EC-COUNCIL CERTIFIED SECURITY ANALYST

COURSE OUTLINE

EC-Council Accredited Training Center

ECSA EC-Council Certified Security Analyst

EC-Council

TABLE OF CONTENT

1 COURSE DESCRIPTION

The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report. The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and elevates your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology

- Focuses on pentesting methodology with an emphasis on hands-on learning
- The exam will now have a prerequisite of submitting a pentesting report
- The goal of these changes is to make passing ECSA more difficult; therefore, making it a more respected certification

2 MODULE-1: NEED FOR SECURITY ANALYSIS

- Computer Security Concerns
  - Protect Information
  - Security Concerns Due to Intrusions
  - Greatest Challenges of Security
  - Environmental Complexity
  - New Technologies
  - New Threats and Exploits
  - Limited Focus
  - Limited Expertise
  - Threat Agents
- Information Security Measures
  - Data Security Measures
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation
- Risk Analysis
  - Assessment Questions
  - Security Limit
  - Risk

- Simplifying Risk
- Risk Analysis
- Risk Assessment Answers Seven Questions
- Steps of Risk Assessment
- Risk Assessment Values

- Hardening Security
  - No Simple Solutions
  - We Must be Diligent
  - Information Security Awareness
- Security Policies
  - Security Policies
  - Security Policy Basics
  - Policy Statements
  - Types of Security Policies
  - Promiscuous Policy
  - Permissive Policy
  - Prudent Policy
  - Paranoid Policy
- Sample Policies
  - Acceptable-Use Policy

- Remote-Access Policy
- Wireless Security Policy
- Email Security Policy
- Email and Internet Usage Policies
- Personal Computer Acceptable Use Policy
- Firewall-Management Policy
- Internet Acceptable Use Policy
- User Identification and Password Policy
- Software License Policy
- User-Account Policy
- Information-Protection Policy
- Special-Access Policy
- Network-Connection Policy
- Business-Partner Policy
- Data Classification Policy
- Intrusion Detection Policy
- Virus Prevention Policy
- Laptop Security Policy
- Personal Security Policy
- Cryptography Policy

- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- FACTA Policy

- Other Important Policies
- Information Security Standards
  - ISO 17799
  - Domains of ISO 17799
  - ISO/IEC 27001
- COBIT
- Information Security Acts and Laws
  - 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
  - Affect of Law on 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

3 MODULE-2: SECURING OPERATING SYSTEMS

- Introduction to TCP/IP
  - TCP/IP Model
  - Comparing OSI and TCP/IP
  - Port Numbers
  - Internet Assigned Numbers Authority (IANA)
  - IP Header
  - IP Header: Protocol Field
  - TCP
  - TCP Header
- TCP/IP Connection
  - Source and Destination Port Connection
  - What Makes Each Connection Unique
  - TCP/UDP Connection State Checking Using netstat
  - TCP Operation
  - Three-Way Handshake
  - Flow Control
  - Flow Control Mechanism: Synchronization
  - Flow Control Mechanism: Sequencing Numbers
  - Flow Control Mechanism: Positive Acknowledgment with Retransmission

- (PAR)
- Flow Control Mechanism: Windowing
- Windowing
- Sliding Windows
- Sliding Window Example
- TCP Services
- User Datagram Protocol (UDP)
- UDP Operation

- Introduction to IPv6
  - 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

- TCP/IP Security
  - IPsec
  - DNSSEC
  - DNSSEC Features
  - DNSSEC Working
  - Managing DNSSEC for Your Domain Name
  - What Is a DS Record?
  - How Does DNSSEC Protect Internet Users?
  - Operation of DNSSEC
  - Firewalls and Packet Filtering
  - Denial-of-Service (DoS) Attacks
  - DoS SYN Flooding Attack
- Internet Control Message Protocol (ICMP)
  - 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

- TCP/IP in Mobile Communications
  - TCP/IP Concepts in Mobile Technology
  - TCP Options That Can Help Improve Performance

4 MODULE-3: PENETRATION TESTING METHODOLOGIES

- Introduction to Penetration Testing
  - What Is Penetration Testing?
  - Why Penetration Testing?
  - Penetration Test vs. Vulnerability Test
  - What Should Be Tested?
  - What Makes a Good Penetration Test?
  - Constraints of Penetration Testing
- Types of Penetration Testing
  - 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
  - Penetration Testing Strategies: Internal Security Assessment
- Phases of Penetration Testing
  - Penetration Testing Process
  - Phases of Penetration Testing

- Pre-Attack Phase
- Pre-Attack Phase: Passive Reconnaissance
- Pre-Attack Phase: Active Reconnaissance
- Attack Phase
- Attack Phase Activities
- Activity: Perimeter Testing
- Activity: Web Application Testing - I
- Activity: Web Application Testing - II
- Activity: Web Application Testing - III
- Activity: Wireless Testing
- Activity: Application Security Assessment
- Types of Application Security Assessment
- Activity: Network Security Assessment
- Activity: Wireless/Remote Access Assessment
- Activity: Database Penetration Testing
- Activity: File Integrity Checking
- Log Management Penetration Testing
- Telephony Security Assessment
- Data Leakage Penetration Testing
- Social Engineering

- Post-Attack Phase and Activities

- Penetration Testing Methodology
  - Need for a Methodology
  - Penetration Testing Methodology
  - Reliance on Checklists and Templates
- Pen Test Strategies
  - Operational Strategies for Security Testing
  - Categorization of the Information System Security
  - Identifying Benefits of Each Test Type
  - Prioritizing the Systems for Testing
  - ROI for Penetration Testing
  - Determining Cost of Each Test Type
  - Penetration Testing Best Practices
  - Guidelines for Security Checking
- Penetration Testing Consultants
  - Penetration Testing Consultants
  - Required Skills Sets of a Penetration Tester
  - Hiring a Penetration Tester
  - Responsibilities of 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

- Ethics of a Licensed Penetration Tester
  - What Makes a Licensed Penetration Tester
  - Modus Operandi
  - Preparation
  - Ethics of a Penetration Tester
  - Evolving as a Licensed Penetration Tester
  - Dress Code
    - Example: Licensed Penetration Tester Dress Code
  - Communication Skills of a Penetration Tester
  - LPT Audited Logos
    - Example: LPT Audited Logos

5 MODULE-4: CUSTOMERS AND LEGAL AGREEMENTS

- Do Organizations Need Pen Testing?
  - Why Do Organizations Need Pen Testing?
  - Initial Stages in Penetration Testing
  - Understand Customer Requirements
  - Create a Checklist of the Testing Requirements

- Penetration Testing 'Rules of Behavior'
  - Penetration Testing 'Rules of Behavior'
  - Penetration Testing Risks
  - Penetration Testing by Third Parties
  - Precautions While Outsourcing Penetration Testing

- Legal Issues in Penetration Testing
  - Legal Issues in Penetration Testing
  - Get Out of Jail Free Card
  - Permitted Items in Legal Agreement
  - Confidentiality and Non-Disclosure Agreements (NDAs)

- Penetration Testing Contract
  - Penetration Testing Contract
  - Drafting Contracts
  - XSECURITY: Sample Penetration Testing Contract
  - Sample Penetration Testing Contract
  - XSECURITY: Sample Rules of Engagement Document

- Liability Issues
- Negligence Claim
- Limitations of the Contract
- Plan for the Worst

- How Much to Charge?
  - How Much to Charge?
  - How to Reduce the Cost of Penetration Testing

6 MODULE-5: RULES OF ENGAGEMENT

- Rules of Engagement (ROE)
  - Statement of Work (SOW)
  - Rules of Engagement (ROE)
  - Scope of ROE
  - Points of Contact Template

- Steps for Framing ROE
  - Steps for Framing ROE
  - Review Engagement Letter

- Clauses in ROE
  - Clauses in ROE
  - Rules of Engagement Template (Sample)

