

# EC-Council - Certified Security Analyst

## Course Introduction

3 m

## Student Introduction

9m

Student Introduction  
Certification  
ECSA Track  
LPT Track  
What next after ECSA Training?  
Demo - Overview of Available Resources  
Lab Sessions  
Student Introduction Review

## Module 01 - The Need for Security Analysis

2h 41m

The Need for Security Analysis  
What are we Concerned About?  
So What are you Trying to Protect?  
Why are Intrusions so Often Successful?  
What are the Greatest Challenges?  
Environmental Complexity  
New Technologies  
New Threats and Exploits  
Demo - Keep Updated with Research  
Limited Focus  
Limited Expertise  
Tool: Data Loss Cost Calculator  
Demo - Tech//404 Data Loss Calculator  
In Order to Ensure...  
Authentication  
Authorization  
Confidentiality  
Integrity  
Availability  
Non-Repudiation  
We Must be Diligent  
Threat Agents  
Assessment Questions  
How Much Security is Enough?  
Risk  
Simplifying Risk  
Risk Analysis  
Risk Assessment Answers Seven Questions:  
Steps of Risk Assessment  
Demo - Risk Assessment  
Demo - CIO-view Self-assessment  
Risk Assessment Values  
Demo - Quantitative Threat Analysis  
Information Security Awareness  
Security Policies  
Security Policy Basics  
Demo - Policy Templates  
Types of Policies  
Promiscuous Policy

Permissive Policy  
Prudent Policy  
Paranoid Policy  
Acceptable-Use Policy  
User-Account Policy  
Remote-Access Policy  
Information-Protection Policy  
Firewall-Management Policy  
Special-Access Policy  
Network-Connection Policy  
Business-Partner Policy  
Data Classification Policies  
Intrusion Detection Policies  
Virus Prevention Policies  
Laptop Security Policy  
Personal Security Policy  
Cryptography Policy  
Fair and Accurate Credit Transactions Act of 2003 (FACTA)  
Other Important Policies  
Policy Statements  
Basic Document Set of Information Security Policies  
ISO 17799  
Domains of ISO 17799  
No Simple Solutions  
U.S. Legislation  
California SB 1386  
Sarbanes-Oxley 2002  
Gramm-Leach-Bliley Act (GLBA)  
Health Insurance Portability and Accountability Act (HIPAA)  
USA Patriot Act 2001  
U.K. Legislation  
How Does This Law Affect a Security Officer?  
The Data Protection Act 1998  
The Human Rights Act 1998  
Interception of Communications  
The Freedom of Information Act 2000  
The Audit Investigation and Community Enterprise Act 2005  
Demo - Vmware Overview  
Demo - Opening an Existing XP VMware System  
Demo - Opening VM Appliance  
Demo - Installing a New VM System  
Demo - Booting XP from Backtrack ISO  
Module 01 Review

## **Module 02 - Advanced Googling**

39m

Advanced Googling  
Site Operator  
intitle:index.of  
Demo - Default Pages: tsweb  
error | warning  
Demo - Google as a Proxy  
login | logon  
username | userid | employee.ID | "your username is"  
password | passcode | "your password is"  
admin | administrator  
-ext:html -ext:htm -ext:shtml -ext:asp -ext:php

inurl:temp | inurl:tmp | inurl:backup | inurl:bak  
Google Advanced Search Form  
Categorization of the Operators  
allinanchor:  
allintext:  
Demo - Google Locating Live Cams  
Locating Public Exploit Sites  
Locating Exploits via Common Code Strings  
Locating Vulnerable Targets  
Locating Targets via Demonstration Pages  
Demo - Google Hack HoneyPot  
Demo - Goolag and Wikto  
Demo - Wikto Results and Google Guide  
Module 02 Review

### **Module 03 - TCP/IP Packet Analysis**

1h 21m

TCP/IP Packet Analysis  
TCP/IP Model  
Demo - TCP/IP Movie Recommendation  
Application Layer  
Transport Layer  
Internet Layer  
Network Access Layer  
Comparing OSI and TCP/IP  
Demo - Engage Packet Builder  
TCP  
TCP Header  
IP Header: Protocol Field  
UDP  
TCP and UDP Port Numbers  
Port Numbers  
Demo - Warriors of the Net  
IANA  
Source and Destination Port Numbers  
Demo - Techtionary.com Port Numbers  
What Makes Each Connection Unique?  
Structure of a Packet  
TCP Operation  
Three-Way Handshake  
Demo - Techtionary.com TCP Handshake  
Flow Control  
Windowing  
Windowing and Window Sizes  
Simple Windowing  
Acknowledgement  
Sliding Windows  
Sequencing Numbers  
Synchronization  
Positive Acknowledgment and Retransmission (PAR)  
What is Internet Protocol v6 (IPv6)?  
Why IPv6?  
IPv4/IPv6 Transition Mechanisms  
IPv6 Security Issues  
Security Flaws in IPv6  
IPv6 Infrastructure Security  
Ipsec

Firewalls and Packet Filtering  
Denial-of-Service (DoS) Attacks  
UDP Operation  
Internet Control Message Protocol (ICMP)  
ICMP Message Delivery  
Format of an ICMP Message  
Unreachable Networks  
Time Exceeded Message  
IP Parameter Problem  
ICMP Control Messages  
ICMP Redirects  
Clock Synchronization and Transit Time Estimation  
Information Requests and Reply Message Formats  
Address Masks  
Router Solicitation and Advertisement  
Module 03 Review

## **Module 04 - Advanced Sniffing Techniques**

50m

Advanced Sniffing Techniques  
Demo - Basic Sniffers  
Demo - Packet Capturing with Windows Packetizer  
What is Wireshark?  
Wireshark: Filters  
Wireshark: Tshark  
Wireshark: Tcpdump  
Demo - Tcpdump  
Protocol Dissection  
Steps to Solve GNU/ Linux Server Network Connectivity Issues  
Using Wireshark for Network Troubleshooting  
Using Wireshark for System Administration  
ARP Problems  
Demo - Sniffers and ARP  
ICMP Echo Request/Reply Header Layout  
TCP Flags  
Scenario 1: SYN no SYN+ACK  
Scenario 2: SYN Immediate Response RST  
Scenario 3: SYN SYN+ACK ACK  
Tapping into the Network  
Using Wireshark for Security Administration  
Sniffer Detection  
Wireless Sniffing with Wireshark  
Frequency  
Using Channel Hopping  
Interference and Collisions  
Recommendations for Sniffing Wireless Traffic  
Analyzing Wireless Traffic  
IEEE 802.11 Header  
Filters  
Unencrypted Data Traffic  
Identifying Hidden SSIDs  
Identifying EAP Authentication Failures  
Identifying WEP  
Identifying IPsec/VPN  
Decrypting Traffic  
Scanning  
TCP Connect Scan

SYN Scan  
XMAS Scan  
Null Scan  
Remote Access Trojans  
Wireshark DNP3 Dissector Infinite Loop Vulnerability  
Time Stamps  
Time Zones  
Packet Reassembling  
Checksums  
Module 04 Review

## **Module 05 - Vulnerability Analysis with Nessus**

50m

Vulnerability Analysis with Nessus  
Nessus  
Features of Nessus  
Nessus Assessment Process  
Demo - Nessus on Windows  
Demo - Nessus on Windows Cont'd and GFI LANguard Comparison  
False Positives  
Examples of False Positives  
Identifying False Positives  
Suspicious Signs  
Demo - Backtrack 4 Nessus Install  
Module 05 Review

## **Module 06 - Advanced Wireless Testing**

2h 42m

Advanced Wireless Testing  
Wireless Concepts  
Demo - Techtionary Website  
802.11 Types  
Core Issues with 802.11  
What's the Difference?  
Other Types of Wireless  
Spread Spectrum Background  
Channels  
Access Point  
Service Set ID  
Demo - Linksys-AP Config SSID  
Default SSIDs  
Chipsets  
Wi-Fi Equipment  
Expedient Antennas  
Vulnerabilities to 802.1x and RADIUS  
Security - WEP  
Wired Equivalent Privacy (WEP)  
Exclusive OR  
Encryption Process  
Chipping Sequence  
WEP Issues

