ECSA™

EC-Council Certified Security Analyst

EC-Council Certified Security Analyst

Course Outline

(Version 9)

Module 01: Security Analysis and Penetration Testing Methodologies

- OPM Government Data Breach Impacted 21.5 Million
- Hackers Steal up to $1 Billion from Banks
- Information Security Breach Survey
- Data Breach Statistics
- Module Objectives
- Security Concerns
  - Greatest Challenges of Security
  - Threat Agents
  - Protect Information
  - Data Security Measures
  - Understand the Risk
  - Assessment Questions
  - Risk Analysis
    - Risk Assessment Answers Seven Questions
    - Risk Assessment Steps
    - Risk Assessment Values
  - Information Security Awareness
- Security Policies

- Security Policy Basics
- Policy Statements
- Types of Security Policies
- An Organization's Security Policies

- Information Security Standards
  - ISO/IEC 27001:2013
  - ISO/IEC 27002:2013
- COBIT
- Information Security Acts
  - Payment Card Industry Data Security Standard (PCI-DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes Oxley Act (SOX)
  - Gramm-Leach-Bliley Act (GLBA)
  - The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
- Information Security Acts and Laws
- Penetration Testing Methodology
  - What Is Penetration Testing?
  - Why Penetration Testing?
  - Penetration Test vs. Vulnerability Test
  - What Should Be Tested?
  - What Makes a Good Penetration Test?
  - Scope of Penetration Testing
  - Blue Teaming/Red Teaming
  - Types of Penetration Testing
    - Black-box Penetration Testing
    - White-box Penetration Testing
    - Grey-box Penetration Testing
  - Penetration Testing Strategies
    - External Penetration Testing
    - Internal Security Assessment

- Penetration Testing Process
- Penetration Testing Phases
  - Pre-Attack Phase
    - Passive Reconnaissance
    - Active Reconnaissance
  - Attack Phase
    - Attack-Phase Activities
      - ✓ Perimeter Testing
      - ✓ Web Application Testing – I
      - ✓ Web Application Testing – II
      - ✓ Web Application Testing – III
      - ✓ Wireless Testing
      - ✓ Application Security Assessment
      - ✓ Network Security Assessment
      - ✓ Wireless/Remote Access Assessment
      - ✓ Database Penetration Testing
      - ✓ File Integrity Checking
      - ✓ Log Management Penetration Testing
      - ✓ Telephony Security Assessment
      - ✓ Data Leakage Penetration Testing
      - ✓ Social Engineering
  - Post-Attack Phase and Activities
- Need for a Methodology
- Penetration Testing Methodologies
- Reliance on Checklists and Templates
- Penetration Testing Strategies
  - Operational Strategies for Security Testing
  - Categorization of the Information System Security
  - Identifying Benefits of Each Test Type
  - Prioritizing Systems for Testing
  - ROI for Penetration Testing

- Determining Cost of Each Test Type
- Penetration Testing Best Practices
- Guidelines for Security Checking
- Penetration Testing Consultants
  - Required Skills Sets of a Penetration Tester
  - Hiring a Penetration Tester
  - Responsibilities of a Penetration Tester
  - Profile of a Good Penetration Tester
  - Why Should the Company Hire You?
  - Companies' Concerns
  - Sample Job and Salary Range for Penetration Testers
  - Penetration Tester Salary Trend
  - What Makes a Licensed Penetration Tester
    - Modus Operandi
    - Preparation
  - Ethics of a Penetration Tester
  - Evolving as a Licensed Penetration Tester
  - Dress Code
  - Communication Skills of a Penetration Tester
  - LPT Audited Logos
    - Example: LPT Audited Logos
- Module Summary

Module 02: TCP/IP Packet Analysis

- Module Objectives
- Module Flow
- Overview of TCP/IP Protocol Stack
  - TCP/IP Model
  - Comparing OSI and TCP/IP
    - Port Numbers
    - Internet Assigned Numbers Authority (IANA)

- Analysis of Application Layer Protocols
  - Dynamic Host Configuration Protocol (DHCP)
    - DHCP Packet Format
    - DHCP Packet Analysis
  - Domain Name System (DNS)
    - DNS Packet Format
    - DNS Packet Analysis
  - DNSSEC
    - DNSSEC Features
    - How DNSSEC Works?
    - Managing DNSSEC for Your Domain Name
    - What is a DS Record?
    - How Does DNSSEC Protect Internet Users?
    - Operation of DNSSEC
- Analysis of Transport Layer Protocols
  - Transmission Control Protocol (TCP)
    - TCP Header Format
    - TCP Services
  - User Datagram Protocol (UDP)
    - UDP Operation
- Analysis of Internet Layer Protocols
  - IP Header
    - Protocol Field
  - What is Internet Protocol v6 (IPv6)?
    - IPv6 Header
    - IPv4/IPv6 Transition Mechanisms
    - IPv6 Security Issues
    - IPv6 Infrastructure Security Issues
    - IPv6 Address Notation
    - IPv6 Address Prefix
    - IPv6 Address Lifetime

- IPv6 Address Structure
  - Address Allocation Structure
  - Hierarchical Routing
- Types of IPv6 Addresses
- IPv4 Compatible IPv6 Address
- IPv4 vs. IPv6

o IPsec

o Internet Control Message Protocol (ICMP)

- Error Reporting and Correction
- ICMP Message Delivery
- Format of an ICMP Message
- Unreachable Networks
- Destination Unreachable Message
- ICMP Echo (Request) and Echo Reply
- 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

o Address Resolution Protocol (ARP)

- ARP Packet Format
- ARP Packet Encapsulation
- ARP Packet Analysis

▪ Analysis of a TCP/IP Connection

o Source and Destination Port Connection

o What Makes Each Connection Unique

o TCP/UDP Connection State Checking Using netstat

o TCP Operation

- Three-Way Handshake
- Flow Control
- Flow Control Mechanism
  - Synchronization
  - Sequencing Numbers
  - Positive Acknowledgment with Retransmission (PAR)
  - Windowing
  - Sliding Windows
    - Sliding Window Example

- TCP/IP in Mobile Networks
  - TCP/IP Concepts in Mobile Networks
  - TCP Options That Can Help Improve Performance
- Module Summary

Module 03: Pre-penetration Testing Steps

- Module Objectives
- Pre-penetration Testing Steps
  - Step 1: Send Preliminary Information Request Document to the Client
  - Step 2: List the Client Organization's Penetration Testing Requirements
  - Step 3: List the Client Organization's Purpose for Penetration Testing
  - Step 4: Obtain a Detailed Proposal of Tests and Services to Be Carried Out
  - Step 5: List the Tests that Will Not Be Carried Out on the Client's Network
  - Step 6: Identify the Type of Testing to Be Carried Out: Black-box or White-box Testing
  - Step 7: Identify the Type of Testing to Be Carried Out: Announced/Unannounced
  - Step 8: List the Servers, Workstations, Desktops, and Network Devices That Need to Be Tested
  - Step 9: Understand Customer Requirements
  - Step 10: Create a Checklist of the Testing Requirements
  - Step 11: Draft the Timeline for the Penetration Testing Project
  - Step 12: Draft a Quote for the Services You Will Provide to the Client's Organization