7 MODULE-6: PENETRATION TESTING PLANNING AND SCHEDULING

- Test Plan Identifier
- Test Deliverables
- Penetration Testing Planning Phase
  - Define the Pen Testing Scope
    - Project Scope: Components to Be Tested
    - Project Scope: When to Retest?
    - Project Scope: Responsibilities
  - Staffing
    - Skills and Knowledge Required
    - Internal Employees
    - Penetration Testing Teams
    - Tiger Team
    - Questions to Ask Before Hiring Consultants for the Tiger Team
  - Kickoff Meeting
    - Meeting with the Client
    - Kickoff Meeting
  - Develop the Project Plan
    - Contents of a Pen Testing Project Plan
    - Project Plan Overview
    - Work Breakdown Structure or Task List
    - Penetration Testing Schedule
    - Penetration Testing Project Scheduling Tools: Project Professional 2013
    - Penetration Testing Project Scheduling Tools
    - XSECURITY: Test Plan Checklist

- XSECURITY: Test Plan Checklist
- Penetration Testing Hardware/Software Requirements

8 MODULE-7: PRE-PENETRATION TESTING STEPS

- Pre-penetration Testing Steps
  - Step 1: List the Client Organization's Penetration Testing Requirements of the Test 1 (a)
  - Step 1: List the Client Organization's Penetration Testing Purpose for the Test 1 (b)
  - Step 2: Obtain Penetration Testing Permission from the Company's Stakeholders
  - Step 3: Obtain Special Permission if Required from the Local Law Enforcement Agency
  - Step 4: Obtain the Detailed Proposal of Tests and Services That Are to Be Carried Out
  - Step 5: List the Tests That Will Not Be Carried Out at the Client's Network
  - Step 6: Identify the Type of Testing That Would Be Carried Out: Black-box or White- box Testing
  - Step 7: Identify the Type of Testing That Would Be Carried Out:
  - Announced/Unannounced
  - Step 8: List the Servers, Workstations, Desktops, and Network Devices That Need to Be Tested
  - Step 9: Request Previous Penetration Testing/Vulnerability Assessment Reports (If Possible)
  - Step 10: Prepare the Rules of Engagement That Lists the Company's Core Competencies/Limitations/Time Scales
  - Step 11: Hire a Lawyer Who Can Handle Your Penetration Testing Legal Documents

- Step12: Prepare the Penetration Testing Legal Document and Get It Vetted with Your Lawyer
- Step 13: Prepare a Non-Disclosure Agreement (NDA) and Have the Client Sign It
- 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 Dollars)
- Step 17: Identify the List of Penetration Testers Required for This Project
- Step 18: Identify Who Will Be Leading the Penetration Testing Project (Chief Penetration Tester)
- Step 19: Prepare a Tiger Team
- Step 20: Obtain Temporary Identification Cards from the Client for the Team Members Involved in the Process
- Step 21: Identify the Office Space/Location Your Team Would Be Working on for This Project
- Step 22: Gather Information about the Client Organization's History and Background
- Step 23: Visit the Client Organization's Premises and Become Familiar with the Surroundings
- Step 24: Identify the Network Topology in Which the Test Would Be Carried Out
- Step 25: List the Security Tools That You Will Be Using for the Penetration Testing Project
- Step 26: List the Hardware and Software Requirements for the Penetration Testing Project

- Step 27: Identify the Local Equipment Required for Pen Test
- Step 28: Identify the Local Manpower Required for Pen Test
- Step 29: Identify the Client's IT Security Admin Who Will Be Helping You in the Pen Testing (if Possible)
- Step 30: List the Contacts at the Client Organization Who Will Be in Charge of the Pen Testing Project
- Step 31: Obtain the Contact Details of the Key Person at the Client's Company During an Emergency
- Step 32: List the Points of Contact During an Emergency
- Step 33: List the Known Waivers/Exemptions
- Step 34: List the Contractual Constraints in the Penetration Testing Agreement
- Step 35: Identify the Reporting Time Scales with the Client's Organization
- Step 36: Negotiate Per Day/Per Hour Fee That You Will Be Charging for the Penetration Testing Project
- Step 37: Draft the Timeline for the Penetration Testing Project
- Step 38: Draft a Quotation for the Services That You Will Be Providing to the Client's Origination
- Step 39: Identify How the Final Penetration Testing Report Will Be Delivered to the Client's Organization
- Step 40: Identify the Reports to Be Delivered After Pen Test

9 MODULE-8: INFORMATION GATHERING

- What Is Information Gathering?
- Information Gathering Terminologies
- Information Gathering Steps
  - Step 1: Find the Company's URL
  - Step 2: Locate Internal URLs
  - Step 3: Identify a Company's Private and Public Websites
  - Step 4: Search for Company's Information
    - Tools to Extract Company's Data
  - Step 5: List the Contact Information, Email Addresses, and Telephone Numbers
    - Search Telephone Numbers Using http://www.thephonebook.bt.com
  - Step 6: List Employees of the Company and Personal Email Addresses
  - Step 7: Investigate Key Persons – Searching in Google, Look Up Their Resumes and Cross Link Information
  - Step 8: Search the Internet, Newsgroups, Bulletin Boards, and Negative Websites for Information about the Company
  - Step 9: Find the Geographical Location of a Company
    - Geographical Location Search Using Google Earth
  - Step 10: Use People Search Online Services to Collect the Information
    - Search People Using http://pipl.com
    - Search People Using http://www.intelius.com
    - Search People on Online Services
    - People Search Online Services

- Step 11: Browse Social Network Websites to Find the Information about the Company
  - Search People on Social Networking Services
- Step 12: Use Google/ Yahoo! Finance to Search for Press Releases Issued by the Company
- Step 13: Search for Link Popularity of the Company's Website
  - Search Link Popularity on Alexa
  - Search Link Popularity on SeoCentro
  - Search Link Popularity on Link Appeal
  - Link Popularity Search Online Services
- Step 14: Search for Company's Job Postings through Job Sites
- Step 15: Monitor Target Using Google Alerts
- Step 16: Gather Competitive Intelligence
  - Competitive Intelligence - When Did This Company Begin? How Did It Develop?
  - Competitive Intelligence - What Are the Company's Plans?
  - Competitive Intelligence - What Does Expert Opinion Say About the Company?
  - Competitive Intelligence: Use the EDGAR Database to Research Company Information
  - Competitive Intelligence: Search Company Business Reports and Profiles at Hoovers
  - Competitive Intelligence Tools
  - Competitive Intelligence Consulting Companies
- Step 17: Search for Trade Association Directories
- Step 18: List the Products Sold by the Company

- Search on Ebay for the Company's Presence
- Step 19: List the Company's Partners and Distributors
- Step 20: Compare Price of Product or Service with Competitor
  - Price Comparison Services
- Step 21: Search for Web Pages Posting Patterns and Revision Numbers
- Step 22: Visit the Company as Inquirer and Extract Privileged Information
- Step 23: Visit the Company Locality
- Step 24: Email the Employee Disguised as Customer Asking for Quotation
- Step 25: Use Web Investigation Tools to Extract Sensitive Data Targeting the Company
- Step 26: Look Up Registered Information in Whols Database
  - Whols Lookup Result
  - Whols Lookup Tools
  - Whols Lookup Tools: SmartWhois
- Step 27: Extract DNS Information using Domain Research Tools
  - DNS Interrogation Tools
  - Domain Research Tool (DRT)
  - DNS Interrogation Tools
- Step 28: Search Similar or Parallel Domain Name Listings
- Step 29: Retrieve the DNS Record of the Organization from Publicly Available Servers
  - DNS Interrogation Online Tools
- Step 30: Locate the Network Range
  - Traceroute Analysis
  - Traceroute Tool: VisualRoute 2010
  - Traceroute Tool: Path Analyzer Pro

ECSA™
EC-Council Certified Security Analyst

- Traceroute Tools
- Step 31: Search the Internet Archive Pages about the Company
- Step 32: Monitor Web Updates Using Website Watcher
- Step 33: Crawl the Website and Mirror the Pages on Your PC
  - Website Mirroring Tools
- Step 34: Crawl the FTP Site and Mirror the Pages on Your PC
  - FTP Site Mirroring Tool: WebCopier Pro
- Step 35: Track Email Communications
  - Email Tracking Tools
- Step 36: Use GHDB and Search for the Company's Internal Resources
  - GHDB Screenshot