WEP - Authentication Phase  
WEP - Shared Key Authentication  
WEP - Association Phase  
WEP Flaws  
WEP Attack

Demo - Authentication Settings  
Demo - WEP Set-Up Security  
Demo - Cain and Abel WEP Cracking  
WPA Interim 802.11 Security  
WPA  
Demo - Cracking WPA with Cain and Abel  
WPA2 (Wi-Fi Protected Access 2)  
802.1X Authentication and EAP  
EAP Types  
Cisco LEAP  
TKIP (Temporal Key Integrity Protocol)  
Wireless Networks Testing  
Wireless Communications Testing  
Report Recommendations  
Wireless Attack Countermeasures  
Demo - MAC-SSID Security  
Wireless Penetration Testing with Windows  
War Driving  
The Jargon – WarChalking  
Wireless: Tools of the Trade  
Demo - Kismet in Windows  
Demo - Tool: Kismet in Linux  
Demo - Vistumbler War Driving and GPS Map Plotting  
How Does NetStumbler Work?  
“Active” vs. “Passive” WLAN Detection  
Disabling the Beacon  
Running NetStumbler  
Demo - Tool: Netstumbler  
AirCrack-ng  
AirCrack-ng: How Does it Work?  
AirCrack-ng: FMS and Korek Attacks  
AirCrack-ng: Notes  
Demo - Hacking WEP Encryption  
Determining Network Topology: Network View  
WarDriving and Wireless Penetration Testing with OS X  
Using a GPS  
Deauthenticating Clients  
StumbVerter  
MITM Attack Design  
MITM Attack Variables  
Hardware for the Attack: Antennas, Amps, and WiFi Cards  
Choosing the Right Antenna  
Amplifying the Wireless Signal  
IP Forwarding and NAT using IPTables  
Demo - Jasager for Router  
Module 06 Review

## **Module 07 - Designing a DMZ**

Designing a DMZ  
Introduction  
DMZ Concepts  
DMZ Design Fundamentals

27m

Advanced Design Strategies  
Types of Firewall and DMZ Architectures  
"Inside vs. Outside" Architecture  
"Three-Homed Firewall" DMZ Architecture  
Weak Screened Subnet Architecture  
Strong Screened Subnet Architecture  
Designing a DMZ using IPtables  
Designing Windows DMZ  
Precautions for DMZ Setup  
Demo - Designing DMZs  
Advanced Implementation of a Solaris DMZ Server  
Solaris DMZ Servers in a Conceptual Highly Available Configuration  
Hardening Checklists for DMZ Servers and Solaris  
Placement of Wireless Equipment  
Access to DMZ and Authentication Considerations  
Wireless DMZ Components  
WLAN DMZ Security Best Practices  
Ethernet Interface Requirements and Configuration  
DMZ Router Security Best Practice  
Six Ways to Stop Data Leaks  
Module 07 Review

## **Module 08 - Snort Analysis**

48m

Snort Analysis  
Snort Overview  
Modes of Operation  
Features of Snort  
Configuring Snort  
Snort: Variables  
Snort: Pre-processors  
Snort: Output Plug-ins  
Snort: Rules  
How Snort Operates  
Initializing Snort  
Demo - Snort IDS Testing Scanning Tools  
Signal Handlers  
Parsing the Configuration File  
Decoding  
Possible Decoders  
Pre-processing  
Detection  
Content Matching  
The Stream4 Pre-processor  
Inline Functionality  
Writing Snort Rules  
Snort Rule Header  
Snort Rule Header: Actions  
Snort Rule Header: Other Fields  
IP Address Negation Rule  
IP Address Filters  
The direction Operator  
Rule Options  
Activate/Dynamic Rules  
Metadata Rule Options: msg  
The reference Keyword  
The sid/rev Keyword

The classtype Keyword  
Payload Detection Rule Options: content  
Modifier Keywords  
The uricontent Keyword  
The fragoffset Keyword  
Writing Good Snort Rules  
Tool for Writing Snort Rules: IDS Policy Manager  
HoneyNet Security Console Tool  
Key Features  
Module 08 Review

## **Module 09 - Log Analysis**

30m

Log Analysis  
Logs  
Events that Need to be Logged  
What to Look Out For in Logs  
Automated Log Analysis Approaches  
Log Shipping  
Syslog  
Setting up a Syslog  
System Error Logs  
Kiwi Syslog Daemon  
Configuring Kiwi Syslog to Log to a MS SQL Database  
Configuring a Cisco Router for Syslog  
Configuring a DLink Router for Syslog  
Gathering Log Files from an IIS Web Server  
Apache Web Server Log  
AWStats Log Analyzer  
Cisco Router Logs  
Analyzing Netgear Wireless Router Logs  
Wireless Traffic Analysis Using Wireshark  
Configuring Firewall Logs in Local Windows System  
Viewing Local Windows Firewall Log  
Viewing Windows Event Log  
Collecting & Monitoring UNIX Syslog  
iptables  
Log Prefixing with iptables  
Firewall Log Analysis with grep  
SQL Database Log  
Using SQL Server to Analyze Web Logs  
Analyzing Oracle Logs: The Oracle Metric Log File  
ApexSQL Log  
Analyzing Solaris System Logs  
Demo - Splunk  
Module 09 Review

## **Module 10 - Advanced Exploits and Tools**

1h 39m

Advanced Exploits and Tools  
Common Vulnerabilities  
Buffer Overflows Revisited  
Smashing the Stack for Fun and Profit  
Smashing the Heap for Fun and Profit



Format Strings for Chaos and Mayhem  
The Anatomy of an Exploit  
Demo - Fuzzing for Weaknesses  
Vulnerable Code  
Shellcode  
Shellcode Examples  
Shellcode (cont'd)  
Demo - Stack Function  
Delivery Code  
Delivery Code: Example  
Demo - Compiling Exploits from Source Code  
Linux Exploits versus Windows  
Windows versus Linux  
Tools of the Trade: Debuggers  
Tools of the Trade: GDB  
Tools of the Trade: Metasploit  
Demo - Metasploit Intro  
Demo - Metasploit 101  
Demo - Metasploit Interactive  
Tools of the Trade: Canvas  
Lab  
Tools of the Trade: CORE Impact  
Ways to Use CORE Impact  
Microsoft Baseline Security Analyzer (MBSA)  
Network Security Analysis Tool (NSAT)  
Sunbelt Network Security Inspector (SNSI)  
Demo - Saint Exploit of Windows XP  
Demo - dcom101 Exploit Autoshovel of Shell  
Demo - dcom Exploit Netcat Shovel of Shell and Extracting Hashes  
Demo - Backtrack 4 Milw0rm Metasploit Updates  
Module 10 Review

## **Module 11 - Penetration Testing Methodologies**

1h 54m

Penetration Testing Methodologies  
Demo - dradis Effective Information Sharing  
What is Penetration Testing?  
Why Penetration Testing?  
What Should be Tested?  
What Makes a Good Penetration Test?  
Common Penetration Testing Techniques  
Penetration Testing Process  
Scope of Penetration Testing  
Blue Teaming/Red Teaming  
Types of Penetration Testing  
Black-box Penetration Testing  
White-box Penetration Testing  
Announced Testing/ Unannounced Testing  
Grey-box Penetration Testing  
Strategies of Penetration Testing  
External Penetration Testing  
Internal Security Assessment  
Application Security Assessment  
Types of Application Security Assessment  
Network Security Assessment  
Wireless/Remote Access Assessment  
Telephony Security Assessment

- Social Engineering
- Penetration Testing Consultants
- Required Skills Sets
- Hiring a Penetration Tester
- Responsibilities of a Penetration Tester
- Profile of a Good Penetration Tester
- Why Should the Company Hire You?
- Companies' Concerns
- Methodology
- Demo - NIST Methodology
- Demo - PenTest Templates and Methodologies
- Penetration Testing Roadmap
- Guidelines for Security Checking
- Operational Strategies for Security Testing
- Security Category of the Information System
- Identifying Benefits of Each Test Type
- Prioritizing the Systems for Testing
- ROI on Penetration Testing
- Determining Cost of Each Test Type
- Need for a Methodology
- Penetration Test vs. Vulnerability Test
- Reliance on Checklists and Templates
- Phases of Penetration Testing
- Pre-Attack Phase
- Best Practices
- Results that can be Expected
- Passive Reconnaissance
- Active Reconnaissance
- Attack Phase
- Activity: Perimeter Testing
- Activity: Web Application Testing - I
- Activity: Web Application Testing – II
- Activity: Wireless Testing
- Activity: Acquiring Target
- Activity: Escalating Privileges
- Activity: Execute, Implant, and Retract
- Post-Attack Phase and Activities
- Module 11 Review