- Step 13: Identify How the Final Penetration Testing Report Will Be Delivered to the Client's Organization
- Step 14: Identify the Reports to Be Delivered After Pen Test
- Step 15: Identify the Reporting Time Scales with the Client's Organization
- Step 16: Negotiate Per Day/Per Hour Fee That You Will Be Charging for the Penetration Testing Project
  - How Much to Charge?
  - How to Reduce the Cost of Penetration Testing?
- Step 17: Hire a Lawyer Who Can Handle Your Penetration Testing Legal Documents
  - Penetration Testing Contract
- Step 18: Drafting Contracts
  - Sample Penetration Testing Contract
- Step 19: Create Penetration Testing 'Rules of Behavior'
- Step 20: Create Get Out of Jail Free Card
- Step 21: List Permitted Items in Legal Agreement
- Step 22: Create Confidentiality and Non-Disclosure Agreements (NDAs) Clauses
- Step 23: Define Liability Issues
- Step 24: Define Negligence Claim
- Step 25: Define Limitations of the Contract
- Step 26: Get the Engagement Letter Vetted with Your Lawyer
- Step 27: Allocate a Budget for the Penetration Testing Project (X Amount of Dollars)
- Step 28: Obtain (if Possible) Liability Insurance from a Local Insurance Firm
- Step 29: Identify Who Will Be Leading the Penetration Testing Project (Chief Penetration Tester)
- Step 30: Prepare a Tiger Team
  - Skills and Knowledge Required
  - Internal Employees
  - Penetration Testing Teams
  - Tiger Team
  - Questions to Ask Before Hiring Consultants for the Tiger Team
- Step 31: Review the Signed Engagement Letter (EL)
- Step 32: Create Engagement Log

- Step 33: Conduct Initial Teleconference with Target point-of-contact (TPOC)
  - Meeting with the Client
  - Kickoff Meeting
- Step 34: Conduct Independence, Check of the Team Members
- Step 35: Prepare a Non-Disclosure Agreement (NDA) and Have the Client Sign It
- Step 36: Create Rules of Engagement (ROE)
  - Statement of Work (SOW)
  - Scope of ROE
  - Points of Contact Template
  - Steps for Framing ROE
    - Step 36.1: Review Engagement Letter
    - Step 36.2: Prepare the Rules of Engagement That Lists the Company's Core Competencies/Limitations/Time Scales
    - Step 36.3: Identify the Network Topology in Which the Test Would Be Carried Out
    - Step 36.4: List the Security Tools That You Will Be Using for the Penetration Testing Project
    - Step 36.5: List the Hardware and Software Requirements for the Penetration Testing Project
    - Step 36.6: Identify the Client's IT Security Admin Who Will Be Helping You in the Pen Testing (if Possible)
    - Step 36.7: List the Contacts at the Client Organization Who Will Be in Charge of the Pen Testing Project
    - Step 36.8: Obtain the Contact Details of the Key Person at the Client's Company During an Emergency
    - Step 36.9: List the Points of Contact During an Emergency
    - Step 36.10: List the Known Waivers/Exemptions
    - Step 36.11: List the Contractual Constraints in the Penetration Testing Agreement
  - Clauses in ROE
  - Sample Rules of Engagement Document
  - Rules of Engagement Template (Sample)
- Step 37: Prepare Test Plan

- Test Plan
- Content of a Test Plan
- Building a Penetration Test Plan
- Test Plan Identifier
- Work Breakdown Structure or Task List
- Penetration Testing Schedule
- Penetration Testing Project Scheduling Tools: Project Professional 2013
- Penetration Testing Project Scheduling Tools
- Test Plan Checklist
- Penetration Testing Hardware/Software Requirements
- Assign Resources

o Step 38: Send Internal Control Questionnaires (ICQ) to the Client (Provided By Client (PBC) Information)

o Step 39: Request Previous Penetration Testing/Vulnerability Assessment Reports (If Possible)

o Step 40: Create Data Use Agreement (DUA) (if required)

o Step 41: Conduct Working Teleconference

o Step 42: Send the Final Engagement Control Documents to Client for Signature

o Step 43: Obtain Penetration Testing Permission from the Company's Stakeholders

o Step 44: Obtain Special Permission if Required from the Local Law Enforcement Agency

o Step 45: Obtain Temporary Identification Cards from the Client for the Team Members Involved in the Process

o Step 46: Identify the Office Space/Location Where Your Team Will Work during This Project

o Step 47: Gather Information about the Client Organization's History and Background

o Step 48: Visit and Become Familiar with the Client Organization's Premises and Environment

o Step 49: Identify the Local Equipment Required for Pen Test

o Step 50: Identify the Local Human Resources Required for the Pen Test

o Step 51: Conduct Mission Briefing

▪ Module Summary

Module 04: Information Gathering Methodology

- Module Objectives
- What is Information Gathering?
- Information Gathering Terminologies
- Information Gathering Steps
  - Step 1: Find the Company's URL
  - Step 2: Locate the Internal URLs
  - Step 3: Find the Geographical Location of a Company
  - Step 4: List the Contact Information, Email Addresses, and Telephone Numbers
    - Search Telephone Numbers Using http://www.thephonebook.bt.com
  - Step 5: List Key Persons of the Company
  - Step 6: Search the Internet, Newsgroups, Bulletin Boards, and Negative Websites for Information about the Company
  - Step 7: Use People Search Online Services to Collect the Information
    - People Search Online Services
  - Step 8: Browse Social Network Websites to Find the Information about the Company and Employees
  - Step 9: Use Google/ Yahoo! Finance to Search for Press Releases Issued by the Company
  - Step 10: Monitor the Company's Website for Information
  - Step 11: Search for Link Popularity of the Company's Website
    - Link Popularity Search Online Services
  - Step 12: Search for Company's Job Postings through Job Sites
    - Example of Company's Job Postings
  - Step 13: Monitor Target Using Alerts
  - Step 14: Collect Company's Information through Groups, Forums, and Blogs
  - Step 15: Gather Competitive Intelligence
    - Competitive Intelligence
    - Competitive Intelligence Tools
    - Competitive Intelligence Consulting Companies
  - Step 16: Search for Trade Association Directories
  - Step 17: List the Products/Services Sold by the Company