10 MODULE-9: VULNERABILITY ANALYSIS

- What Is Vulnerability Assessment?
- Why Assessment
- Vulnerability Classification
- Types of Vulnerability Assessment
- 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
  - Product-based Solutions
  - Service-based Solutions
  - Tree-based Assessment
  - Inference-based Assessment
- Characteristics of a Good Vulnerability Assessment Solution
- Vulnerability Assessment Considerations
- Vulnerability Assessment Reports
  - Sample Vulnerability Assessment Report
- Vulnerability Report Model
- Timeline
- Types of Vulnerability Assessment Tools
  - Host-based Vulnerability Assessment Tools

- Application-layer Vulnerability Assessment Tools
- Depth Assessment Tools
- Scope Assessment Tools
- Active/Passive Tools
- Location/Data Examined Tools

- Choosing a Vulnerability Assessment Tool
- Criteria for Choosing a Vulnerability Assessment Tool
- Best Practices for Vulnerability Assessment Tools
- Vulnerability Assessment Tools
  - QualysGuard Vulnerability Management
  - Retina Network Security Scanner
  - GFI LANGuard
  - SAINT Vulnerability Scanner
  - Microsoft Baseline Security Analyzer (MBSA)
  - Nessus
- Report
  - Vulnerability Assessment Reports
  - Security Vulnerability Report
  - Security Vulnerability Summary
  - AVDS - Automated Vulnerability Detection System
  - Automated Scanning Server Reports
- Vulnerability Analysis Chart

11 MODULE-10: EXTERNAL PENETRATION TESTING

- External Intrusion Test and Analysis
- Why Is It Done?
- Client Benefits
- External Penetration Testing
- Steps for Conducting External Penetration Testing
  - 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

    Traceroute Example
  - Step 5/6: Locate TCP/UDP Traffic Path to the Destination
    - Traffic Sniffing and Analysis Tool: Tstat
  - Step 7: Identify the Physical Location of the Target Servers
  - Step 8: Examine the Use of IPv6 at the Remote Location
  - Step 9: Look Up Domain Registry for IP Information
    - DNS Interrogation Tools
  - Step 10: Find IP Block Information about the Target
    - WHOIS Lookup Tools
  - Step 11: Locate the ISP Servicing the Client
  - Step 12: Port Scan Every Port (65,536) on the Target's Network
    - Common Ports List
  - Step 13: List Open Ports

- Scanning Tool: NetScan Tools Pro

- Step 14: List Closed Ports
  - Scanning Tools
- Step 15: List Suspicious Ports That Are Half Open/Closed
- Step 16: Use SYN Scan on the Target and See the Response
- Step 17: Use Connect Scan on the Target and See the Response
- Step 18: Use XMAS Scan on the Target and See the Response
- Step 19: Use FIN Scan on the Target and See the Response
- Step 20: Use NULL Scan on the Target and See the Response
- Step 21: Use Fragmentation Scanning and Examine the Response
- Step 22: Firewalk on the Router's Gateway and Guess the Access List
- Step 23: Examine TCP Sequence Number Prediction
- Step 24: Examine the Use of Standard and Non-Standard Protocols
- Step 25: Examine IPID Sequence Number Prediction

  Hping2 IPID Example
- Step 26: Examine the System Uptime of Target Server
- Step 27: Examine Operating System Used for Different Targets
- Step 28: Examine the Patches Applied to the Operating System
- Step 29: Locate DNS Record of the Domain and Attempt DNS Hijacking

- Step 30: Download Applications from the Company's Website and Reverse Engineer the Binary Code
- Step 31: List Programming Languages Used and Application Software to Create Various Programs from the Target Server
- Step 32: Look for Error and Custom Web Pages
- Step 33: Guess Different Subdomain Names and Analyze Responses
- Step 34: Examine the Session Variables
- Step 35: Examine Cookies Generated by the Server
- Step 36: Examine the Access Controls Used by the Web Application
- Step 37: Brute Force URL Injections and Session Tokens
- Step 38: Check for Directory Consistency and Page Naming Syntax of the Web Pages
- Step 39: Look for Sensitive Information in Web Page Source Code
- Step 40: Attempt URL Encodings on the Web Pages
- Step 41: Try Buffer Overflow Attempts in Input Fields
    - Look for Invalid Ranges in Input Fields
    - Attempt Escape Character Injection
- Step 42: Try Cross Site Scripting (XSS) Techniques
- Step 43: Record and Replay the Traffic to the Target Web Server and Note the Response
- Step 44: Try Various SQL Injection Techniques

- Step 45: Examine Hidden Fields
    - Examine Server Side Includes (SSI)
- Step 46: Examine E-commerce and Payment Gateways Handled by the Web Server
- Step 47: Examine Welcome Messages, Error Messages, and Debug Messages
- Step 48: Probe the Service by SMTP Mail Bouncing
- Step 49: Grab the Banner of HTTP Servers
- Step 50: Grab the Banner of SMTP Servers
- Step 51: Grab the Banner of POP3 Servers
- Step 52: Grab the Banner of FTP Servers
- Step 53: Identify the Web Extensions Used at the Server
- Step 54: Try to Use HTTPS Tunnel to Encapsulate Traffic
- Step 55: OS Fingerprint Target Servers
- Step 56: Check for ICMP Responses
- Step 57: Check for ICMP Responses from Broadcast Address
- Step 58: Port Scan DNS Servers (TCP/UDP 53)
- Step 59: Port Scan TFTP Servers (Port 69)
- Step 60: Test for NTP Ports (Port 123)
- Step 61: Test for SNMP Ports (Port 161)
- Step 62: Test for Telnet Ports (Port 23)

- Step 63: Test for LDAP Ports (Port 389)
- Step 64: Test for NetBIOS Ports (Ports 135-139, 445)
- Step 65: Test for SQL Server Ports (Port 1433, 1434)
- Step 66: Test for Citrix Ports (Port 1495)
- Step 67: Test for Oracle Ports (Port 1521)
- Step 68: Test for NFS Ports (Port 2049)
- Step 69: Test for Compaq, HP Inside Manager Ports (Port 2301, 2381)
- Step 70: Test for Remote Desktop Ports (Port 3389)
- Step 71: Test for Sybase Ports (Port 5000)
- Step 72: Test for SIP Ports (Port 5060)
- Step 73: Test for VNC Ports (Port 5900/5800)
- Step 74: Test for X11 Ports (Port 6000)
- Step 75: Test for Jet Direct Ports (Port 9100)
- Step 76: Port Scan FTP Data (Port 20)
- Step 77: Port Scan Web Servers (Port 80)
- Step 78: Port Scan SSL Servers (Port 443)
- Step 79: Port Scan Kerberos-Active Directory (Port TCP/UDP 88)
- Step 80: Port Scan SSH Servers (Port 22)

- Recommendations to Protect Your System from External Threats

12 MODULE-11: INTERNAL NETWORK PENETRATION TESTING

- Internal Testing
- Steps for Internal Network Penetration Testing
  - Step 1: Map the Internal Network
  - Step 2: Scan the Network for Live Hosts
  - Step 3: Port Scan the Individual Machines
  - Step 4: Try to Gain Access Using Known Vulnerabilities
  - Step 5: Attempt to Establish Null Sessions
  - 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
  - Step 10: Attempt Replay Attacks
  - Step 11: Attempt ARP Poisoning
  - 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
    - Copying Commands in Knoppix
    - Microsoft Diagnostics and Recovery Toolset (DART)
    - Reset the Administrator's Password
- Step 17: Attempt to Plant a Software Keylogger to Steal Passwords
    - Keyloggers and Spy Softwares
- Step 18: Attempt to Plant a Hardware Keylogger to Steal Passwords
- Step 19: Attempt to Plant Spyware on the Target Machine
- Step 20: Attempt to Plant a Trojan on the Target Machine
- Step 21: Attempt to Create a Backdoor Account on the Target Machine
- Step 22: Attempt to Bypass Antivirus Software Installed on the Target Machine
- Step 23: Attempt to Send a Virus Using the Target Machine
- Step 24: Attempt to Plant Rootkits on the Target Machine
- Step 25: Hide Sensitive Data on Target Machines
    - WinMend Folder Hidden
- Step 26: Hide Hacking Tools and Other Data on Target Machines
- Step 27: Use Various Steganography Techniques to Hide Files on Target Machines
    - Whitespace Steganography Tool: SNOW
- Step 28: Escalate User Privileges