## **Module 12 - Customers and Legal Agreements**

27m

- Customers and Legal Agreements
- Why do Organizations Need Pen-Testing?
- Initial Stages in Penetration Testing
- Understand Customer Requirements
- Create a Checklist of Testing Requirements
- Penetration Testing 'Rules of Behavior'
- Demo - ISSAF Customers and Legal
- Penetration Testing Risks
- Penetration Testing by Third Parties
- Precautions While Outsourcing Penetration Testing
- Legal Consequences
- Demo - Computer Crimes and Implications
- Get Out of Jail Free Card
- Permitted Items in Legal Agreement
- Confidentiality and NDA Agreements
- Non-Disclosure and Secrecy Agreements (NDA)

The Contract  
Liability Issues  
Negligence Claim  
Plan for the Worst  
Drafting Contracts  
How Much to Charge?  
Module 12 Review

### **Module 13 - Rules of Engagement**

11m

Rules of Engagement  
Rules of Engagement (ROE)  
Demo - OSSTMM Model  
Scope of ROE  
Steps for Framing ROE  
Clauses in ROE  
Demo - ScreenHunter Desktop Capture Tool  
Module 13 Review

### **Module 14 - Penetration Testing Planning and Scheduling**

1h 10m

Penetration Testing Planning and Scheduling  
Test Plan  
Purpose of Test Plan  
Building a Penetration Test Plan  
Demo - Overview OSSTMM  
IEEE STD. 829–1998 SECTION HEADINGS  
Test Plan Identifier  
Test Deliverables  
Penetration Testing Planning Phase  
Define the Scope  
Project Scope  
When to Retest?  
Responsibilities  
Skills and Knowledge Required  
Internal Employees  
Penetration Testing Teams  
Tiger Team  
Building Tiger Team  
Questions to Ask Before Hiring Consultants to the Tiger Team  
Meeting With the Client  
Kickoff Meeting  
Penetration Testing Project Plan  
Work Breakdown Structure or Task List  
Penetration Testing Schedule  
Penetration Testing Project Scheduling Tools  
Test Plan Checklist  
Penetration Testing Hardware/Software Requirements  
EC-Council's Vampire Box  
Begin Penetration Testing  
Demo - Installing Backtrack 4 into VMWare Environment  
Module 14 Review

### **Module 15 - Pre-Penetration Testing Checklist**

25m

Pre-Penetration Testing Checklist  
Demo - Pentest Checklist  
Step 1: Gather Information about Client Organization's History and Background

Step 2: Visit the Client Organization Premises  
 Step 3: List the Client Organization's Penetration Testing Requirements  
 Step 4: Obtain Penetration Testing Permission from the Company's Stakeholders  
 Step 5: Obtain Detailed Proposal of Test and Services that are Proposed to be carried out  
 Step 6: Identify the Office Space/Location your Team would be Working in for this Project  
 Step 7: Obtain Temporary Identity Cards from the Organization for the Team who is Involved in the Process  
 Step 8: Identify who will be Leading the Penetration Testing Project (Chief Penetration Tester)  
 Step 9: Request from the Client Organization the Previous Penetration Testing/Vulnerability Assessment Reports  
 Step 10: Prepare Rules of Engagement that Lists the Company's Core Competencies/ Limitations/ Timescales  
 Step 11: Hire a Lawyer who Understands IT and can Handle your Penetration Testing Legal Documents  
 Step 12: Prepare PT Legal Document and get Vetted with your Lawyer  
 Step 13: Prepare Non Disclosure Agreement (NDA) and have the Client Sign them  
 Step 14: Obtain (if possible) Liability Insurance from a Local Insurance Firm  
 Step 15: Identify your Core Competencies/Limitations  
 Step 16: Allocate a Budget for the Penetration Testing Project ( X amount of \$ )  
 Step 17: Prepare a Tiger Team  
 Step 18: List the Security Tools that you will be using for the Penetration Testing Project  
 Step 19: List the Hardware and Software Requirements for the Penetration Testing Project  
 Step 20: Identify the Clients Security Compliance Requirements  
 Step 21: List the Servers, Workstations, Desktops and Network Devices that need to be Tested  
 Step 22: Identify the Type of Testing that would be carried out - Black Box or White Box Testing  
 Step 23: Identify the Type of Testing that would be carried out - Announced/ Unannounced  
 Step 24: Identify Local Equipment Required for Pen Test  
 Step 25: Identify Local Manpower Required for Pen Test  
 Step 26: List the Contact Details of Personnel from Client Organization who will be in Charge of the Pen Test  
 Step 27: Obtain the Contact Details of the Key Personnel for Approaching in case of an Emergency  
 Step 29: List the Tests that will not be carried out at the Client Network  
 Step 30: Identify the Purpose of the Test you are carrying out at the Client Organization  
 Step 31: Identify the Network Topology in which the Test would be carried out  
 Step 32: Obtain Special Permission if Required from Local Law Enforcement Agency  
 Step 33: List known Waivers/Exemptions  
 Step 34: List the Contractual Constraints in the Penetration Testing Agreement  
 Step 35: Identify the Reporting Timescales with the Client Organization  
 Step 36: Identify the List of Penetration Testers Required for this Project  
 Step 37: Negotiate per Day/per Hour Fee that you will be Charging for the Penetration Testing Project  
 Step 38: Draft the Timeline for the Penetration Testing Project  
 Step 39: Draft a Quotation for the Services that you'll be Providing to the Client Organization  
 Step 40: Identify how the Final Penetration Testing Report will be Delivered to the Client Organization  
 Step 41: Identify the Reports to be Delivered After Pen Test  
 Step 42: Identify the Information Security Administrator who will be helping you in the Penetration Testing  
 Module 15 Review

## **Module 16 - Information Gathering**

1h 30m

Information Gathering

What is Information Gathering?

Information Gathering Steps

Step 1: Crawl the Website and Mirror the Pages on Your PC

Demo - HTTrack Website Copier

Step 2: Crawl the FTP Site and Mirror the Pages on Your PC

Demo - Wget and Backtrack 4 Live CD

Step 3: Look up Registered Information in the Whois Database

Demo - CentralOps and Domains by Proxy

Demo - Backtrack and Whois

Step 4: List the Products Sold by the Company

Demo - Firecat (Firefox Addons)

Step 5: List the Contact Information, Email Addresses, and Telephone Numbers

Step 6: List the Company's Distributors  
Step 7: List the Company's Partners  
Demo - Email Spider  
Step 8: Search the Internet, Newsgroups, Bulletin Boards, Negative Websites for Information about the Company  
Demo - Maltego  
Step 9: Search for Trade Association Directories  
Step 10: Search for Link Popularity of Company Website  
Demo - Alexa  
Step 11: Compare Price of Product or Service with the Competitor  
Step 12: Find the Geographical Location  
Demo - Shazou  
Use Google Map to Find Geographical Location  
Step 13: Search the Internet Archive Pages about the Company  
Demo - Archive.org  
Step 14: Search Similar or Parallel Domain Name Listings  
Demo - ServerSniff TLDs  
Step 15: Search Job Posting Sites about the Company  
Step 16: Browse Social Network Websites  
Demo - Social Networking  
Step 17: Write Down Key Employees  
Step 18: Investigate Key Persons – Searching in Google, Look up their Resumes and Cross Link Information  
Step 19: List Employee Company and Personal Email Address  
Step 20: Search for Web Pages Posting Patterns and Revision Numbers  
Demo - No Tech Hacking  
Step 21: Email the Employee Disguised as Customer Asking for Quotation  
Step 22: Visit the Company as Inquirer and Extract Privileged Information  
Step 23: Visit the Company Locality  
Step 24: Use Web Investigation Tools to Extract Sensitive Data Targeting the Company  
Step 25: Use Intelius and Conduct Background Check on Company Key Personnel  
Step 26: Search on eBay for Company's Presence  
Step 27: Use the Domain Research Tool to Investigate the Company's Domain  
Step 28: Use the EDGAR Database to Research Company Information  
Step 34: Use GHDB and Search for the Company Name  
Demo - Summary  
Demo - Vmware 64bit Error Fix  
Demo - SEAT  
Demo - Metagoofil Search  
Demo - CORE Impact Email Info Gathering  
Module 16 Review