- Search on Ebay for the Company's Presence

- Step 18: List the Company's Partners and Distributors
- Step 19: Compare Price of Product or Service with Competitor
  - Price Comparison Services
- Step 20: Search for Web Pages Posting Patterns and Revision Numbers
- Step 21: Use Web Investigation Tools to Extract Sensitive Data Targeting the Company
- Step 22: Look Up Registered Information in Whois Database
  - Whois Lookup Result
  - Whois Lookup Tools
- Step 23: Extract DNS Information using Domain Research Tools
  - DNS Interrogation Tools
  - Domain Research Tool (DRT)
- Step 24: Search Similar or Parallel Domain Name Listings
- Step 25: Retrieve the DNS Record of the Organization from Publicly Available Servers
  - DNS Interrogation Tools
- Step 26: Locate the Network Range
  - Traceroute Analysis
  - Traceroute Tools
- Step 27: Search the Internet Archive Pages about the Company
- Step 28: Monitor Web Updates Using WebSite-Watcher
- Step 29: Crawl the Website and Mirror the Pages on Your PC
  - Website Mirroring Tools
- Step 30: Crawl the FTP Site and Mirror the Pages on Your PC
  - FTP Site Mirroring Tool: WebCopier Pro
- Step 31: Track Email Communications
  - Email Tracking Tool: eMailTrackerPro
  - Email Tracking Tools
- Step 32: Search for the Company's Internal Resources using Google Hacking Database
  - Google Hacking Database

- Step 33: Perform Social Engineering
  - Steps to Perform Social Engineering
    - Step 33.1: Visit the Company as Inquirer and Extract Privileged Information
    - Step 33.2: Visit the Company Locality
    - Step 33.3: List Employees of the Company and Personal Email Addresses
    - Step 33.4: Email the Employee Disguised as Customer Asking for Quotation
    - Step 33.5: Attempt Social Engineering Using the Phone (Vishing)
      - ✓ Example of Social Engineering Using the Phone
    - Step 33.6: Attempt Social Engineering Using Email
      - ✓ Example of Social Engineering Using Email
    - Step 33.7: Attempt Social Engineering by Dumpster Diving
    - Step 33.8: Attempt Social Engineering by Shoulder Surfing
    - Step 33.9: Attempt Social Engineering by Eavesdropping
    - Step 33.10: Attempt Social Engineering Using Phishing
      - ✓ Phishing Example
    - Step 33.11: Attempt Identity Theft
      - ✓ Steps for Identity Theft
    - Step 33.12: Identify "Disgruntled Employees" and Engage in Conversation to Extract Sensitive Information
- Step 34: Document Everything

- Footprinting Tools
  - Maltego
  - FOCA
- Module Summary

Module 05: Vulnerability Analysis

- Module Objectives
- What Is Vulnerability Assessment?
  - Why Assessment?
  - Vulnerability Classification
  - Types of Vulnerability Assessment

- Vulnerability-Management Life Cycle
  - Pre-Assessment Phase
    - Creating a Baseline
    - Vulnerability Assessment
  - Post Assessment Phase
- Comparing Approaches to Vulnerability Assessment
- Working of Vulnerability Scanning Solutions
- Characteristics of a Good Vulnerability Assessment Solution
- Vulnerability Assessment Assignment Considerations
- Timeline
- Types of Vulnerability Assessment Tools
  - Choosing a Vulnerability Assessment Tool
  - Criteria for Choosing a Vulnerability Assessment Tool
  - Best Practices for Selecting Vulnerability Assessment Tools
- Vulnerability Assessment Tools
  - QualysGuard Vulnerability Management
  - Retina Network Security Scanner
  - GFI LANGuard
  - SAINT Vulnerability Scanner
  - Microsoft Baseline Security Analyzer (MBSA)
  - Nessus
  - AVDS - Automated Vulnerability Detection System
  - Vulnerability Assessment Tools
- Vulnerability Assessment Reports
  - Sample Vulnerability Assessment Report
  - Vulnerability Report Model
  - Sample Security Vulnerability Report – 1
  - Sample Security Vulnerability Report – 2
  - Sample Security Vulnerability Report – 3
  - Vulnerability Analysis Report Template

- Module Summary

Module 06: External Network Penetration Testing Methodology

- Module Objectives
- External Intrusion Test and Analysis
- Why Is It Done?
- Client Benefits
- External Penetration Testing
- Steps for Conducting External Penetration Testing
  - Step 1: Perform Information Gathering
  - Step 2: Create Topological Map of the Network
  - Step 3: Locate TCP/UDP Traffic Path to the Destination
    - Proxy Tools
  - Step 4: Identify the Physical Location of the Target Servers
  - Step 5: Locate the ISP Servicing the Client
  - Step 6: Examine the Use of IPv6 at the Remote Location
  - Step 7: Examine the System Uptime of Target Server
  - Step 8: Examine the Patches Applied to the Target Operating System
  - Step 9: Checking for Live Systems - ICMP Scanning
    - ICMP Scanning Tools
  - Step 10: Port Scan Every Port (65,536) on the Target's Network
    - Common Ports List
  - Step 11: List Open and Closed Ports
    - Scanning Tool: NetScan Tools Pro
    - Scanning Tools
  - Step 12: Use Connect Scan (Full Open Scan) on the Target and See the Response
  - Step 13: Use SYN Scan (Half-open Scan) on the Target and See the Response
  - Step 14: Use XMAS Scan on the Target and See the Response
  - Step 15: Use FIN Scan on the Target and See the Response
  - Step 16: Use NULL Scan on the Target and See the Response
  - Step 17: Use ACK Flag Probe Scan on the Target and See the Response
  - Step 18: Use UDP Scan on the Target and See the Response

- Step 19: Use Fragmentation Scanning and Examine the Response
- Step 20: OS Fingerprint Target Servers
- Step 21: Grab the Banner of HTTP Servers
- Step 22: Grab the Banner of SMTP Servers
- Step 23: Grab the Banner of POP3 Servers
- Step 24: Grab the Banner of FTP Servers
- Step 25: Firewalk on the Router's Gateway and Guess the Access List
- Step 26: Examine TCP Sequence Number Prediction
- Step 27: Examine IPID Sequence Number Prediction
  - Hping3 IPID Example
- Step 28: Examine the Use of Standard and Non-Standard Protocols
- Step 29: Download Applications from the Company's Website and Reverse Engineer the Binary Code
- Step 30: List Programming Languages Used and Application Software to Create Various Programs from the Target Server
- Step 31: Look for Error and Custom Web Pages
- Step 32: Guess Different Subdomain Names and Analyze Responses
- Step 33: Examine the Session Variables
- Step 34: Perform Various Attacks on Web Applications
- Step 35: Check for Directory Consistency and Page Naming Syntax of the Web Pages
- Step 36: Look for Sensitive Information in Web Page Source Code
- Step 37: Record and Replay the Traffic to the Target Web Server and Note the Response
- Step 38: Perform SQL Injection
- Step 39: Examine Server Side Includes (SSI)
- Step 40: Examine E-commerce and Payment Gateways Handled by the Web Server
- Step 41: Examine Welcome Messages, Error Messages, and Debug Messages
- Step 42: Probe the Service by SMTP Mail Bouncing
- Step 43: Identify the Web Extensions Used at the Server
- Step 44: Try to Use HTTPS Tunnel to Encapsulate Traffic
- Step 45: Port Scan DNS Servers (TCP/UDP 53)
- Step 46: Port Scan TFTP Servers (Port 69)