- Step 29: Run Wireshark with The Filter ip.src==[ip_address]
- Step 30: Run Wireshark with The Filter ip.dst==[ip_address]
- Step 31: Run Wireshark with Protocol-based Filters
- Step 32: Run Wireshark with The Filter tcp.port==[port_no]
- Step 33: Capture POP3 Traffic
- Step 34: Capture SMTP Traffic
- Step 35: Capture IMAP Email Traffic
- Step 36: Capture the Communications between FTP Client and FTP Server
- Step 37: Capture HTTP Traffic
- Step 38: Capture HTTPS Traffic (Even Though It Cannot Be Decoded)
- Step 39: Capture RDP Traffic
- Step 40: Capture VoIP Traffic
- Step 41: Spoof the MAC address
- Step 42: Poison the Victim's IE Proxy Server
- Step 43: Attempt Session Hijacking on Telnet Traffic
- Step 44: Attempt Session Hijacking on FTP Traffic
- Step 45: Attempt Session Hijacking on HTTP Traffic
    - Automated Internal Network Penetration Testing Tool: Metasploit
    - Automated Internal Network Penetration Testing Tool: CANVAS
    - Vulnerability Scanning Tools

- Recommendations for Internal Network Penetration Testing

13 MODULE-12: FIREWALL PENETRATION TESTING

- 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
- Hardware Firewall
- Software Firewall
- Types of Firewalls
    - Packet Filtering Firewall
    - IP Packet Filtering Firewall
    - Circuit Level Gateway
    - TCP Packet Filtering Firewall
    - Application Level Firewall
    - Application Packet Filtering Firewall
    - Stateful Multilayer Inspection Firewall
    - Multilayer Inspection Firewall

- Firewall Penetration Testing Tool: Firewall Test Agent
- Firewall Penetration Testing Tools
- Firewall Ruleset Mapping
- Best Practices for Firewall Configuration
- 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 the Firewall Architecture
    - Step 8: Testing Firewall Policy
    - Step 9: Test the Firewall Using a 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: Try to Bypass Firewall Using IP Address Spoofing

- Step 16: Try to Bypass Firewall Using Tiny Fragments
- Step 17: Try to Bypass Firewall Using IP Address in Place of URL
- Step 18: Try to Bypass Firewall Using Anonymous Website Surfing Sites
- Step 19: Try to Bypass Firewall Using Proxy Server
- Step 20: Test HTTP Tunneling Method
- Step 21: Test ICMP Tunneling Method
- Step 22: Test ACK Tunneling Method
- Step 23: Try to Bypass Firewall through MITM Attack
- Step 24: Test Firewall-Specific Vulnerabilities

Document Everything

14 MODULE-13: IDS PENETRATION TESTING

- Introduction to IDS
- Application-based IDS
- Multi-Layer Intrusion Detection Systems
- Multi-Layer Intrusion Detection System Benefits
- Wireless Intrusion Detection Systems (WIDSs)
- Common Techniques Used to Evade IDS Systems
- IDS Penetration Testing Steps
    - Step 1: Test for Resource Exhaustion
    - Step 2: Test the IDS by Sending ARP Flood
    - Step 3: Test the IDS by MAC Spoofing
    - Step 4: Test the IDS by IP Spoofing
    - Step 5: Test the Insertion on IDS
    - Step 6: Test by Sending a Packet to the Broadcast Address
    - Step 7: Test by Sending Inconsistent Packets
    - Step 8: Test IP Packet Fragmentation
        - Packet Fragmentation
    - Step 9: Test for Overlapping
    - Step 10: Test for Ping of Death
    - Step 11: Test for TTL Evasion
    - Step 12: Test by Sending a Packet to Port 0

- Step 13: Test for UDP Checksum
- Step 14: Test for TCP Retransmissions
- Step 15: Test the IDS by TCP Flag Manipulation
    - TCP Flags
- Step 16: Test the IDS by Sending SYN Floods
- Step 17: Test Initial Sequence Number Prediction
- Step 18: Test for Backscatter
- Step 19: Check for False Positive Generation
- Step 20: Test the IDS Using Covert Channels
- Step 21: Test Using TCPReplay
- Step 22: Test the IDS Using TCPopera
- Step 23: Test the IDS Using Method Matching
- Step 24: Test the IDS Using URL Encoding
- Step 25: Test the IDS Using Double Slashes
- Step 26: Test the IDS for Reverse Traversal
- Step 27: Test for Self-Referencing Directories
- Step 28: Test for Premature Request Ending
- Step 29: Test for IDS Parameter Hiding
- Step 30: Test for HTTP Misformatting
- Step 31: Test for Long URLs

- Step 32: Test for Win Directory Syntax
- Step 33: Test for Null Method Processing
- Step 34: Test for Case Sensitivity
- Step 35: Test Session Splicing
- Step 36: Try to Bypass Invalid RST Packets through IDS
    - Automated IDS Auditing Tool: Traffic IQ Professional
    - Intrusion Detection Tool: Snort
    - Intrusion Detection Tools

- Recommendations for IDS Penetration Testing

15 MODULE-14: PASSWORD CRACKING PENETRATION TESTING

- Password - Terminology
- Importance of Passwords
- Password Types
  - Cleartext Passwords
  - Obfuscated Passwords
  - Hashed Passwords
- Common Password Vulnerabilities
  - Organizational Password Vulnerabilities
  - Technical Password Vulnerabilities
- Password Cracking Techniques
  - Dictionary Attacks
  - Brute Forcing Attacks
  - Hybrid Attack
  - Syllable Attack
  - Rule-based Attack
- Types of Password Attacks
- How Are Passwords Stored in Windows?
- LM Authentication
- NTLM Authentication
- Kerberos Authentication

- LM, NTLMv1, and NTLMv2
- How Are Passwords Stored in Linux?
- Steps for Password Cracking Penetration Testing
    - Step 1: Identify the Target Person's Personal Profile
        - People Search Using http://pipl.com
        - People Search on Online Services
        - People Search on Social Networking Services
        - People Search on Job Sites
    - Step 2: Perform Non-Electronic Attacks
    - Step 3: Build a Dictionary of Word Lists
        - Dictionary Maker Tool: Word List Compiler
    - Step 4: Attempt to Guess Passwords
    - Step 5: Perform Brute-Force and Dictionary Attacks
        - Password Cracking Tool: Cain & Abel
    - Step 6: Perform Wire Sniffing to Capture Passwords
        - Packet Sniffing Tool: Wireshark
        - Packet Sniffing Tool: NetworkMiner
        - Packet Sniffing Tools
    - Step 7: Perform Man-in-the-Middle Attack to Collect Passwords
        - Man-in-the-Middle Attack Using Ettercap
    - Step 8: Perform Replay Attack to Collect Passwords

- Network Analyzer: Tcpdump/WinDump

- Step 9: Extract SAM File in Windows Machines
  - Tool: SAMInside
- Step 10: Perform Hash Injection (Pass-the-Hash) Attack
- Step 11: Perform Rainbow Attack (Perform Password Attack Using Pre-Computed Hashes)
- Step 12: Extract Cleartext Passwords from an Encrypted LM Hash
- Step 13: Perform Password Cracking Using Distributed Network Attack
  - Elcomsoft Distributed Password Recovery
- Step 14: Extract/etc/passwd and /etc/shadow Files in Linux Systems
- Step 15: Use Automated Passwords Crackers to Break Password-protected Files
  - Password Cracking Tools
- Step 16: Use Trojan/Spyware/Keyloggers to Capture Passwords
  - Spyware Tools
  - Keyloggers