## **Module 17 - Vulnerability Analysis**

1h 23m

Vulnerability Analysis  
Why Assess?  
Vulnerability Classification  
What is Vulnerability Assessment?  
Demo - Vulnerability Research Resources  
Demo - Nessus 4 Windows Install and Wikto Scan Webgoat  
Types of Vulnerability Assessment  
Demo - Nessus 3 Webgoat Scan BT4  
Demo - Nessus 4 Webgoat Scan  
Demo - GFI LANguard  
How to Conduct a Vulnerability Assessment  
How to Obtain a High Quality Vulnerability Assessment  
Vulnerability Assessment Phases  
Pre-Assessment Phase  
Assessment Phase

Post-Assessment Phase  
Vulnerability Analysis Stages  
Comparing Approaches to Vulnerability Assessment  
Characteristics of a Good Vulnerability Assessment Solution  
Vulnerability Assessment Considerations  
Vulnerability Assessment Reports  
Demo - Nessus 3 BT Exporting NBE Report  
Vulnerability Report Model  
Timeline  
Types of Vulnerability Assessment Tools  
Choosing a Vulnerability Assessment Tool  
Vulnerability Assessment Tools Best Practices  
Vulnerability Assessment Tools  
Demo - Retina Security Scanner  
Other Vulnerability Tools  
Report  
Vulnerability Assessment Reports  
Automated Scanning Server Reports  
Periodic Vulnerability Scanning Report  
Module 17 Review

## **Module 18 - External Penetration Testing**

1h 10m

External Penetration Testing  
Penetration Testing Roadmap  
External Intrusion Test and Analysis  
How is it Done?  
Client Benefits  
External Penetration Testing  
Steps – Conduct External Penetration Testing  
Demo - CORE Impact Network Vulnerability Test  
Demo - Samurai Live CD Intro  
Step 1: Inventory Company's External Infrastructure  
Step 2: Create Topological Map of the Network  
Step 3: Identify the IP Address  
Step 4: Locate the Traffic Route that Goes to the Web Servers  
Step 5/6: Locate TCP/UDP Traffic Path to the Destination  
Step 7: Identify the Physical Location of the Target Servers  
Step 8: Examine the Use IPV6 at the Remote Location  
Step 9: Lookup Domain Registry for IP Information  
Step 10: Find IP Block Information about the Target  
Step 11: Locate the ISP Servicing the Client  
Step 12: List Open Ports  
Open Ports on Web Server  
Step 13: List Closed Ports  
Port Scanning Tools  
Step 14: List Suspicious Ports that are Half Open/Closed  
Step 15: Port Scan Every Port (65,536) on the Target's Network  
Step 16: Use SYN Scan on the Target and See the Response  
Step 17: Use Connect Scan on the Target and See the Response  
Demo - N-stalker Results Webgoat  
Demo - Breaking Access Control Passwords with Xhydra  
Demo - Viewing Website with Telnet  
Demo - Input-injection Attack  
Demo - Fast-track Overview and Install  
Demo - Fast-track Exploits  
Demo - Fast-track Clientside Attacks

## **Module 19 - Internal Network Penetration Testing**

Internal Network Penetration Testing  
Penetration Testing Roadmap  
Internal Testing  
Methods of Internal Testing  
Enumerate Other Machines  
Step 1: Map the Internal Network  
Demo - Spiceworks Inventory  
Step 2: Scan the Network for Live Hosts  
Demo - SNMP Enumerating with BT  
Demo - FireScope MIB Tool  
Step 3: Port Scan Individual Machines  
Step 4: Try to Gain Access Using Known Vulnerabilities  
Demo - SMB NAT Dictionary Attacks  
Demo - Injecting the Abel Service  
Demo - Nslookup DNS Zone Transfer  
Step 5: Attempt to Establish Null Sessions  
Demo - Enumerate Banners  
Demo - Null Session Multiple Tools  
Demo - Null Session Countermeasures  
Step 6: Enumerate Users  
Step 7: Sniff the Network Using Wireshark  
Step 8: Sniff Pop3/FTP/Telnet Passwords  
Step 9: Sniff Email Messages/VoIP Traffic  
Sniffer Tools  
Demo - ARP Poisoning with Cain  
Step 10: Attempt Replay Attacks  
Demo - SSL MITM  
Step 11: Attempt ARP Poisoning  
Step 11a: Attempt Mac Flooding  
Step 12: Conduct a Man-in-the Middle Attack  
Step 13: Attempt DNS Poisoning  
Demo - Cain DNS Spoof  
Step 14: Try a Login to a Console Machine  
Step 15: Boot the PC Using Alternate OS and Steal the SAM File  
Demo - Local Password Reset  
Demo - Backtrack Local XP Password Attack  
Copying Commands in Knoppix  
ERD Commander 2005  
Reset Administrator Password  
Step 16: Attempt to Plant a Software Keylogger to Steal Passwords  
Keyloggers and Spy Software  
Demo - Hardware Keystroke Loggers  
Step 17: Attempt to Plant a Hardware Keylogger to Steal Passwords  
Step 18: Attempt to Plant a Spyware on the Target Machine  
Step 19: Attempt to Plant a Trojan on the Target Machine  
Step 20: Attempt to Create a Backdoor Account on the Target Machine  
Demo - Secure Tunnels and Anonymizer Techniques  
Step 21: Attempt to Bypass Anti-virus Software Installed on the Target Machine  
Demo - Stealth Tools v2 to Hide Viruses and Malware  
Step 22: Attempt to Send Virus Using the Target Machine  
Step 23: Attempt to Plant Rootkits on the Target Machine  
Demo - Dreampakpl Rootkit

Step 24: Hide Sensitive Data on Target Machines  
Demo - Alternate Data Streams  
Step 25: Hide Hacking Tools and Other Data in Target Machines  
Step 26: Use Various Steganography Techniques to Hide Files on Target Machine  
Demo - Steganography  
Step 27: Escalate User Privileges  
Demo - Privilege Escalation  
Step 28: Capture POP3 Traffic  
Step 29: Capture SMTP Traffic  
Step 32: Capture HTTP Traffic  
Step 33: Capture HTTPS Traffic (Even Though it cannot be Decoded)  
Step 34: Capture RDP Traffic  
Step 35: Capture VoIP Traffic  
Demo - Cain VoIP RDP Interception  
Steps 40 and 41  
Step 42: Attempt Session Hijacking on Telnet Traffic  
Steps 43 and 44  
Continue Testing  
CORE Impact - Automated Tool  
Metasploit - Tool  
Canvas – Automated Tool  
Vulnerability Scanning Tools  
Document Everything  
Module 19 Review

## **Module 20 - Router and Switches Penetration Testing**

53m

Router and Switches Penetration Testing  
Demo - Cain and Abel Routing Protocols and ID Networks  
Penetration Testing Roadmap  
Router Testing Issues  
Need for Router Testing  
General Requirements  
Technical Requirements  
Try to Compromise the Router  
Steps for Router Penetration Testing  
Step 1: Identify the Router Hostname  
Step 2: Port Scan the Router  
Step 3: Identify the Router Operating System and its Version  
Steps 4/5: Identify Protocols Running/Testing for Package Leakage at the Router  
Step 6: Test for Router Misconfigurations  
Step 7: Test for VTY/TTY Connections  
The Process to Get Access to the Router  
Step 8: Test for Router Running Modes  
Privilege Mode Attacks  
Step 9: Test for SNMP Capabilities  
SNMP "Community String"  
Step 10: Test for TFTP Connections  
TFTP Testing  
Step 11: Test if Finger is Running on the Router  
Step 12: Test for CDP Protocol Running on the Router  
How to Test CDP Protocol?  
Step 13: Test for NTP Protocol  
Step 14: Test for Access to Router Console Port  
Step 15: Test for Loose and Strict Source Routing  
Steps 16 and 17: Test for IP Spoofing/IP Handling Bugs  
Step 18: Test ARP Attacks



