WEP Key  
Step 5: Sniffing the Network  
Wireless Security  
Radius: Used as Additional Layer in Security  
Securing Wireless Networks  
WLAN Security: Passphrase

Don'ts in Wireless Security  
Wireless Security Tools  
Google Secure Access  
Hands-on: Tool: Insider  
Hands-on: Tool: WiSpy Spectrum Analyzer  
Hands-on: Tool: Jasager Fon Router  
Hands-on: Tips and Resources  
Hacking Wireless Networks Review

## **Module 21 - Physical Security**

48m

Physical Security  
Security Facts  
Understanding Physical Security  
Physical Security 02  
What Is the Need for Physical Security  
Who Is Accountable for Physical Security  
Factors Affecting Physical Security  
Physical Security Checklist 01  
Physical Security Checklist: Company Surroundings  
Gates  
Security Guards  
Physical Security Checklist: Premises  
CCTV Cameras  
Physical Security Checklist: Reception  
Physical Security Checklist: Server  
Physical Security Checklist: Workstation Area  
Physical Security Checklist: Wireless Access Points  
Physical Security Checklist: Other Equipment  
Physical Security Checklist: Access Control  
Physical Security Checklist: Biometric Devices  
Biometric Identification Techniques  
Authentication Mechanisms  
Authentication Mechanisms Challenges: Biometrics  
Faking Fingerprints  
Physical Security Checklist 02  
Smart Cards  
Security Token  
Computer Equipment Maintenance  
Wiretapping  
Remote Access  
Locks  
Lock Picking  
Lock Picking Tools  
Information Security  
EPS (Electronic Physical Security)  
Wireless Security  
Laptop Theft Statistics for 2007  
Statistics for Stolen and Recovered Laptops  
Laptop Theft

Laptop Security Tools  
Laptop Tracker - Xtool Computer Tracker  
Laptop Security Countermeasures  
Mantrap  
TEMPEST  
Challenges in Ensuring Physical Security  
Spyware Technologies  
Physical Security: Lock Down USB Ports  
Hands-on: Bump Key Animation  
Physical Security Review

## **Module 22 - Linux Hacking**

1h 24m

Linux Hacking  
Why Linux  
Linux - Basics  
Linux Live CD-ROMs  
Basic Commands of Linux: Files & Directories  
Linux Networking Commands  
Directories in Linux  
Installing, Configuring, and Compiling Linux Kernel  
How to Install a Kernel Patch  
Compiling Programs in Linux  
Make Files  
Make Install Command  
Linux Vulnerabilities  
Chrooting  
Why is Linux Hacked  
How to Apply Patches to Vulnerable Programs  
Port Scan Detection Tools  
Password Cracking in Linux: Xcrack  
Firewall in Linux: IPTables  
Basic Linux Operating System Defense  
Linux Loadable Kernel Modules  
Hacking Tool: Linux Rootkits  
Rootkit: Countermeasures  
Linux Tools: Application Security  
Advanced Intrusion Detection Environment (AIDE)  
Linux Tools: Encryption  
Steps for Hardening Linux  
Hands-on: BackTrack2 KDE or FluxBox Desktops  
Hands-on: BT2 Shell Basics  
Hands-on: BT2 Password Files  
Hands-on: BT2 User Account Changes  
Hands-on: BT2 Network Config  
Hands-on: BT2 Mounting with VMWare  
Hands-on: BT2 Compiling from Source Code  
Hands-on: BT2 Overview of Services  
Linux Hacking Review

## **Module 23 - Evading IDS, Firewalls and Honeypots**

1h 17m

Evading IDS, Firewalls and Honeypots

Introduction to Intrusion Detection Systems

Terminologies

Intrusion Detection System

Intrusion Detection System (IDS)

IDS Placement

Ways to Detect an Intrusion

Types of Intrusion Detection Systems

System Integrity Verifiers (SIV)

Tripwire ([www.tripwire.com](http://www.tripwire.com))

Cisco Security Agent (CSA)