Recommendations for Password Cracking Penetration Testing

16 MODULE-15: SOCIAL ENGINEERING PENETRATION TESTING

- What Is Social Engineering?
- Social Engineering Pen Testing
- Impact of Social Engineering on the Organization
- Common Targets of Social Engineering
- Requirements of Social Engineering
- Steps in Conducting Social Engineering Penetration Test
    - Step 1: Attempt Social Engineering Using the Phone
        - Technical Support Example
        - Authority Support Example
    - Step 2: Attempt Social Engineering by Vishing
    - Step 3: Attempt Social Engineering Using Email
        - Email Spoof: Example
    - Step 4: Attempt Social Engineering by Using Traditional Mail
        - Example 1
        - Example 2
    - Step 5: Attempt Social Engineering in Person
        - Example
    - Step 6: Attempt Social Engineering by Dumpster Diving
        - Steps for Dumpster Diving
    - Step 7: Attempt Social Engineering through Insider Accomplice

- Accomplice

- Step 8: Attempt Social Engineering by Shoulder Surfing
- Step 9: Attempt Social Engineering by Desktop Information
- Step 10: Attempt Social Engineering by Extortion and Blackmail
- Step 11: Attempt Social Engineering Using Phishing Attacks
- Step 12: Attempt Identity Theft
  - Steps for Identity Theft
  - Identity Theft Example
- Step 13: Try to Obtain Satellite Imagery and Building Blueprints
  - Satellite Picture of a Organization
- Step 14: Try to Obtain the Details of an Employee from Social Networking Sites
  - Social Engineering Example: LinkedIn Profile
  - Social Engineering Example: Facebook Profile
  - Social Engineering Example: Twitter Profile
  - Social Engineering Example: Orkut Profile
  - Social Engineering Example: MySpace Profile
- Step 15: Use a Telephone Monitoring Device to Capture Conversation
  - Telephone Recorders and Call Recorders
- Step 16: Use Video Recording Tools to Capture Images
- Step 17: Use a Vehicle/Asset Tracking System to Monitor Motor Vehicles

- Vehicle/Asset Tracking System Examples
- Spy Gadgets

- Step 18: Identify "Disgruntled Employees" and Engage in Conversation to Extract Sensitive Information
- Step 19: Document Everything

17 MODULE-16: WEB APPLICATION PENETRATION TESTING

- Introduction to Web Applications
- Web Application Components
- Web App Pen Testing Phases
    - Fingerprinting Web Application Environment
        - Step 1.1: Manually Browse the Target Website
        - Step 1.2: Check the HTTP and HTML Processing by the Browser
            - HTTP and HTML Analysis Tools
        - Step 1.3: Perform Web Spidering
        - Step 1.4: Perform Search Engine Reconnaissance
        - Step 1.5: Perform Server Discovery
        - Step 1.6: Perform Banner Grabbing to Identify the Target Server
        - Step 1.7: Perform Service Discovery
        - Step 1.8: Identify Server-side Technologies
        - Step 1.9: Identify Server-side Functionality
        - Step 1.10: Investigate the Output from HEAD and OPTIONS HTTP Requests
        - Step 1.11: Investigate the Format and Wording of 404/Other Error Pages
        - Step 1.12: Test for the Recognized File Types/Extensions/Directories
        - Step 1.13: Examine Source of the Available Pages

- Step 1.14: Manipulate Inputs in Order to Elicit a Scripting Error
- Step 1.15: Test for Hidden Fields (Discover Hidden Content)
- Step 1.16: Test for/Discover Default Content
- Step 1.17: Test for Directory Traversal
- Step 1.18: Test for Debug Parameters

- 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
    - Vulnerability Scanners
  - Step 2.6: Test for Server-side Include Injection Attack
- 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 Parameter/Form Tampering
- Step 3.9: Test for URL Manipulation
- Step 3.10: Test for Hidden Field Manipulation Attack
- Step 3.11: Map the Attack Surface
- Step 3.12: Test for Known Vulnerabilities
- Step 3.13: Perform Denial-of-Service Attack
- Step 3.14: Check for Insufficient Transport Layer Protection
- Step 3.15: Check for Weak SSL Ciphers
- Step 3.16: Check for Insecure Cryptographic Storage
- Step 3.17: Check for Unvalidated Redirects and Forwards

- 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

- Testing 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
- 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

- 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
  - Testing Data Validation Mechanism
  - Step 8.1: Test for LDAP Injection

- 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

- 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

18 MODULE-17: SQL PENETRATION TESTING

- Introduction to SQL Injection
- How Do Web Applications Work?
- How Does SQL Injection Work?
- SQL Injection Attack Paths
- Impact of SQL Injection Attacks
- Types of SQL Injection Attacks
- SQL Injection Attack Characters
- SQL Injection Cheat Sheet
- SQL Injection Penetration Testing Steps
    - Step 01: List All Input Fields and Hidden Fields of POST Requests
    - Step 02: Perform Information Gathering
    - Step 03: Attempt to Inject Codes into the Input Fields to Generate an Error
    - Step 04: Try to Find SQL Injection Vulnerabilities by Interface
        - GET/POST Requests Interceptor: Burp Suite Tool
    - Step 05: Try to Find SQL Injection Vulnerabilities by Manipulating a Parameter
    - Step 06: Try to Find SQL Injection Vulnerabilities Using Database Errors and Application Response
    - Step 07: Perform Fuzz Testing to Detect SQL Injection Vulnerabilities
    - Step 08: Perform Function Testing to Detect SQL Injection Vulnerabilities
    - Step 09: Perform Static/Dynamic Testing to Detect SQL Injection Vulnerabilities

- Step 10: Perform Black Box Pen Testing
- Step 11: Try to Detect SQL Injection Vulnerability Using Automated Web-App Vulnerability Scanners
    - SQL Injection Detection Tool: IBM AppScan
    - SQL Injection Detection Tools
- Step 12: Perform a Simple SQL Injection Attack
- Step 13: Perform an Error-based SQL Injection Attack
- Step 14: Try to Bypass Website Logins Using SQL Injection
- Step 15: Perform SQL Manipulation Attacks Using a WHERE Clause
- Step 16: Perform UNION-based SQL Injection
- Step 17: Perform Blind SQL Injection Attack
    - Blind SQL Injection Attack
- Step 18: Try to Extract Database Name by Blind SQL Injection
- Step 19: Try to Extract Database Users by Blind SQL Injection
- Step 20: Try to Extract Column Names Using Blind SQL Injection
- Step 21: Try to Enumerate First Table Entry Using Blind SQL Injection
- Step 22: Try to Extract Data from Rows Using Blind SQL Injection
- Step 23: Determine Privileges, DB Structure, and Column Names
- Step 24: Try Advanced Enumeration Techniques
    - Blind SQL Injection Tool: Absinthe

ECSA™
EC-Council Certified Security Analyst

- Step 25: Perform Code Injection Attack
- Step 26: Perform Function Call Injection Attack
- Step 27: Perform Buffer Overflow Attack
- Step 28: Try to Grab SQL Server Hashes
- Step 29: Extract SQL Server Hashes
- Step 30: Try to Transfer Database to a Different Machine
- Step 31: Extract OS and Application Passwords
- Step 32: Access System Files and Execute Commands
- Step 33: Try to Perform Network Reconnaissance
- Step 34: Try IDS Evasion Using 'OR 1=1 Equivalents
- Step 35: Try to Evade IDS Using Hex Encoding
- Step 36: Try to Evade IDS Using Char Encoding
- Step 37: Try to Evade IDS by Manipulating White Spaces
- Step 38: Try to Evade IDS Using In-line Comments
- Step 39: Try to Evade IDS Using Obfuscated Code
    - SQL Injection Penetration Testing Tool: CORE IMPACT Pro
    - SQL Penetration Testing Tool: Safe3SI
    - SQL Penetration Testing Tool: BSQLHacker
    - SQL Penetration Testing Tool: SQL Power Injector
    - SQL Penetration Testing Tool: Havij

ECSA™
EC-Council Certified Security Analyst

- SQL Penetration Testing Tools

- Best Practices to Prevent SQL Injection

19 MODULE-18: PENETRATION TESTING REPORTS AND POST TESTING ACTIONS

- Penetration Testing Deliverables
  - 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 finalization of 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 Recommendation
- 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
  - Report Retention
  - Destroy the Report
  - Sign-off Document
  - Sign-off Document Template