- Step 47: Test for NTP Ports (Port 123)
- Step 48: Test for SNMP Ports (Port 161)
- Step 49: Test for Telnet Ports (Port 23)
- Step 50: Test for LDAP Ports (Port 389)
- Step 51: Test for NetBIOS Ports (Ports 135-139, 445)
- Step 52: Test for SQL Server Ports (Port 1433, 1434)
- Step 53: Test for Citrix Ports (Port 1495)
- Step 54: Test for Oracle Ports (Port 1521)
- Step 55: Test for NFS Ports (Port 2049)
- Step 56: Test for Compaq, HP Inside Manager Ports (Port 2301, 2381)
- Step 57: Test for Remote Desktop Ports (Port 3389)
- Step 58: Test for Sybase Ports (Port 5000)
- Step 59: Test for SIP Ports (Port 5060)
- Step 60: Test for VNC Ports (Port 5900/5800)
- Step 61: Test for X11 Ports (Port 6000)
- Step 62: Test for Jet Direct Ports (Port 9100)
- Step 63: Port Scan FTP Data (Port 20)
- Step 64: Port Scan Web Servers (Port 80)
- Step 65: Port Scan SSL Servers (Port 443)
- Step 66: Port Scan Kerberos-Active Directory (Port TCP/UDP 88)
- Step 67: Port Scan SSH Servers (Port 22)
- Step 68: Perform Vulnerability Scanning
- Step 69: Document Everything

- Recommendations to Protect Your System from External Threats
- Module Summary

Module 07: Internal Network Penetration Testing Methodology

- Module Objectives
- Internal Network Penetration Testing
- Why Internal Network Penetration Testing?
- Internal Network

- Steps for Internal Network Penetration Testing
  - Step 1: Perform Information Gathering
  - Step 2: Map the Internal Network
  - Step 3: Scan the Network for Live Hosts
    - Network Scanning Tools
  - Step 4: Port Scan the Individual Machines
  - Step 5: Try to Gain Access Using Known Vulnerabilities
  - Step 6: Attempt to Establish Null Sessions
  - Step 7: Perform Enumeration
    - Enumeration Tools
    - Enumeration Techniques and Tools
  - Step 8: Sniff the Network
    - Sniffing Tool: Wireshark
    - Sniffing Tools
  - Step 9: Check for ICMP Responses from Broadcast Address
  - Step 10: Attempt Replay Attacks
  - Step 11: Attempt ARP Poisoning
    - ARP Poisoning Tools
  - Step 12: Attempt Mac Flooding
  - Step 13: Conduct a Man-in-the-Middle Attack
  - Step 14: Attempt DNS Poisoning
    - Example of a Normal Host File Under DNS Poisoning Attack
  - Step 15: Try to Log into a Console Machine
  - Step 16: Boot the PC Using Alternate OS and Steal the SAM File
  - Step 17: Reset the Local Administrator or other User Account Passwords
  - Step 18: Attempt to Plant a Software Keylogger to Steal Passwords
    - Keyloggers
  - Step 19: Attempt to Plant a Hardware Keylogger to Steal Passwords
  - Step 20: Attempt to Plant Spyware on the Target Machine
    - Spyware Examples
  - Step 21: Attempt to Plant a Trojan on the Target Machine

- Step 22: Attempt to Create a Backdoor Account on the Target Machine
- Step 23: Attempt to Bypass Antivirus Software Installed on the Target Machine
- Step 24: Attempt to Send a Virus Using the Target Machine
- Step 25: Attempt to Plant Rootkits on the Target Machine
- Step 26: Hide Sensitive Data on Target Machines
  - Data Hiding Tool: WinMend Folder Hidden
- Step 27: Hide Hacking Tools and Other Data on Target Machines
- Step 28: Use Various Steganography Techniques to Hide Files on Target Machines
  - Whitespace Steganography Tool: SNOW
- Step 29: Escalate User Privileges
- Step 30: Run Wireshark with the Filter ip.src==[ip_address]
- Step 31: Run Wireshark with the Filter ip.dst==[ip_address]
- Step 32: Run Wireshark with Protocol-based Filters
- Step 33: Run Wireshark with the Filter tcp.port==[port_no]
- Step 34: Capture POP3 Traffic
- Step 35: Capture SMTP Traffic
- Step 36: Capture IMAP Email Traffic
- Step 37: Capture the Communications between FTP Client and FTP Server
- Step 38: Capture HTTP Traffic
- Step 39: Capture HTTPS Traffic (Even Though It Cannot Be Decoded)
- Step 40: Capture RDP Traffic
- Step 41: Capture VoIP Traffic
- Step 42: Spoof the MAC address
- Step 43: Poison the Victim's IE Proxy Server
- Step 44: Attempt Session Hijacking on Telnet Traffic
- Step 45: Attempt Session Hijacking on FTP Traffic
- Step 46: Attempt Session Hijacking on HTTP Traffic

- Automated Internal Network Penetration Testing Tools
  - Metasploit
  - Kali Linux
  - Immunity CANVAS

- Recommendations for Internal Network Penetration Testing
- Module Summary

Module 08: Firewall Penetration Testing Methodology

- Module Objectives
- What is a Firewall?
  - Hardware Firewall
  - Software Firewall
- What Does a Firewall Do?
- What Can't a Firewall Do?
- Types of Firewalls
- Packet Filtering
- Firewall Policy
  - Periodic Review of Information Security Policies
- Firewall Implementation
- Build a Firewall Ruleset
- Maintenance and Management of Firewall
  - Firewall Management and Testing Tool: Firewall Builder
  - Firewall Management and Testing Tools
- Steps for Conducting Firewall Penetration Testing
  - Step 1: Find the Information about Target
  - Step 2: Perform WHOIS Lookup and Locate the Network Range
  - Step 3: Perform Port Scanning
  - Step 4: Locate the Firewall Using Packet Crafter
  - Step 5: Locate the Firewall by Conducting Traceroute
    - Traceroute Tools
  - Step 6: Grab the Banner
  - Step 7: Create Custom Packets and Look for Firewall Responses
  - Step 8: Test Access Control Enumeration
  - Step 9: Identify the Firewall Architecture
  - Step 10: Test the Firewall Policy

- Step 11: Test the Firewall Using a Firewalking Tool
  - Firewall Ruleset Mapping
- Step 12: Test for Port Redirection
  - Firewall Identification
- Step 13: Test the Firewall from Both Sides
- Step 14: Overt Firewall Test from Outside
- Step 15: Test Covert Channels
- Step 16: Covert Firewall Test from Outside
- Step 17: Try to Bypass Firewall Using IP Address Spoofing
- Step 18: Try to Bypass Firewall Using Tiny Fragments
- Step 19: Try to Bypass Firewall Using IP Address in Place of URL
- Step 20: Try to Bypass Firewall Using Anonymous Website Surfing Sites
- Step 21: Try to Bypass Firewall Using Proxy Server
- Step 22: Try to Bypass Firewall Using Source Routing
- Step 23: Test HTTP Tunneling Method
- Step 24: Test ICMP Tunneling Method
- Step 25: Test ACK Tunneling Method
- Step 26: Test SSH Tunneling Method
- Step 27: Try to Bypass Firewall through MITM Attack
- Step 28: Try to Bypass Firewall Using Malicious Contents
- Step 29: Test Firewall-Specific Vulnerabilities
- Step 30: Document Everything