Step 19: Test for Routing Protocol Assessment  
Step 20: RIP Testing  
Step 21: Test for OSPF Protocol  
Step 22: Test BGP Protocol  
Step 23: Test for EIGRP Protocol  
Step 24: Test Router Denial of Service Attacks  
Step 25: Test Router's HTTP Capabilities  
Step 26: Test Through HSRP Attack  
Router Testing Report  
Steps for Testing Switches  
Step 1: Testing Address Cache Size  
Step 2: Data Integrity and Error Checking Test  
Step 3: Testing for Back-to-Back Frame Capacity  
Step 4: Testing for Frame Loss  
Step 5: Testing for Latency  
Step 6: Testing for Throughput  
Step 7: Test for Frame Error Filtering  
Step 8: Fully Meshed Test  
Step 9: Stateless QoS Functional Test  
Step 10: Spanning Tree Network Convergence Performance Test  
Step 11: OSPF Performance Test  
Step 12: Test for VLAN Hopping  
Step 13: Test for MAC Table Flooding  
Step 14: Testing for ARP Attack  
Step 15: Check for VTP Attack  
Module 20 Review

## **Module 21 - Firewall Penetration Testing**

2h 12m

Firewall Penetration Testing  
Penetration Testing Roadmap  
What is a Firewall?  
What Does a Firewall Do?  
Packet Filtering  
What Can't a Firewall Do?  
How Does a Firewall Work?  
Firewall Logging Functionality  
Firewall Policy  
Periodic Review of Information Security Policies  
Firewall Implementation  
Build a Firewall Ruleset  
Maintenance and Management of Firewall  
Types of Firewall  
Demo - Introduction to Vyatta  
Packet Filtering Firewall  
IP Packet Filtering Firewall  
Circuit Level Gateway  
Application Level Firewall  
Stateful Multilayer Inspection Firewall  
Multilayer Inspection Firewall  
Steps for Conducting Firewall Penetration Testing  
Step 1: Locate the Firewall  
Step 2: Traceroute to Identify the Network Range  
Step 3: Port Scan the Firewall  
Step 4: Grab the Banner  
Step 5: Create Custom Packets and Look for Firewall Responses  
Step 6: Test Access Control Enumeration

Step 7: Test to Identify Firewall Architecture  
Step 8: Testing Firewall Policy  
Step 9: Test Firewall Using Firewalking Tool  
Step 10: Test for Port Redirection  
Firewall Identification  
Step 11: Testing the Firewall from Both Sides  
Step 12: Overt Firewall Test from Outside  
Step 13: Test Covert Channels  
Step 14: Covert Firewall Test from Outside  
Step 15: Test HTTP Tunneling  
Step 16: Test Firewall Specific Vulnerabilities  
Demo - Vyatta  
Demo - CORE Impact Targeting Vyatta  
Document Everything  
Module 21 Review

## **Module 22 - IDS Penetration Testing**

47m

IDS Penetration Testing  
Penetration Testing Roadmap  
What is an IDS?  
Demo - IDS Blink and Ossec.net  
Network IDS  
Host-based IDS  
Demo - Blink Personal IPS IDS  
Application-based IDS  
Multi-Layer Intrusion Detection Systems  
Multi-Layer Intrusion Detection System Benefits  
Wireless Intrusion Detection Systems (WIDS)  
IDS Testing Tool - Evasion Gateway  
Common Techniques Used to Evade IDS Systems  
IDS Penetration Testing Steps  
Steps 1/2: Test for Resource Exhaustion/ IDS by Sending ARP Flood  
Steps 3/4: Test the IDS by MAC Spoofing/ IP Spoofing  
Steps 5/6: Test by Sending a Packet to the Broadcast Address/Inconsistent Packets  
Steps 7/8: Test IP Packet Fragmentation/Duplicate Fragments  
Steps 9/10: Test for Overlapping Fragments/Ping of Death  
Steps 11/12: Test for Odd Sized Packets/TTL Evasion  
Steps 13/14: Test by Sending a Packet to Port 0/UDP Checksum  
Steps 15/16: Test for TCP Retransmissions/ TCP Flag Manipulation  
The TCP Header looks like this:  
Step 17: Test TCP Flags  
Steps 18/19: Test the IDS by Sending SYN Floods/ Sequence Number Prediction  
Step 20: Test for Backscatter  
Steps 21/22: Test the IDS with ICMP Packets/ IDS Using Covert Channels  
Step 23: Test Using TCPReplay  
Step 24: Test Using TCPOpera  
Step 26: Test the IDS Using URL Encoding  
Step 27: Test the IDS Using Double Slashes  
Step 28: Test the IDS for Reverse Traversal  
Step 29: Test for Self Reference Directories  
Step 31: Test for IDS Parameter Hiding  
Step 32: Test for HTTP-Misformatting  
Step 33: Test for Long URLs  
Step 34: Test for DoS/Win Directory Syntax  
Step 35: Test for Null Method Processing  
Step 36: Test for Case Sensitivity

Step 37: Test Session Splicing  
Module 22 Review

### **Module 23 - Wireless Network Penetration Testing**

18m

Wireless Network Penetration Testing  
Penetration Testing Roadmap  
Wireless Security Threats  
Wireless Assessment  
Attempt Wireless Monitoring  
Wireless Vulnerability Testing  
Wireless Penetration Testing Steps  
Demo - inSSIDer  
Demo - Wi-Spy Spectrum Analyzer  
Demo - Tips Resources  
Module 23 Review

### **Module 24 - Denial of Service Penetration Testing**

11m

Denial of Service Penetration Testing  
How Does a Denial of Service Attack Work?  
Distributed Denial of Service Attack  
Warning  
How to Conduct Denial of Service Attack Penetration Testing?  
Demo - Ping of Death and Nemesy  
Module 24 Review

### **Module 25 - Password Cracking Penetration Testing**

42m

Password Cracking Penetration Testing  
Passwords  
Common Password Vulnerabilities  
Password Cracking Techniques  
Types of Password Cracking Attacks  
Demo - Cain and Abel Dictionary Attack  
Demo - Cracking your Local XP 64-bit Password with Ophcrack  
Demo - Cracking the Hash Imported into Cain and Abel  
Demo - Rainbow Table Cracking  
Steps in Password Cracking Penetration Testing  
Step 5: Attempt to Guess Passwords  
Demo - Removing a PDF Password  
Module 25 Review

### **Module 26 - Social Engineering Penetration Testing**

29m

Social Engineering Penetration Testing  
What is Social Engineering?  
Requirements of Social Engineering  
Steps in Conducting Social Engineering Penetration Test  
Before you Start  
Dress Like a Businessman  
Step 1: Attempt Social Engineering Techniques Using Phone  
Step 2: Attempt Social Engineering by Vishing  
Step 3: Attempt Social Engineering by Telephone  
Step 4: Attempt Social Engineering Using Email  
Demo - Hotmail Social Engineering  
Step 10: Attempt Social Engineering by Desktop Information  
Step 12: Attempt Social Engineering Using Websites  
Module 26 Review

## **Module 27 - Stolen Laptops, PDAs, and Cell Phones Penetration Testing**

29m

Stolen Laptops, PDAs, and Cell Phones Penetration Testing  
Penetration Testing Roadmap  
Stolen Laptop Testing  
Laptop Theft  
Demo - Darik's Boot and Nuke  
Penetration Testing Steps  
Step 1: Identify Sensitive Data in the Devices  
Look for Personal Information in the Stolen Laptop  
Step 2: Look for Passwords  
Step 3: Look for Company Infrastructure or Finance Documents  
Step 4: Extract the Address Book and Phone Numbers  
Step 5: Extract Schedules and Appointments  
Step 6: Extract Applications Installed on these Devices  
Step 7: Extract Email Messages from these Devices  
Step 8: Gain Access to Server Resources by Using Information you Extracted  
Step 9: Attempt Social Engineering with the Extracted Information  
Check for BIOS Password  
Look into the Encrypted File  
Check Cookies in Web Browsers  
Install Software  
Attempt to Enable Wireless  
Module 27 Review