20 SELF-STUDY MODULES

21 MODULE-19: ROUTER AND SWITCHES PENETRATION TESTING

- Router Testing Issues
- Test for HTTP Configuration Vulnerabilities in Cisco Routers
- Analyze the Router Configuration
- Try to Recover Router Passwords from Config File
- 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
    - Step 4: Identify Protocols Running
    - Step 5: 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
        - Privileged Mode Attacks

- Step 9: Test for SNMP Capabilities
- Step 10: Perform SNMP Bruteforcing
    - SNMP "Community String"
- Step 11: Test for TFTP Connections
    - TFTP Testing
- Step 12: Test if Finger Is Running on the Router
- Step 13: Test for CDP Protocol Running on the Router
    - How to Test Cisco Discovery Protocol (CDP)?
- Step 14: Test for NTP Protocol
- Step 15: Test for Access to Router Console Port
- Step 16: Test for Loose and Strict Source Routing
- Step 17: Test for IP Spoofing
- Step 18 : Test for IP Handling Bugs
- Step 19: Test ARP Attacks
- Step 20: Test for Routing Protocol Assessment
- Step 21: RIP Testing
- Step 22: Test for OSPF Protocol
- Step 23: Test BGP Protocol
- Step 24: Test for EIGRP Protocol
- Step 25: Test Router Denial-of-Service Attacks

- Step 26: Test Router's HTTP Capabilities
- Step 27: Test Through HSRP Attack
    - Router Testing Report

- Penetration Testing Steps for Switches
    - Step 1: Testing Address of 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
    - Step 16: Automated Tool for Switch: Switch Center

- Recommendations for Router and Switches Penetration Testing

22 MODULE-20: WIRELESS NETWORK PENETRATION TESTING

- Wireless Penetration Testing
- Wireless Security Threats
- Wireless Penetration Testing Steps
  - Step 1: Discover the Wireless Networks
    - Wi-Fi Discovery Tool: NetSurveyor
    - Wi-Fi Discovery Tool: NetStumbler
    - 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
    - Wireless Packet Sniffer: OmniPeek
    - Wireless Packet Sniffer: CommView for Wi-Fi
    - Wireless Packet Sniffers
  - Step 6: Create Ad Hoc Associations with Unsecured AP
  - Step 7: Create a Rogue Access Point and Try to Create a Promiscuous Client
  - Step 8: Perform a Denial-of-Service Attack (De-authentication Attack)

- Step 9: Attempt Rapid Traffic Generation
- Step 10: Jam the Signal
    - Wi-Fi Jamming Devices
- Step 11: Attempt Single Packet Decryption
- Step 12: Perform Fragmentation Attack
- Step 13: Perform ARP Poisoning Attack
- Step 14: Try to Inject the Encrypted Packet
- Step 15: Crack Static WEP Keys
    - WEP Cracking Tool: Cain & Abel
    - WPA Cracking Tool: KisMAC
    - WPA Cracking Tool: WepDecrypt
- Step 16: Crack WPA-PSK Keys
    - WPA Brute Forcing Using Cain & Abel
    - WPA-PSK Cracking Tool: Elcomsoft Wireless Security Auditor
- Step 17: Check for MAC Filtering
- Step 18: Spoof MAC Address
- Step 19: Create a Direct Connection to the Wireless Access Point
- Step 20: Attempt MITM Attack

Wireless Penetration Testing Tools

- Aircrack-ng Suite

- Kismet
- WirelessMon
- AirMagnet WiFi Analyzer
- AirDefense
- WEPCrack
- MiniStumbler

23 MODULE-21: DENIAL-OF-SERVICE PENETRATION TESTING

- How Does a Denial-of-Service Attack Work?
- Distributed Denial-of-Service Attack
- How Do Distributed Denial-of-Service Attacks Work?
- Warning
- How to Conduct DoS Penetration Testing
    - Step 1: Test Heavy Loads on Server
        - Load Testing Tool: IxChariot
        - Load Testing Tool: StressTester
        - Load Testing Tool: Proxy Sniffer
        - Load Testing Tools
    - Step 2: Check for DoS Vulnerable Systems
        - DoS Vulnerability Scanner – GFI LanGuard
    - Step 3: Run SYN Attack on Server
    - Step 4: Run Port Flooding Attack on Server
    - Step 5: Run IP Fragmentation Attack on Server
    - Step 6: Run Ping of Death
    - Step 7: Run Teardrop Attack
    - Step 8: Run Smurf (Ping Flooding or ICMP Storm) Attack
    - Step 9: Run an Email Bomber on Email Servers
    - Step 10: Flood the Website Forms and Guestbook with Bogus Entries

- Step 11: Run Service Request Floods
- Step 12: Run Permanent Denial-of-Service Attacks
- Step 13: Run Peer-to-Peer Attacks
- Step 14: Test for SQL Wildcard Injection Attacks
- Step 15: Try to Log In to Customer Accounts
- Step 16: Test for Buffer Overflow Attacks That Result in Denial of Service
- Step 17: Test for DoS User-Specified Object Allocation
- Step 18: Test for User Input as a Loop Counter
- Step 19: Try to Generate Large Application Log Files
- Step 20: Test for Memory Allocation in Applications
- Step 21: Try to Store Too Much Data in Sessions
    - DDoS Attack Tool: LOIC
    - DoS Attack Tools

- Recommendations to Prevent Denial of Service

24 MODULE-22: STOLEN LAPTOP, PDAS AND CELL PHONES PENETRATION TESTING

- Stolen Digital Data
- Type of Information Lost in Laptop Theft
  - Strategic Information
  - Tactical Information
  - Network Information
  - Personal Information
- Penetration Testing Steps
  - Step 1: Look for the Laptop Login Password
  - Step 2: Check if the Sensitive Data Is Encrypted or Not in the Devices
  - Step 3: Perform Penetration Testing in Android Applications
    - Penetration Testing in Mobiles Using CORE IMPACT Pro
    - Tools to Extract the Personal Information in Cell Phones
  - Step 4: Perform PDA Penetration Testing
    - Pen-Testing Tools for the Pocket PC
    - Pen Testing for the Pocket PC Using MiniStumbler
  - Step 5: Look for Sensitive Information in the PDA or Laptop by Cracking MS Outlook
  - Step 6: Identify the Sensitive Data in Devices
  - Step 7: Look for Personal Information in the Stolen Laptop

- Step 8: Look for Passwords
- Step 9: Look for the Company's Infrastructure or Finance Documents
- Step 10: Extract the Address Book and Phone Numbers
- Step 11: Extract Schedules and Appointments
- Step 12: Extract Information from Applications Installed on These Devices
- Step 13: Extract Email Messages from These Devices
- Step 14: Check for the BIOS Password
- Step 15: Look into the Encrypted Files
- Step 16: Check Cookies in Web Browsers
    - Cookies Screenshot
    - Install Software
- Step 17: Attempt to Enable Wireless
    - Template

25 MODULE-23: SOURCE CODE PENETRATION TESTING

- Introduction
- Need for Source Code Penetration Testing
- Prerequisites for Source Code Penetration Testing
- Vulnerable Components in an Application
- Attacker's Goals
- Threat Models
- Application Decomposition
- Identify and Rank Threats
- Discover the Countermeasures and Mitigation
- Threat Analysis
- Steps for Source Code Penetration Testing
    - Step 1: Identify the Programming Language Used
    - Step 2: Determine the Application Architecture
        - Example
    - Step 3: Verify Input and Data Validations
    - Step 4: Verify Authentication
        - Step 4.1: Check for Strong Password Verification
    - Step 5: Check for Proper Authorization
    - STEP 6: Identify for Proper Session Management
        - Example for Checking Invalidated Session
    - STEP 7: Check for Cross Site Scripting Vulnerabilities

- Example for Cross Site Scripting

- Step 8: Check for SQL Injection Vulnerability
  - Example of SQL Injection
- Step 9: Check for Buffer Overflows and Overruns
  - Example of Buffer Overflow
- Step 10: Check for Vulnerabilities in Error Handling Mechanisms
- Step 11: Check for Secured Cryptography
- Step 12: Check for Secured Logging
  - Tools for Automated Source Code Penetration Testing for Java
  - Tools for Automated Source Code Penetration Testing for C, C++, and .NET