- Best Practices for Firewall Configuration
- Module Summary

Module 09: IDS Penetration Testing

- Penetration Testing Methodology
- Module Objectives
- Introduction to Intrusion Detection System (IDS)
- Types of Intrusion Detection Systems
  - Application-based IDS

- Multi-Layer Intrusion Detection Systems (mIDS)
- Multi-Layer Intrusion Detection System Benefits
- Wireless Intrusion Detection Systems (WIDSs)

- Why IDS Penetration Testing?
- Common Techniques Used to Evade IDS Systems
- IDS Penetration Testing Steps
  - Step 1: Find the Information about Target
    - Packet Sniffing Tools
  - Step 2: Test for Resource Exhaustion
    - Network Traffic Generator Tools
  - Step 3: Test the IDS by Sending ARP Flood
  - Step 4: Test the IDS by MAC Spoofing
  - Step 5: Test the IDS by IP Spoofing
  - Step 6: Test the IDS by Sending SYN Floods
  - Step 7: Test the IDS by Editing and Replaying Captured Network Traffic
  - Step 8: Test the IDS for Denial-of-Service (DoS) Attack
    - Denial-of-Service (DoS) Attack Tools
  - Step 9: Try to Bypass IDS Using Anonymous Website Surfing Sites and Proxy Server
  - Step 10: Try to Bypass IDS Using Botnet
  - Step 11: Test the Insertion on IDS
  - Step 12: Test the IDS by Sending a Packet to the Broadcast Address
  - Step 13: Test the IDS by Sending Inconsistent Packets
  - Step 14: Test the IDS for IP Packet Fragmentation
    - Packet Fragmentation
  - Step 15: Test the IDS for Overlapping Fragments
  - Step 16: Test the IDS for Ping of Death
  - Step 17: Test the IDS for Unicode Evasion
  - Step 18: Test the IDS for Polymorphic Shellcode
  - Step 19: Check for Obfuscation
  - Step 20: Check for False Positive Generation
  - Step 21: Test the IDS Using URL Encoding

- Step 22: Test the IDS Using Double Slashes
- Step 23: Test for TTL Evasion
- Step 24: Test the IDS by Sending a Packet to Port 0
- Step 25: Test for UDP Checksum
- Step 26: Test for TCP Retransmissions
- Step 27: Test the IDS by TCP Flag Manipulation
  - TCP Flags
- Step 28: Test Initial Sequence Number Prediction
- Step 29: Test for Backscatter
- Step 30: Test the IDS Using Covert Channels
- Step 31: Test the IDS Using Method Matching
- Step 32: Test the IDS for Reverse Traversal
- Step 33: Test for Self-Referencing Directories
- Step 34: Test for Premature Request Ending
- Step 35: Test for IDS Parameter Hiding
- Step 36: Test for HTTP Misformatting
- Step 37: Test for Long URLs
- Step 38: Test for Win Directory Syntax
- Step 39: Test for Null Method Processing
- Step 40: Test for Case Sensitivity
- Step 41: Try to Bypass IDS using Compressed Media Files
- Step 42: Test Session Splicing
- Step 43: Try to Bypass Invalid RST Packets through IDS
- Step 44: Document Everything

- IDS Evasion Tool: Traffic IQ Professional
- IDS Evasion Tools
- Intrusion Detection System: Snort
- Intrusion Detection Tools
- IDS Countermeasures
- Module Summary

Module 10: Web Application Penetration Testing Methodology

- Module Objectives
- Why Web Application are So Critical
- Web Application Penetration Testing/Security Testing
  - Typical Web Application Components
- Web App Pen Testing Methodology
  - Web App Pen Testing Steps
    - Step 1: Fingerprinting Web Application Environment
      - Step 1.1: Perform Basic Website Footprinting, using Netcraft
      - Step 1.2: Manually Browse the Target Website
      - Step 1.3: Analyze the HTML Source Code
      - Step 1.4: Check the HTTP and HTML Processing by the Browser
        - ✓ HTTP and HTML Analysis Tools
      - Step 1.5: Perform Web Spidering
      - Step 1.6: Perform Search Engine Reconnaissance
      - Step 1.7: Determine Whether Target Is Load Balanced
      - Step 1.8: Determine Whether the Target is Protected using Web Application Firewall (WAF)
      - Step 1.9: Perform Banner Grabbing to Identify the Target Web Server
      - Step 1.10: Perform Web Server Fingerprinting using httprint
      - Step 1.11: Perform Advanced Web Server Fingerprinting using HTTPRecon
      - Step 1.12: Perform Service Discovery
      - Step 1.13: Identify Server-side Technologies
        - ✓ Server-side Technologies and Extensions
      - Step 1.14: Identify the Sitemap of Target Website
      - Step 1.15: Identify the Restricted Directories of Target Website
      - Step 1.16: Identify Server-side Functionality
      - Step 1.17: Investigate the Output from HEAD and OPTIONS HTTP Requests
      - Step 1.18: Investigate the Format and Wording of 404/Other Error Pages
      - Step 1.19: Test for Recognized File Types/Extensions/Directories
      - Step 1.20: Test for Hidden Fields

- Step 1.21: Discover Hidden Content of the Target Website
- Step 1.22: Test for/Discover Default Content
- Step 1.23: Test for Directory Traversal
- Step 1.24: Test for Debug Parameters
- Step 1.25: Test for XSS Vulnerabilities

- Step 2: Testing for Web Server Vulnerabilities
  - Step 2.1: Test for Default Credentials
  - Step 2.2: Test for Dangerous HTTP Methods
  - Step 2.3: Test for Proxy Functionality
  - Step 2.4: Test for Virtual Hosting Misconfiguration
  - Step 2.5: Test for Web Server Software Bugs
    - ✓ Web Vulnerability Scanners
  - Step 2.6: Test for Server-side Include Injection Attack
- Step 3:Testing Configuration Management
  - Step 3.1: Test the Inner Workings of a Web Application
  - Step 3.2: Test the Database Connectivity
  - Step 3.3: Test the Application Code
  - Step 3.4: Test the Use of GET and POST in the Web Application
  - Step 3.5: Test for Improper Error Handling
  - Step 3.6: Identify Functionality
  - Step 3.7: Identify Entry Points for User Input
  - Step 3.8: Test for XSS
  - Step 3.9: Test for Parameter/Form Tampering
  - Step 3.10: Test for URL Manipulation
  - Step 3.11: Test for Hidden Field Manipulation Attack
    - ✓ Map the Attack Surface
  - Step 3.12: Perform Denial-of-Service Attack
  - Step 3.13: Check for Insufficient Transport Layer Protection
  - Step 3.14: Check for Weak SSL Ciphers
  - Step 3.15: Check for Insecure Cryptographic Storage
  - Step 3.16: Check for Unvalidated Redirects and Forwards