True/False, Positive/Negative

Signature Analysis

General Indications of Intrusion System Indications

General Indications of Intrusion File System Indications

General Indications of Intrusion Network Indications

Intrusion Detection Tools

Snort

Hands-on: Snort IDS Testing Scanning Tools

Running Snort on Windows 2003

Snort Rules

SnortSam

Steps to Perform After an IDS Detects an Attack

Evading IDS Systems

Ways to Evade IDS

Tools to Evade IDS

Hands-on: Secure Tunnels and Anonymizer Techniques

Firewall

What is a Firewall

What does a Firewall do

Packet Filtering

What can't a Firewall do

How does a Firewall Work

Hands-on: Video: Warriors of the Net

Hardware Firewall

Types of Firewalls

Packet Filtering Firewall

Circuit-Level Gateway

Application-Level Firewall

Stateful Multilayer Inspection Firewall

Firewall Identification

Firewalking

Banner Grabbing

Breaching Firewalls

Placing Backdoors Through Firewalls

Honeypot

What is a Honeypot

The HoneyNet Project

Types of Honeypots

Advantages and Disadvantages of a Honeypot  
Where to Place a Honeypot  
Physical and Virtual Honeypots  
Tools to Detect Honeypots  
What to do When Hacked  
Evading IDS, Firewalls and Honeypots Review

## **Module 24 - Buffer Overflows**

1h 8m

Buffer Overflows  
Why are Programs/Applications Vulnerable  
Buffer Overflows 02  
Reasons for Buffer Overflow Attacks  
Knowledge Required to Program Buffer Overflow Exploits  
Understanding Stacks  
Hands-on: Stack Function  
Hands-on: Saint Exploit of Windows XP  
Understanding Heaps  
Types of Buffer Overflows: Stack-Based Buffer Overflow  
Stack Based Buffer Overflows  
Types of Buffer Overflows: Heap-Based Buffer Overflow  
Heap-Based Buffer Overflow  
Understanding Assembly Language  
Shellcode  
How to Detect Buffer Overflows in a Program  
Hands-on: Fuzzing for Weaknesses  
Attacking a Real Program  
Hands-on: Metasploit Introduction  
Hands-on: Metasploit 101  
Hands-on: Metasploit Interactive  
NOPS  
How to Mutate a Buffer Overflow Exploit  
Once the Stack is Smashed...  
Defense Against Buffer Overflows  
Tool to Defend Buffer Overflow: Return Address Defender (RAD)  
Tool to Defend Buffer Overflow: StackGuard  
Valgrind  
Insure++  
Hands-on: Compiling Exploits from Source Code  
Buffer Overflows Review

## **Module 25 – Cryptography**

1h 15m

Cryptography  
Cryptography 02  
Classical Cryptographic Techniques  
Hands-on: Cryptanalysis with Cryptool  
Encryption  
Decryption  
Cryptographic Algorithms

Hands-on: Hashes to Verify Downloads  
RSA (Rivest Shamir Adleman)  
RSA Attacks  
RSA Challenge  
Data Encryption Standard (DES)  
DES Overview  
RC4, RC5, RC6, Blowfish  
Hands-on: RC4 with Cryptool  
RC5  
Message Digest Functions  
One-way Hash Functions  
MD5  
SHA (Secure Hash Algorithm)  
SSL (Secure Sockets Layer)  
What is SSH  
Hands-on: IPSEC Sessions  
Algorithms and Security  
Hands-on: Hardware Encryption  
Disk Encryption  
Government Access to Keys (GAK)  
Digital Signature  
Hands-on: Digital Signatures with Cryptool  
Components of a Digital Signature  
Method of Digital Signature Technology  
Digital Signature Applications  
Digital Signature Standard  
Digital Signature Algorithms: ECDSA, ElGamal Signature Scheme  
Challenges and Opportunities  
Digital Certificates  
Encryption Engine  
Code Breaking: Methodologies  
Cryptanalysis  
Cryptography Attacks  
Brute-Force Attack  
Cryptography Review  
Course Closure

**Total Duration: 35h 11m**