- STRIDE Threat Model Countermeasures
- Authentication Countermeasures
- Authorization Countermeasures
- Countermeasures for Data Validation
- Countermeasures for Error Handling
- Countermeasures for Session Management
- Countermeasures for Configuration Management and Data Protection
- Recommendations for Source Code Penetration Testing

26 MODULE-24: PHYSICAL SECURITY PENETRATION TESTING

- Physical Attacks
- Steps in Conducting Physical Security Penetration Testing
  - Step 1: Overview from Outside
  - Step 2: Map the Physical Perimeter
    - Google Maps Image
  - Step 3: Map the Possible Entrances
  - Step 4: Check Whether the Entry Points Are Guarded and Monitored
  - Step 5: Try to Bypass the Security Checks
  - Step 6: Attempt Lock Picking Techniques to Penetrate Locks Used by the Gates,
  - Door, and Closets
  - Step 7: Intercept and Analyze Guard Communication
  - Step 8: Check Physical Access Controls Implemented in the Facilities
  - Step 9: Test "After Office Hours" Entry Methods
  - Step 10: Check if CCTV and Motion Sensors Are Implemented
  - Step 11: Dress as a FedEx/UPS Employee and Try to Gain Access to the Building
  - Step 12: Attempt to Use Fake ID to Gain Access
  - Step 13 and Step 14

- Step 13: Attempt Piggybacking on Guarded Doors
- Step 14: Check Windows/Doors for Visible Alarm Sensors

- Step 15 and Step 16
  - Step 15: Attempt Dumpster Diving Outside the Company Trash Area
  - Step 16: Create a Map of the Company's Floor Plan
- Step 17: Use Active High Frequency Voice Sensors to Hear Private Conversation Among the Company's Staff
- Step 18: Find Vulnerable Fire Detection Systems
- Step 19 and Step 20
  - Step 19: Find Breach in Air Conditioning Systems
  - Step 20: Electromagnetic Interception
- Step 21 and Step 22
  - Step 21: Check for Receptionist/Guard Leaving Lobby
  - Step 22: Check for Accessible Printers in the Lobby – Print Test Page
- Step 23 and Step 24
  - Step 23: Obtain Phone/Personnel Listing from the Lobby Receptionist
  - Step 24: Listen to Employee Conversation in Communal Areas/ Cafeteria
- Step 25 and Step 26
  - Step 25: Check Areas for Sensitive Information
  - Step 26: Try to Shoulder Surf Users Logging On

- Step 27: Test if the Company Has a Physical Security Policy
- Step 28: Try to Enter into the Secure Rooms through Ceiling Space
- Step 29: Assess the Value of the Physical Assets
- Step 30: Check Access Authorization List
- Step 31: Check How These Documents Are Protected
- Step 32: Test if any Valuable Paper Documents Are Kept at the Facility
- Step 33: Test People in the Facility
- Step 34: Penetrate Server Rooms, Cabling, and Wires
- Step 35: Test for Radio Frequency ID (RFID)
- Step 36: Check for Active Network Jacks in Company Lobby and Meeting Rooms
- Step 37: Check for Sensitive Information Lying Around Meeting Rooms
- Step 38: Document Everything
    - Template

27 MODULE-25: SURVEILLANCE CAMERA PENETRATION TESTING

- Introduction to Surveillance Systems
- Pen Testing Requirements
- Surveillance Camera Network Architecture
- Need for Surveillance System Pen Testing
- Steps for Surveillance Camera Penetration Testing
    - Step 1: Check the Type of Surveillance Equipment Used
        - Surveillance Equipment
    - Step 2: Check whether Cameras Are Deployed in Critical Areas
    - Step 3: Check the Video Transmission Medium
    - Step 4: Attempt Tampering with the Wire/Wireless Connectivity to the Cameras
    - Step 5: Check the Bandwidth Available for the Surveillance Cameras
        - Try to Manipulate Resolution
        - Check the Compression
        - Check the Frame Rate
    - Step 6: Check the Settings of the Monitoring Computer
    - Step 7: Check Video Footage Clarity
    - Step 8: Attempt Changing Video Formats
    - Step 9: Scanning for Suspicious Device Drivers in Monitoring Computer
    - Step 10: Check the Video Viewing Options

- Step 11: Identify the Possible Threats while Integrating Video with Other Systems
- Step 12: Check if the Footage Storage Duration Meets the Organization's Requirements
- Step 13: Check the Optimization of DVR/NVR Storage
- Step 14: Check Network Settings of the DVR/NVR System
- Step 15: Check if All Connections Are Working Properly
- Step 16: Check Who Has Local and Remote Access to the DVR/NVR
- Step 17: Scan the Organization's Network Range to Detect DVR Systems
- Step 18: Check if Access to the DVR/NVR Is Protected
- Step 19: Try Cracking DVR/NVR Access Passwords

- Recommendations for Video Surveillance

28 MODULE-26: DATABSE PENETRATION TESTING

- Database Penetration Testing Steps
  - Step 1: Identify the Password Management in Oracle
    - McAfee Security Scanner for Databases
  - Step 2: Retrieve the Information about the Database via a Vulnerable Web Application
  - Step 3: Identify Execution of Public Privileges on Oracle
  - Step 4: Identify Privilege Escalation via Cursor Technique in Oracle
  - Step 5: Identify Public Privileges from Object Types
    - Oracle Auditing – Wrong Statements Logged
    - Possible Attacks Against Oracle Database Vault
  - Step 6: Identify Oracle Java Vulnerabilities in SQL Injection
  - Step 7: Determine Oracle Service ID (SID) Using Metasploit
  - Step 8: Determine Oracle Version Using Metasploit
  - Step 9: Identify Attack into Database Target DB by Using a Simulated User
  - Step 10: Scan for Default Ports Used by the Database
  - Step 11: Scan for Non-Default Ports Used by the Database
  - Step 12: Identify the Instance Names Used by the Database
  - Step 13: Identify the Version Numbers Used by the Database
  - Step 14: Attempt to Brute-Force Password Hashes from the Database

- Step 15: Sniff Database-related Traffic on the Local Wire
- Step 16: Microsoft SQL Server Testing
    - Step 16.1: Test for Direct Access Interrogation
    - Step 16.2: Scan for Microsoft SQL Server Ports (TCP/UDP 1433)
    - Step 16.3: Test for SQL Server Resolution Service (SSRS)
    - Step 16.4: Test for Buffer Overflow in the pwdencrypt() Function
    - Step 16.5: Test for Heap/Stack Buffer Overflow in SSRS
    - Step 16.6: Test for Buffer Overflows in the Extended Stored Procedures
    - Step 16.7: Test for Service Account Registry Key
    - Step 16.8: Test the Stored Procedure to Run Web Tasks
    - Step 16.9: Exploit SQL Injection Attack
        - SQL Injection Tool: BSQLHacker
    - Step 16.10: Blind SQL Injection
    - Step 16.11: Google Hacks
    - Step 16.12: Attempt Direct-Exploit Attacks
    - Step 16.13: Try to Retrieve the Server Account List
    - Step 16.14: Using OSQL, Test for Default/ Common Passwords
    - Step 16.15: Try to Retrieve the Sysxlogins Table
        - Try to Retrieve Sysxlogins Table Views
        - SQL Server System Tables

- Step 16.16: Brute-force SA Account
  - Oracle Server Testing
  - Port Scanning Basic Techniques
  - Port Scanning Advanced Techniques

- Step 17: Port Scan UDP/TCP Ports (TCP/UDP 1433)
  - Step 17.1: Check the Status of the TNS Listener Running at Oracle Server
    - Oracle TNS Listener: Screenshot
    - Finding the TNS Listener
    - Listener Modes
  - Step 17.2: Try to Log in Using Default Account Passwords
  - Step 17.3: Try to Enumerate SIDs
  - Step 17.4: Use SQL *Plus to Enumerate System Tables