- Step 4: Testing for Client-side Vulnerabilities
  - Step 4.1: Test for Bad Data
  - Step 4.2: Test Transmission of Data via the Client
  - Step 4.3: Test Client-side Controls over User Input
  - Step 4.4: Identify Client-side Scripting
  - Step 4.5: Test Thick-client Components
  - Step 4.6: Test ActiveX Controls
  - Step 4.7: Test Shockwave Flash Objects
  - Step 4.8: Check for Frame Injection
  - Step 4.9: Test with User Protection via Browser Settings
- Step 5: Testing the Authentication Mechanism
  - Step 5.1: Understand the Mechanism
  - Step 5.2: Test Password Quality
  - Step 5.3: Test for Username Enumeration
  - Step 5.4: Test Resilience to Password Guessing
  - Step 5.5: Test Any Account Recovery Function and Remember Me Function
  - Step 5.6: Perform Password Brute-forcing
  - Step 5.7: Perform Session ID Prediction/Brute-forcing
  - Step 5.8: Perform Authorization Attack
  - Step 5.9: Perform HTTP Request Tampering
  - Step 5.10: Perform Authorization Attack – Cookie Parameter Tampering
- Step 6: Testing Session Management Mechanism
  - Step 6.1: Understand the Mechanism
  - Step 6.2: Test Tokens for Meaning
  - Step 6.3: Session Token Prediction (Test Tokens for Predictability)
    - ✓ Session Token Sniffing
  - Step 6.4: Check for Insecure Transmission of Tokens
  - Step 6.5: Check for Disclosure of Tokens in Logs
  - Step 6.6: Check Mapping of Tokens to Sessions
  - Step 6.7: Test Session Termination
  - Step 6.8: Test for Session Fixation Attack

- Step 6.9: Test for Session Hijacking
- Step 6.10: Check for XSRF
- Step 6.11: Check Cookie Scope
- Step 6.12: Test Cookie Attacks

- Step 07: Testing Authorization Controls
  - Step 7.1: Understand the Access Control Requirements
  - Step 7.2: Testing with Multiple Accounts
  - Step 7.3: Testing with Limited Access
  - Step 7.4: Test for Insecure Access Control Methods
  - Step 7.5: Test Segregation in Shared Infrastructures
  - Step 7.6: Test Segregation between ASP-hosted Applications

- Connection String Injection
  - Connection String Parameter Pollution (CSPP) Attacks
  - Connection Pool DoS

- Step 08: Testing the Data Validation Mechanism
  - Step 8.1: Test for LDAP Injection
- Step 09: Testing Web Services
  - ✓ Web Services Footprinting Attack
  - ✓ Web Services Probing Attacks
  - Step 9.1: Test for XML Structure
  - Step 9.2: Test for XML Content-level
    - ✓ Web Services XML Poisoning
  - Step 9.3: Test for WS HTTP GET Parameters/REST Attacks
  - Step 9.4: Test for Suspicious SOAP Attachments
    - ✓ SOAP Injection
  - Step 9.5: Test for XPath Injection Attack
  - Step 9.6: Test for WS Replay
- Step 10: Testing for Logic Flaws
  - Step 10.1: Identify the Key Attack Surface
  - Step 10.2: Test for Logic Flaws
  - Step 10.3: Test Multistage Processes

- Step 10.4: Test Handling of Incomplete Input
- Step 10.5: Test Trust Boundaries
- Step 10.6: Test Transaction Logic

- Module Summary

Module 11: SQL Penetration Testing Methodology

- Module Objectives
- An Overview to SQL Injection
  - Automated vs. Manual SQL Injection Penetration Testing
  - Types of SQL Injection
  - SQL Injection Penetration Methodology
  - SQL Injection Pen-Testing Characters
  - SQL Injection Pen-Testing Cheat Sheet
  - SQL Injection Penetration-Testing Steps
    - Step 01: Identify the Injection Points
    - Step 02: Identify the SQL Injectable Entry points in the HTTP Request
      - Entry Points in HTTP Requests
    - Step 03: Identify Injection Points using SQLMAP
    - Step 04: Perform Database Fingerprinting
    - Step 05: Identify Databases Using SQLMAP
    - Step 06: Detect SQL Injection Vulnerabilities by Manipulating a Parameter
    - Step 07: Detect SQL Injection Vulnerabilities Using Function Testing
    - Step 08: Perform Fuzz Testing to Detect SQL Injection Vulnerabilities
    - Step 09: Detect SQL Injection Vulnerabilities Using Automated Web-App Vulnerability Scanners
      - SQL Injection Detection Tool: IBM Security AppScan
      - SQL Injection Detection Tools
    - Step 10: Detect SQL Injection Vulnerabilities Using Source-Code Review
    - Step 11: Determine the Database Schema Using Error-Based SQL Injection
    - Step 12: Determine the Database Schema Using UNION-Based SQL Injection
    - Step 13: Determine the Database Schema Using Blind SQL Injection

- Step 14: Determine Privileges, DB Structure, and Column Names
- Step 15: Identifying Tables Using SQLMAP
- Step 16: Identifying Columns Using SQLMAP
- Step 17: Extract Data Using Blind SQL Injection
- Step 18: Extract the First Table Entry Using Blind SQL Injection
- Step 19: Extract Data from Rows Using Blind SQL Injection
- Step 20: Extract SQL-Server Password Hashes
- Step 21: Extract OS and Application Passwords
- Step 22: Extract Data from Database Tables Using SQLMAP
- Step 23: Extract Authentication Credentials Using SQLMAP
- Step 24: Insert, Update, Delete Data from Database
- Step 25: Perform DoS attack Attempt using SQL Injection
- Step 26: Evade IDS Detection Using 'OR 1=1 Equivalents
- Step 27: Evade IDS Detection Using Char Encoding
- Step 28: Evade IDS Detection by Manipulating White Spaces
- Step 29: Evade IDS Detection Using Inline Comments
- Step 30: Evade IDS Detection Using Obfuscated Code
- Step 31: Bypass Website Authentication
- Step 32: Perform a Function-Call Injection Attack
- Step 33: Perform a Buffer Overflow Attack
- Step 34: Access System Files and Execute Remote Commands
- Step 35: Use OPENROWSET to Escalate Privileges on the Microsoft SQL Server

  - An SQL Injection Pen-Testing Tool
    - BSQLHacker
    - SQL Power Injector
    - Havij
    - SQL Injection Penetration Testing Tools
  - Best Practices to Prevent SQL Injection