## **Module 28 - Application Penetration Testing**

1h 8m

Application Penetration Testing  
Application Testing  
What is a Defect?  
Defects vs. Failures  
Defect Ratio  
Requirements and Design Testing  
Web Applications Penetration Testing  
What is a Web Application?  
Demo - Webgoat Hands-on Web Testing  
Demo - Foundstone Overview Hacme Bank Weak Apps  
Web Application Penetration Testing Steps  
Step 1: Fingerprinting the Web Application Environment  
Step 2: Investigate the Output from HEAD and OPTIONS Http Requests  
Step 3: Investigate the Format and Wording of 404/Other Error Pages  
Step 4: Test for Recognized File Types/Extensions/Directories  
Step 5: Examine Source of Available Pages  
Step 6: Manipulate Inputs in Order to Elicit a Scripting Error  
Step 7: Test Inner Working of a Web Application  
Step 8: Test Database Connectivity  
Step 9: Test the Application Code  
Random Numbers vs. Unique Numbers  
Step 10: Testing the Use of GET and POST in Web Application  
Step 11: Test for Parameter-Tampering Attacks on Website  
Step 12: Test for URL Manipulation  
Step 13: Test for Cross Site Scripting  
Step 14: Test for Hidden Fields  
Step 15: Test Cookie Attacks  
Step 16: Test for Buffer Overflows  
Step 17: Test for Bad Data  
Step 18: Test Client-Side Scripting  
Step 19: Test for Known Vulnerabilities

Step 20: Test for Race Conditions  
Step 21: Test with User Protection via Browser Settings  
Step 22: Test for Command Execution Vulnerability  
Step 23: Test for SQL Injection Attacks  
Step 24: Test for Blind SQL Injection  
Step 25: Test for Session Fixation Attack  
Step 26: Test for Session Hijacking  
Step 27: Test for XPath Injection Attack  
Step 28: Test for Server Side Include Injection Attack  
Step 29: Test for Logic Flaws  
Step 30: Test for Binary Attacks  
Step 31: Test for XML Structural  
Step 32: Test for XML Content-level  
Step 33: Test for WS HTTP GET Parameters/REST Attacks  
Step 34: Test for Malicious SOAP Attachments  
Step 35: Test for WS Replay  
Testing Tools  
KSES/ Mieliekoek.pl  
Webgoat  
AppScan  
URL Scan  
Demo - Hacme Bank Scan using N-Stalker  
Demo - Hacme Bank Scan Core Web Testing  
Module 28 Review

## **Module 29 - Physical Security Penetration Testing**

25m

Physical Security Penetration Testing  
Physical Attacks  
Steps in Conducting Physical Security Penetration Testing  
Demo - Bump Key Animation  
Step 1: Map the Possible Entrances  
Step 2: Map the Physical Perimeter  
Step 3: Penetrate Locks Used on the Gates, Doors, and Closets  
Step 4: Observing From a Distance  
Step 5: Penetrate Server Rooms, Cabling, and Wires  
Step 6: Attempt Lock Picking Techniques  
Step 7: Fire Detection Systems  
Step 8: Air Conditioning Systems  
Step 9: Electromagnetic Interception  
Check for the Following  
Step 10: Test if the Company has a Physical Security Policy  
Step 11: Physical Assets  
Step 12: Risk Test  
Step 13: Test if any Valuable Paper Document is Kept at the Facility  
Step 14: Check how these Documents are Protected  
Step 15: Employee Access  
Step 16: Test for Radio Frequency ID (RFID)  
Step 17: Physical Access to Facilities  
Step 18: Documented Process  
Step 19: Test People in the Facility  
Step 20: Who is Authorized?  
Step 21: Test Fire Doors  
Step 22: Check for Active Network Jacks in Meeting Rooms  
Step 23: Check for Active Network Jacks in Company Lobby  
Step 24: Check for Sensitive Information Lying around Meeting Rooms  
Step 25: Check for Receptionist/Guard Leaving Lobby

Step 26: Check for Accessible Printers at the Lobby – Print Test Page  
Step 27: Obtain Phone/Personnel Listing from the Lobby Receptionist  
Step 28: Listen to Employee Conversation in Communal Areas/Cafeteria  
Step 29: Can you Enter the Ceiling Space and Enter Secure Rooms  
Step 30: Check Windows/Doors for Visible Alarm Senses  
Step 31: Check Visible Areas for Sensitive Information  
Step 32: Try to Shoulder Surf Users Logging on  
Step 33: Try to Videotape Users Logging on  
Steps 34 and 35  
Step 36: Intercept and Analyze Guard Communication  
Step 37: Attempt Piggybacking on Guarded Doors  
Step 38: Attempt to Use Fake ID to Gain Access  
Step 39: Test “ After Office Hours” Entry Methods  
Step 40: Identify all Unguarded Entry Points  
Step 43: Attempt to Bypass Sensors Configured on Doors and Windows  
Step 44: Attempt Dumpster Diving Outside the Company Trash Area  
Step 45: Use Binoculars from Outside the Building and See if you can View What is Going On Inside  
Step 46: Use Active High Frequency Voice Sensors to Hear Private Conversation among Company Staff  
Step 47: Dress as a FedEx/UPS Employee and Try to Gain Access to the Building  
Document Everything  
Module 29 Review

## **Module 30 - Database Penetration Testing**

1h 45m

Database Penetration Testing

List of Steps

Demo - NTOSpider

Step 1: Scan for Default Ports Used by the Database  
Step 2: Scan for Non-Default Ports Used by the Database  
Step 3: Identify the Instance Names Used by the Database  
Step 4: Identify the Version Numbers Used by the Database  
Step 5: Attempt to Brute-Force Password Hashes from the Database  
Step 6: Sniff Database Related Traffic on the Local Wire  
Step 7: Microsoft SQL Server Testing  
Step 7.1: Test for Direct Access Interrogation  
Step 7.2: Scan for Microsoft SQL Server Ports ( TCP/UDP 1433)  
Step 7.3: Test for SQL Server Resolution Service (SSRS)  
Step 7.4: Test for Buffer Overflow in pwdencrypt() Function  
Step 7.5: Test for Heap/Stack Buffer Overflow in SSRS  
Step 7.6: Test for Buffer Overflows in Extended Stored Procedures  
Step 7.7: Test for Service Account Registry Key  
Step 7.8: Test the Stored Procedure to Run Web Tasks  
Step 7.9: Exploit SQL Injection Attack  
Step 7.10: Blind SQL Injection  
Demo - SQL Injection with Lee Lawson  
Step 7.11: Google Hacks  
Step 7.12: Attempt Direct-exploit Attacks  
Step 7.13: Try to Retrieve Server Account List  
Step 7.14: Using OSQL Test for Default/Common Passwords  
Step 7.15: Try to Retrieve Sysxlogins Table  
Try to Retrieve Sysxlogins Table Views  
SQL Server System Tables  
Step 7.16: Brute-force SA Account  
Step 8: Oracle Server Testing  
Port Scanning Basic Techniques  
Step 8.2: Check the Status of TNS Listener Running at Oracle Server  
Listener Modes

Step 8.3: Try to Login Using Default Account Passwords  
Step 8.4: Try to Enumerate SIDs  
Step 8.5: Use SQL Plus to Enumerate System Tables  
SQL PLUS: Screenshot  
Step 9: MySQL Server Database Testing  
Step 9.2: Extract the Version of Database being Used  
Step 9.3: Try to Login Using Default/Common Passwords  
Step 9.4: Brute-force Accounts Using Dictionary Attack  
Dictionary Attack Tools  
Dictionary Attack Tool: SQLdict  
Step 9.5: Extract System and User Tables from the Database  
Demo - CORE Impact Webgoat Information Gathering  
Demo - CORE Impact Webgoat SQL Numeric Injection  
Demo - Hacme Bank Testing with Wikto  
Module 30 Review

## **Module 31 - VoIP Penetration Testing**

35m

VoIP Penetration Testing  
Penetration Testing Roadmap  
Vulnerability Assessment  
VoIP Risks and Vulnerabilities  
VoIP Security Threat  
VoIP Penetration Testing Steps  
Demo - VoIP Overview Testing  
Step 1: Test for Eavesdropping  
Step 2: Test for Flooding and Logic Attacks  
Step 3: Test for Denial of Service (DoS) Attack  
Step 4: Test for Call Hijacking & Redirection Attack  
Step 5: Test for ICMP Ping Sweeps  
Step 6: Test for ARP Pings  
Step 7: Test for TCP Ping Scans  
Step 8: Test for SNMP Sweeps  
Step 9: Test for Port Scanning and Service Discovery  
Step 10: Test for Host/Device Identification  
Step 11: Test for Banner Grabbing  
Step 12: Test for SIP User/Extension Enumeration  
Step 13: Test for Automated OPTIONS Scanning with sipsak  
Step 14: Test for Automated REGISTER, INVITE, and OPTIONS Scanning with SIPSCAN against SIP Server  
Step 15: Test for Enumerating TFTP Servers  
Step 16: Test for SNMP Enumeration  
Step 17: Test for Sniffing TFTP Configuration File Transfers  
Step 18: Test for Number Harvesting and Call Pattern Tracking  
VoIP Security Tools  
AuthTool  
VolPong  
Demo - VoIP Interception with Cain and Abel  
VolPong: Screenshots  
Vomit  
PSIPDump  
Netdude  
Netdude: Features  
Oreka  
rtpBreak  
SNScan  
Smap  
Example: Locating Devices

Example: Fingerprinting Devices  
Example: Learning Mode  
SIPScan  
Scanning SIP Phones  
SIPScan: Screenshot  
SIPcrack  
VolPaudit  
Sipsak  
SIPp  
SipBomber  
Spitter  
VoIP Fuzzing Tools  
VoIP Signaling Manipulation Tools  
VoIP Media Manipulation Tools  
Module 31 Review

## **Module 32 - VPN Penetration Testing**

17m

VPN Penetration Testing  
Virtual Private Network (VPN)  
VPN Penetration Testing Steps  
Demo - VPN Testing  
Step 1.1 Scanning: 500 UDP IPSEC  
Step 1.2 Scanning: 1723 TCP PPTP  
Step 1.3 Scanning: 443 TCP/SSL  
Step 1.4 Scanning: nmap -sU -P0 -p 500  
Step 1.5 Scanning: Ipsecscan xxx.xxx.xxx.xxx-255  
Step 2: Fingerprinting  
Step 2.1: Get the IKE Handshake  
Step 2.2: UDP Backoff Fingerprinting  
Step 2.3: Vendor ID Fingerprinting  
Step 2.4: Check for IKE Aggressive Mode  
Step 3.1: PSK Crack: ikeprobe xxx.xxx.xxx.xxx-255  
Step 3.2 PSK Crack: Sniff for Responses with C&A or IKECrack  
Step 4: Test for Default User Accounts  
Step 4.1: Check for Unencrypted Username in a File or the Registry  
Check for Unencrypted Username in a File or the Registry: Screenshot  
Step 4.2: Test for Plain-Text Password  
Step 5: Test for SSL VPN  
Tool: IKE-scan  
IKE-scan: Screenshot  
Tool: IKEProbe  
Tool: VPNmonitor  
Tool: IKECrack  
Module 32 Review

## **Module 33 - War Dialing**

16m

War Dialing  
War Dialing Techniques  
Why Conduct a War Dialing Pentest?  
Pre-Requisites for War Dialing Penetration Testing  
Software Selection for War Dialing  
Guidelines for Configuring Different War Dialing Software  
Recommendations for Establishing an Effective War Dialing Process  
Interpreting War Dialing Results  
List of War Dialing Tools  
Demo - New War Dialing Tool: WarVOX



PhoneSweep  
THC Scan  
ToneLoc  
ModemScan - [www.wardial.net](http://www.wardial.net)  
War Dialing Countermeasures SandTrap Tool  
Module 33 Review

## **Module 34 - Virus and Trojan Detection**

15m

Virus and Trojan Detection  
Steps for Detecting Trojans and Viruses  
Step 1: Use netstat -a to Detect Trojans Connections  
Step 2: Check Windows Task Manager  
Step 3: Check Whether Scanning Programs are Enabled  
Step 3.1: Perform Scanning for Suspicious Running Processes  
Step 3.2: Perform Scanning for Suspicious Registry Entries  
Step 3.3: Check for Suspicious Open Ports  
Step 3.4: Check Whether Suspicious Network Activities are Present  
Step 3.5: Use HijackThis to Scan for Spyware  
Step 4: Check Whether Anti-Virus and Anti-Trojan Programs are Working  
Step 5: Detection of a Boot-Sector Virus  
Spyware Detectors  
Demo - Beast Trojan  
Anti-Trojans  
Anti-Virus Software  
Module 34 Review

## **Module 35 - Log Management Penetration Testing**

10m

Log Management Penetration Testing  
Need for Log Management  
Challenges in Log Management  
Steps for Log Management Penetration Testing  
Step 1: Scan for Log Files  
Step 2: Try to Flood Syslog Servers with Bogus Log Data  
Step 3: Try Malicious Syslog Message Attack (Buffer Overflow)  
Step 4: Perform Man-in-the-Middle Attack  
Step 5: Check Whether the Logs are Encrypted  
Step 6: Check Whether Arbitrary Data Can be Injected Remotely into Microsoft ISA Server Log File  
Step 7: Perform DoS Attack Against Check Point FW-1 Syslog Daemon (Only for CheckPoint Firewall)  
Step 8: Send Syslog Messages Containing Escape Sequences to Syslog Daemon of Check Point FW-1 NG FP3  
Checklist For Secure Log Management  
Module 35 Review

## **Module 36 - File Integrity Checking**

9m

File Integrity Checking  
File Integrity  
Integrity Checking Techniques  
Demo - File Integrity Checkers  
Steps for Checking File Integrity  
Step 1: Check While you Unzip the File  
Step 2: Check for CRC Value Integrity Checking  
CRC Checking in Windows  
Step 3: Check for Hash Value Integrity Checking  
Step 3.1: Get the File and Previously Calculated Hash Value for the File  
Step 3.2: Generate a New Hash Value for the File  
Step 3.3: Match the Old and New Hash Values

## **Module 37 - Bluetooth and Hand Held Device Penetration Testing**

34m

Bluetooth and Hand Held Device Penetration Testing

Jailbreaking an iPhone

Steps for iPhone Penetration Testing

Demo - Jailbreak

Demo - iPod Custom Apps

Step 1: Jailbreak the iPhone

Jailbreaking Using PwnageTool or QuickPwn

Jailbreaking Using QuickPwn

Step-by-Step Guide to Jailbreak iPhone 3G and Preserve Baseband using PwnageTool

Step 2: Unlock the iPhone

Step 4: Hack iPhone using Metasploit

Step 5: Check for Access Point with Same Name and Encryption Type

Step 6: Check Whether Malformed Data Can be Sent to the Device

Step 7: Check Whether Basic Memory Mapping Information Can be Extracted

Vulnerabilities in BlackBerry

Steps for Penetration Testing

Step 1: Try Blackjacking on BlackBerry

Step 2: Try to Attack by Sending Malformed TIFF Image Files

PDA Attacks

Steps for Penetration Testing 2

Step 1: Check Whether Passwords can be Cracked

Step 2: Try for ActiveSync Attacks

Step 3: Check Whether the IR Port is Enabled

Step 4: Check Whether Encrypted Data can be Decrypted

Bluetooth: Introduction

Different Attacks in Bluetooth Devices

Steps for Penetration Testing in Bluetooth

Step 1: Check Whether the PIN Can be Cracked

Step 2: Try to Perform a Blueprinting Attack

Step 3: Check Whether you are able to Extract the SDP Profiles

Step 4: Try Pairing Code Attacks

Step 5: Try a Man-in-the-Middle Attack

Step 6: Try a BlueJacking Attack

Step 7: Try a BTKeylogging Attack

Step 8: Try Bluesmacking -The Ping of Death

Step 9: Try a BlueSnarfing Attack

Try a BlueSnarfing Attack

Step 10: Try a BlueBug Attack

Step 11: Try BlueSpam

Module 37 Review

## **Module 38 - Telecommunication and Broadband Communication Penetration Testing**

22m

Telecommunication and Broadband Communication Penetration Testing

Broadband Communication

Risk in Broadband Communication

Steps for Broadband Communication Penetration Testing

Step 1: Check Whether the Firewall Device is Installed on Network

Step 1.1: Check Whether Personal and Hardware Firewalls are Installed

Step 1.2: Check Whether These Firewalls Prevent Intruders or Detect Any Rogue Software