- Module Summary

Module 12: Database Penetration Testing Methodology

- Module Objectives
- Database Penetration Testing Steps
  - Step 1: Perform Database Port Scanning
  - Step 2: Sniff Database-related Traffic on the Local Wire
  - Step 3: Test for Weak Passwords, Default Accounts On Databases
  - Step 4: Perform Google Hacking for Database Errors
- Oracle Database penetration testing
  - Step 5: Exploit Web Applications to Retrieve Information about Oracle Databases Running at the Backend
  - Step 6: Identify the Version Numbers Used by the Database
  - Step 7: Determine Oracle Version Using Metasploit
  - Step 8: Identify the Password Management in Oracle
  - Step 9: Identify the Execution of Public Privileges on Oracle
  - Step 10: Identify Privilege Escalation via Cursor Technique in Oracle
  - Step 11: Identify Public Privileges from Object Types
- Oracle Auditing – Wrong Statements Logged
  - Possible Attacks Against Oracle Database Vault
    - Step 12: Identify Oracle Java Vulnerabilities in SQL Injection
    - Step 13: Determine Oracle Service ID (SID) Using Metasploit
    - Step 14: Identify Attack in Database Target DB by Using a Simulated User
    - Step 15: Scan for other Default Ports Used by the Oracle Database
    - Step 16: Scan for Non-Default Ports Used by the Oracle Database
    - Step 17: Identify the Instance Names Used by the Oracle Database
    - Step 18: Attempt to Brute-Force Password Hashes from the Oracle Database
    - Step 19: Check the Status of the TNS Listener Running at Oracle Server
      - Oracle TNS Listener: Screenshot
      - Finding the TNS Listener
      - Listener Modes
    - Step 20: Try to Log in Using Default Account Passwords
    - Step 21: Try to Enumerate SIDs

- Step 22: Use SQL *Plus to Enumerate System Tables

- MS SQL Server Penetration Testing
  - Step 23: Extract SQL Server Database Information
  - Step 24: Test for Direct Access Interrogation
  - Step 25: Test for SQL Server Resolution Service (SSRS)
  - Step 26: Test for Buffer Overflow in the pwdencrypt() Function
  - Step 27: Test for Heap/Stack Buffer Overflow in SSRS
  - Step 28: Test for Buffer Overflows in the Extended Stored Procedures
  - Step 29: Test for Service Account Registry Key
  - Step 30: Test the Stored Procedure to Run Web Tasks
  - Step 31: Attempt Direct-Exploit Attacks
  - Step 32: Retrieve all Login Accounts Using T-SQL Query
  - Step 33: Brute-force SA Account
- MySQL Server Penetration Testing
  - Step 34: Extract the Version of the MySQL Server Database Being Used
  - Step 35: Try to Log in Using Default/ Common Passwords
  - Step 36: Brute-force Accounts Using Dictionary Attack
  - Step 37: Extract System and User Tables from the Database
- Database Password Cracking Tool
  - Cain & Abel
  - HexorBase
- Database Vulnerability Assessment Tool
  - AppDetectivePro
  - NGS SQuirreL
- Database Penetration Testing Tool
  - Oracle TNS Password Tester
  - Secure Oracle Auditor (SOA)
  - Oracle Default Password Tester
  - Oracle Access Rights Auditor
  - Database Password Cracking Tools
  - Database Penetration Testing Tools

- Recommendations for Securing Databases
- Module Summary

Module 13: Wireless Network Penetration Testing Methodology

- Module Objectives
- Wireless Penetration Testing
- Wireless Security Threats
- Wireless Penetration-Testing Tools
  - Aircrack-ng Suite
  - Aircrack-ng Screenshot
  - Kismet
  - AirMagnet WiFi Analyzer
  - AirDefense
- Wireless Penetration Testing Steps
  - Step 1: Discover the Wireless Networks
    - Wi-Fi Discovery Tool
      - NetSurveyor
      - WirelessMon
      - Wi-Fi Discovery Tools
  - Step 2: Detect Hidden SSIDs
  - Step 3: Check Physical Security of AP
  - Step 4: Detect Wireless Connections
    - Active Wireless Scanner: inSSIDer
  - Step 5: Sniff Traffic between the AP and Linked Devices
    - Wireless Packet Sniffer
      - Wireshark
      - OmniPeek
      - CommView for Wi-Fi
      - Wireless Packet Sniffers
  - Step 6: Create Ad Hoc Associations with an Unsecured AP
  - Step 7: Create a Rogue Access Point and Try to Create a Promiscuous Client

- Step 8: Use a Wireless Honeypot to Discover Vulnerable Wireless Clients
- Step 9: Perform a Denial-of-Service Attack (De-authentication Attack)
- Step 10: Attempt Rapid Traffic Generation
- Step 11: Jam the Signal
  - Wi-Fi Jamming Devices
- Step 12: Attempt Single-Packet Decryption
- Step 13: Perform Fragmentation Attack
- Step 14: Perform an ARP Poisoning Attack
- Step 15: Try to Inject the Encrypted Packet
- Step 16: Crack Static WEP Keys
  - WEP Cracking Tool: Cain & Abel
- Step 17: Crack WPA-PSK Keys
  - WPA Brute Forcing Using Cain & Abel
  - WPA-PSK Cracking Tool: Elcomsoft Wireless Security Auditor
- Step 18: Crack WPA/WPA2 Enterprise Mode
- Step 19: Crack WPS PIN
- Step 20: Check for MAC Filtering
- Step 21: Spoof the MAC Address
- Step 22: Create a Direct Connection to the Wireless Access Point
- Step 23: Attempt an MITM Attack
- Step 24: Test for Wireless Driver Vulnerabilities

- RFID Penetration Testing
  - Introduction to RFID Penetration Testing
  - RFID Penetration-Testing Steps
    - Step 1: Perform Reverse Engineering
    - Step 2: Perform Power Analysis Attack
    - Step 3: Perform Eavesdropping
    - Step 4: Perform an MITM Attack
    - Step 5: Perform a DoS Attack
    - Step 6: Perform RFID Cloning/Spoofing
    - Step 7: Perform an RFID Replay Attack

- Step 8: Perform a Virus Attack

- RFID Hacking Tool
  - Tastic RFID Thief
  - RFDump
  - Oscilloscopes
  - RFID Antennas
  - RFID Readers

- NFC Penetration Testing
  - Introduction to NFC Penetration Testing
    - Step 1: Perform Eavesdropping
    - Step 2: Perform a Data Modification Attack
    - Step 3: Perform Data Corruption Attack
    - Step 4: Perform an MITM Attack
- IoT Penetration Testing
  - Introduction to IoT Penetration Testing
  - IoT Penetration-Testing Steps
  - IoT Attack Surface
    - Step 1: Testing an IoT Device for an Insecure Web Interface
    - Step 2: Testing an IoT Device for Poor Authentication/Authorization
    - Step 3: Testing an IoT Device for Poor Insecure Network Services
    - Step 4: Testing an IoT Device for Lack of Transport Encryption
    - Step 5: Testing an IoT Device for Privacy Concerns
    - Step 6: Testing an IoT Device for an Insecure Cloud Interface
    - Step 7: Testing an IoT Device for Insecure Mobile Interface
    - Step 8: Testing an IoT Device for Insufficient Security Configurability
    - Step 9: Testing an IoT Device for Insecure Software/Firmware
    - Step 10: Testing an IoT Device for Poor Physical Security
  - IoT Penetration Testing Tool: HardSploit
- Module Summary

Module 14: Mobile Devices Penetration Testing Methodology

- Module Objectives
- Why Mobile Device Penetration Testing
  - Requirements for Mobile Device Penetration Testing
- Mobile Devices Market Share
- Mobile penetration Testing requires rooting/jailbreaking of mobile devices
  - Rooting the Android Phones
  - Jailbreaking iPhones
- Mobile Penetration Testing Methodology
  - Mobile Phone Penetration Testing Steps
    - Communication Channel Penetration Testing
      - Step 1: Intercept HTTP Requests Sent from Phone Browser/Applications
      - Step 2: Intercept HTTP Request using Proxy when using Android Emulator
      - Step 3: Intercept HTTP Request using Proxy on iPhone
      - Step 4: Intercept HTTP Request using Proxy on iOS Simulator
      - Step 5: Intercept iOS Traffic using Burp suite
      - Step 6: Sniff the Traffic using WireShark
      - Step 7: Sniff the Traffic Using FaceNiff
    - Server-side Infrastructure Pen Testing
    - Application Penetration Testing
- Android Application Penetration Testing
  - Setting up the Environment for Android Apps Penetration Testing
    - Step 8: Identify whether iPhone Is Rooted or Not
  - Android Browser-based Applications Penetration Testing
  - Android Platform-based Applications Penetration Testing
    - Step 9: Test for Application Least Privilege
    - Step 10: Explore Installed Packages on Android Phone with Package Play
    - Step 11: Perform Intent Sniffing
    - Step 12: Test Android App using Intent Fuzzer
      - Test whether Application Stores any Sensitive Information
      - Test whether Log of Application Reveals any Sensitive Information

- Step 13: Try to Reverse Engineer the Android Application
- Step 14: Try to Discover the Processes Running on the Android Device
- Step 15: Try to Discover the System Calls Made by Processes
- Step 16: Check for Sensitive Data on SD Card
- Step 17: Test whether SQLite Database Reveals any Sensitive Data
- Step 18: Perform a DoS Attack on Android Phone
- Step 19: Find and Exploit Android app Vulnerabilities using Drozer
- Step 20: Conduct Penetration Testing using Smartphone Pentest Framework
- Step 21: Conduct Vulnerability Scanning using zANTI
- Step 22: Perform Android Penetration Testing using dSploit
  - Android Penetration Testing Tools

- iPhone Application Penetration Testing
  - Setting up the Environment for iOS Apps Penetration Testing
  - Before IPA Penetration Testing
    - Step 23: Identify whether iPhone Is Jailbroken or Not
    - Step 24: Inspect the Plist for Sensitive Information
    - Step 25: Investigate the Keychain Data Storage
    - Step 26: Check the iPhone Logs for Leakage of Sensitive Information (Insecure Logging)
    - Step 27: Explore and Look for Sensitive Files in iOS File System
    - Step 28: Inspecting SQLite Databases
    - Step 29: Inspect Error Application Logs
    - Step 30: Inspect Device Logs
    - Step 31: Look for Sensitive Data Cached in Snapshots
    - Step 32: Inspect Keyboard Cache
    - Step 33: Inspect cookies.binarycookies File for Leakage of Sensitive Information
    - Step 34: Check URL Schemes used by Applications
    - Step 35: Check for Broken Cryptography
    - Step 36: Try to Reverse Engineer the iOS Applications
  - iPhone Penetration Testing Tools
- Mobile Phone Security Best Practices

- Device
- Application
- Data
- Network

- Module Summary

Module 15: Cloud Penetration Testing Methodology

- Module Objectives
- Cloud Computing Security and Concerns
- Security Risks Involved in Cloud Computing
- Security Controls and the Cloud Computing Compliance Model
- Role of Penetration Testing in Cloud Computing
- Key Considerations for Pen Testing in the Cloud
- Scope of Cloud Pen Testing
- Cloud Penetration Testing Steps
  - Step 1: Check for Lock-In Problems
  - Step 2: Check for Governance Issues
  - Step 3: Check for Compliance Issues
  - Step 4: Check for Right Implementation of Security Management
  - Step 5: Check the Cloud for Resource Isolation
  - Step 6: Check whether Anti-malware Applications are Installed and Updated on Every Device
  - Step 7: Check whether Firewalls are Installed at Every Network Entry Point
  - Step 8: Check that Strong Authentication is Deployed for Every Remote User
  - Step 9: Check whether File Transfers to/from Cloud Servers are Encrypted
  - Step 10: Check whether Files Stored on Cloud Servers are Encrypted
  - Step 11: Check the Data Retention Policy of Service Providers
  - Step 12: Check that all Users Follow Safe Internet Practices
  - Step 13: Perform a Detailed Vulnerability Assessment
  - Step 14: Try to Gain Passwords to Hijack Cloud Service
  - Step 15: Test for Virtualization Management (VM) Security

- Step 16: Check Audit and Evidence-gathering Features in the Cloud Service
- Step 17: Perform Automated Cloud Security Testing

- Recommendations for Cloud Testing
- Module Summary

Module 16: Report Writing and Post Test Actions

- Module Objectives
- Module Flow
- Penetration Testing Deliverables
  - Goal of the Penetration Testing Report
  - Types of Pen Test Reports
  - Characteristics of a Good Pen Testing Report
  - Delivering Penetration Testing Report
- Writing Pen Testing Report
  - Writing the Final Report
  - Report Development Process
  - Planning the Report
  - Collect and Document the Information
  - Write a Draft Report
  - Review and Finalize the Report
- Pen Testing Report Format
  - Sample Pen Testing Report Format
  - Report Format – Cover Letter
  - Document Properties/Version History
  - Table of Contents/Final Report
  - Summary of Execution
  - Scope of the Project
  - Evaluation Purpose/System Description
  - Assumptions/Timeline
  - Summary of Evaluation, Findings, and Recommendations
  - Methodologies

- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Result Analysis
- Recommendations
- Appendices
  - Sample Appendix

- Result Analysis
  - Penetration Testing Report Analysis
  - Report on Penetration Testing
  - Pen Test Team Meeting
  - Research Analysis
  - Pen Test Findings
  - Rating Findings
  - Example of Finding - I
  - Example of Finding - II
  - Analyze
- Post Testing Actions
  - Prioritize Recommendations
  - Develop Action Plan
  - Points to Check in Action Plan
  - Develop and Implement Data Backup Plan
  - Create Process for Minimizing Misconfiguration Chances
  - Updates and Patches
  - Capture Lessons Learned and Best Practices
  - Create Security Policies
  - Conduct Training
  - Cleanup and Restoration
- Report Retention
  - Destroy the Report

- Sign-off Document
- Sign-off Document Template

- Module Summary