Step 1.3: Check Whether the Logging is Enabled on the Firewall

Step 1.4: Check Whether the Firewall is in Stealth Mode

Step 2: Check Whether Web Browsers are Properly Configured

Step 2.1: Check Whether the Browser has Default Configuration  
Step 2.2: Check for the Browser Plugins  
Step 2.3: Check Whether Active Code is Enabled  
Step 2.4: Check Whether the Browser Version is Updated  
Step 2.5: Check Whether the Cookies are Enabled  
Step 2.6: Check Whether the Scripting Languages are Enabled  
Step 3: Check for Operating System Configuration Options  
Step 3.1: Check Whether Operating System and Application Software are Updated  
Step 3.2: Check Whether the File and Printer Sharing Option is Enabled  
Step 3.3: Check Whether the Anti-Virus Programs are Enabled  
Step 3.4: Check the Configuration of Anti-Virus Program  
Step 3.5: Check Whether Anti-Spyware is Enabled  
Step 4: Check for Wireless and other Home Networking Technologies  
Step 4.1: Check for VPN Policy Configurations  
Step 4.2: Try for Wiretapping  
Step 4.3: Try to Perform War Driving  
Step 4.4: Check Whether the Wireless Base Station is at Default Configuration  
Step 4.5: Check Whether WEP is Implemented  
Step 4.6: Try to Crack the WEP Key  
Step 4.7: Try to Crack the SSID Password  
Step 4.8: Check Whether the Simple Network Management Protocol (SNMP) is Enabled  
Guidelines for Securing Telecommuting and Home Networking Resources  
Module 38 Review

## **Module 39 - Email Security Penetration Testing**

16m

Email Security Penetration Testing  
Introduction to Email Security  
Pre-Requisite For Email Penetration Testing  
Demo - Hacking Email Accounts  
Steps for Email Penetration Testing  
Step 1: Try to Access Email ID and Password  
Step 2: Check Whether Anti-Phishing Software is Enabled  
Step 3: Check Whether Anti-Spamming Tools are Enabled  
Step 4: Try to Perform Email Bombing  
Step 5: Perform CLSID Extension Vulnerability Test  
Step 6: Perform VBS Attachment Vulnerability Test  
Step 7: Perform Double File Extension Vulnerability Test  
Step 8: Perform Long Filename Vulnerability Test  
Step 9: Perform ActiveX Vulnerability Test  
Step 10: Perform Iframe Remote Vulnerability Test  
Step 11: Perform MIME Header Vulnerability Test  
Step 12: Perform Malformed File Extension Vulnerability Test  
Step 13: Perform Access Exploit Vulnerability Test  
Step 14: Perform Fragmented Message Vulnerability Test  
Step 15: Perform Long Subject Attachment Checking Test  
List of Anti-Phishing Tools  
PhishTank SiteChecker  
PhishTank SiteChecker: Screenshot  
NetCraft  
GFI MailEssentials  
SpooGuard  
List of Anti-Spamming Tools  
AEVITA Stop SPAM Email  
SpamExperts Desktop  
Spytech SpamAgent  
Module 39 Review

## **Module 40 - Security Patches Penetration Testing**

9m

Security Patches Penetration Testing  
Patch Management  
Patch and Vulnerability Group (PVG)  
Countermeasure Testing Steps  
Step 1: Check If Organization has a PVG in Place  
Step 2: Check Whether the Security Environment is Updated  
Step 3: Check Whether Organization uses Automated Patch Management Tools  
Step 4: Check the Last Date of Patching  
Step 5: Check the Patches on Non-Production Systems  
Step 6: Check the Vender Authentication Mechanism  
Step 7: Check Whether Downloaded Patches Contain Viruses  
Step 8: Check for Dependency of New Patches  
Security Checklist for Patch Management  
Patch Management Tools  
Module 40 Review

## **Module 41 - Data Leakage Penetration Testing**

19m

Data Leakage Penetration Testing  
Penetration Testing Roadmap  
Data Leakage  
Data Leakage Statistics  
How Much Security?  
How Data Can be Leaked  
What to Protect  
Steps for Data Leakage  
Step 1: Check Physical Availability of USB Devices  
Step 2: Check Whether USB Drive is Enabled  
Step 3: Try to Enable USB  
Step 4: Check Whether USB Asked for Password  
Step 5: Check Whether Bluetooth is Enabled  
Step 6: Check if the Firewire is Enabled  
Step 7: Check if FTP Ports 21 and 22 are Enabled  
Step 8: Check Whether any Memory Slot is Available and Enabled in Systems  
Step 9: Check Whether Employees are Using Camera Devices within Restricted Areas  
Step 10: Check Whether Systems have Any Camera Driver Installed  
Step 11: Check Whether Anti-Spyware and Anti-Trojans are Enabled  
Step 12: Check Whether Encrypted Data Can be Decrypted  
Step 13: Check if the Internal Hardware Components are Locked  
Step 14: Check Whether Size of Mail and Mail Attachments is Restricted  
Data Privacy and Protection Acts  
Data Protection Tools  
Module 41 Review

## **Module 42 - Penetration Testing Deliverables and Conclusion**

6m

Penetration Testing Deliverables and Conclusion  
Destroy the Report  
Sign-Off Document  
Module 42 Review

## **Module 43 - Penetration Testing Report and Documentation Writing**

20m

Penetration Testing Report and Documentation Writing  
Penetration Testing Report  
Documentation Writing

Table of Contents  
Summary of Execution  
Summary of Weaknesses  
Scope of the Project  
Result Analysis  
Recommendations  
Appendices  
Test Reports on Network  
Summary Recommendations  
Exploited Vulnerabilities  
Payment Card Industry (PCI) Report  
Client-Side Test Reports  
Client-Side Penetration Test Report  
User Report  
Test Reports on Web Applications  
Web Application Testing Report  
Detailed Findings  
Detailed Results  
Strategic and Tactical Directives  
Writing the Final Report  
Creating the Final Report  
Report Format  
Delivery  
Report Retention  
Module 43 Review

#### **Module 44 - Penetration Testing Report Analysis**

13m

Penetration Testing Report Analysis  
Report on Penetration Testing  
Pen-Test Team Meeting  
Research Analysis  
Pen-Test Findings  
Rating Findings  
Demo - Practical Threat Analysis Tool  
Example of Finding- I  
Example of Finding- II  
Analyze

#### **Module 45 - Post Testing Actions**

9m

Post Testing Actions  
Prioritize Recommendations  
Develop Action Plan  
Create Process for Minimizing Misconfiguration Chances  
Updates and Patches  
Capture Lessons Learned and Best Practices  
Create Security Policies  
Conduct Training  
Take Social Engineering Class  
Destroy the Pen-Test Report  
Module 45 Review

#### **Module 46 - Ethics of a Licensed Penetration Tester**

7m

Ethics of a Licensed Penetration Tester  
What Makes a Licensed Penetration Tester?  
Modus Operandi

Evolving as a Licensed Penetration Tester  
Licensed Penetration Tester Dress Code  
LPT Audited Logos  
Example: LPT Audited Logos  
Module 46 Review

**Module 47 - Standards and Compliance**

5m

Standards and Compliance  
Laws  
What is the GLBA?  
HIPAA Compliance  
Sarbanes Oxley Compliance  
FISMA Compliance  
Module 47 Review  
Course Closure

Total Duration: 37h 25m