- Step 18: MySQL Server Database Testing
  - Step 18.1: Port Scan UDP/TCP Ports (TCP/UDP)
  - Step 18.2: Extract the Version of the Database Being Used
  - Step 18.3: Try to Log in Using Default/ Common Passwords
  - Step 18.4: Brute-force Accounts Using Dictionary Attack
  - Step 18.5: Extract System and User Tables from the Database
    - Database Password Cracking Tool: Cain & Abel

- Database Password Cracking Tool: SQLdict
- Database Penetration Testing Tool: Oracle TNS Password Tester
- Database Vulnerability Assessment Tool: AppDetectivePro
- Database Vulnerability Assessment Tool: NGS SQuirreL
- Database Penetration Testing Tool: Secure Oracle Auditor (SOA)
- Database Penetration Testing Tool: Oracle Default Password Tester
- Database Penetration Testing Tool: Oracle Access Rights Auditor
- Database Password Cracking Tools
- Database Penetration Testing Tools
- Recommendations for Securing Databases

29 MODULE 27: VOIP PENETRATION TESTING

- Vulnerability Assessment
- Penetration and Vulnerability Testing
- VoIP Risks and Vulnerabilities
- VoIP Security Threat
- VoIP Penetration Testing Steps
    - 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 and 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 9.1: TCP SYN Scan
        - Step 9.2: UDP Scan
    - 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 the SIP Server
- Step 15: Test for Enumerating TFTP Servers
- Step 16: Test for SNMP Enumeration
    - SNMP Enumeration Tools
- Step 17: Test for Sniffing TFTP Configuration Files Transfers
- Step 18: Test for Number Harvesting and Call Pattern Tracking
    - VoIP Sniffing Tool: Netdude
    - VoIP Sniffing Tools
    - VoIP Scanning Tool: SNScan
    - VoIP Scanning Tools
    - VoIP Packet Creation and Flooding Tools
    - VoIP Signaling Manipulation Tools
    - VoIP Fuzzing Tools/VoIP Media Manipulation Tools

Recommendations for VoIP Penetration Testing

30 MODULE 28: VPN PENETRATION TESTING

- Virtual Private Network (VPN)
- VPN Penetration Testing Steps
  - Step 1: Check the Target Organization's VPN Security Policy
  - Step 2: Scanning
    - Step 2.1: Scanning - 500 UDP IPsec
    - Step 2.2: Scanning - 1723 TCP PPTP
    - Step 2.3: Scanning - 443 TCP/SSL
- Port Scanning Tools
  - SuperScan
  - Advanced Port Scanner
    - Step 2.4: Scanning - Ipsecscan xxx.xxx.xxx.xxx-255
  - Step 3: Fingerprinting
    - Step 3.1: Get the IKE Handshake
    - Step 3.2: UDP Backoff Fingerprinting
    - Step 3.3: Vendor ID Fingerprinting
    - Step 3.4: Check for IKE Aggressive Mode
  - Step 4: Test for Default User Accounts and Passwords
  - Step 5: Check for Unencrypted User Names in a File or the Registry
  - Step 6: Test for Plain-text Password

- Step 7: Perform User Name Enumeration
- Step 8: Check Account Lockout in VPN
    - Check for Split Tunneling
- Step 9: Audit VPN Traffic
    - Try to Recover and Decrypt Pre-Shared Key (PSK)
- Step 10: Check for Proper Firewalling in VPN
- Step 11: Check Denial-of-Services in VPN
    - SSL VPN Scan Tool: ike-scan
    - SSL VPN Scan Tool: IKEProbe and IKECrack
    - SSL VPN Scan Tool: VPNmonitor

- Recommendations for VPN Connection

31 MODULE 29: CLOUD PENETRATION TESTING

- What Is Cloud Computing?
- Cloud Computing Model
- Types of Cloud Computing Services
- Separation of Responsibilities in Cloud
- Security Benefits of Cloud Computing
- Security Risks Involved 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 Cloud for Resource Isolation
    - Step 5: Check if Anti-malware Applications Are Installed and Updated on Every Device
    - Step 6: Check if Firewalls Are Installed at Every Network Entry Point
    - Step 7: Check if Strong Authentication Is Deployed for Every Remote User
    - Step 8: Check if File Transfers to/from Cloud Servers Are Encrypted
    - Step 9: Check if Files Stored on Cloud Servers Are Encrypted
    - Step 10: Check Data Retention Policy of Service Providers
    - Step 11: Check if All Users Follow Safe Internet Practices

- Step 12: Perform a Detailed Vulnerability Assessment
- Step 13: Check Audit and Evidence-gathering Features in Cloud Service
- Step 14: Perform Automated Cloud Security Testing

- Recommendations for Cloud Testing

32 MODULE 30: VIRTUAL MACHINE PENETRATION TESTING

- Introduction to Virtualization
- Prerequisites to Virtual Machine Pen Testing
- Virtualization Security Scenario
- Virtualization Security Issues
- Virtual Environment Pen Testing
- Virtual Machine Penetration Testing Steps
    - Step 1: Scan for Virtual Environments
    - Step 2: Search for Virtual Environments
    - Step 3: Check if a Documented Policy Exists for Creating New Virtual Machines
    - Step 4: Create Inventory of Virtual Machines
    - Step 5: Check Patch Status of Host and Guest Operating Systems
    - Step 6: Check VM Configuration for Unused Emulated Hardware
    - Step 7: Check IP Addressing Information on Virtual NICs
    - Step 8: Check the Network Bandwidth Limit per VM
    - Step 9: Check Virtual Switches for Promiscuous Mode
    - Step 10: Perform Virtual Machines Stress Testing
    - Step 11: Try to Exploit Hypervisors Using Automated Exploit Tools
    - Step 12: Try to Break Out of Guest VM
    - Step 13: Perform Vulnerability Assessment of Virtual Environment

- Vulnerability Assessment Tool: VMinformer
- Configuration Management Tool: Virtualization Manager
- Configuration Management Tool: Tripwire
- Virtualization Assessment Toolkit: VASTO

- Virtualization Best Practices

33 MODULE 31: WAR DIALING

- War Dialing
- War Dialing Techniques
- Why to Conduct a War Dialing Pen Test
- War Dialing Penetration Testing Steps
  - Step 1: Information Gathering
  - Step 2: Pre-Requisites for War Dialing Penetration Testing
  - Step 3: Software Selection for War Dialing
  - Step 4: Configuring Different War Dialing Software
  - Step 5: Identification of (War Dialing) Vulnerabilities
  - Step 6: Assessment of Vulnerabilities
  - Step 7: Reporting
- Recommendations to Improve Modem Security
- War Dialing Tool: THC-Scan
- Intelligent War Dialer: iWar
- War Dialing Tool: ToneLoc
- War Dialing Tools

34 MODULE 32: VIRUS AND TROJAN DETECTION

- What Is a Trojan/Virus?
- Indications of a Trojan Attack
- Indications of a Virus Attack
- Different Ways a Trojan/Virus Can Get into a System
- How Does a Computer Get Infected by a Trojan/Virus?
- Steps for Detecting Trojans and Viruses
  - Step 1: Check for Suspicious Open Ports
    - Netstat: Screenshot
    - Port Monitoring Tools: TCPView and CurrPorts
    - Port Monitoring Tool: IceSword
  - Step 2: Check Windows Task Manager
  - Step 3: Scan for Suspicious Running Processes
    - Process Monitoring Tools
  - Step 4: Scan for Suspicious Registry Entries
    - Registry Entry Monitoring Tools
  - Step 5: Scan for Suspicious Device Drivers
    - Device Drivers Monitoring Tool: DriverView
    - Device Drivers Monitoring Tools
  - Step 6: Scan for Suspicious Windows Services
    - Windows Services Monitoring Tool: Process Hacker

- Step 7: Scan for Suspicious Startup Programs
    - Windows 7 Startup Registry Entries
    - Startup Programs Monitoring Tools
- Step 8: Scan for Suspicious Files and Folders
    - File and Folder Integrity Checkers: FastSum and WinMD5
    - File and Folder Integrity Checkers
- Step 9: Scan for Suspicious Network Activity
    - Detecting Trojans and Viruses with Capsa Network Analyzer
- Step 10: Check Whether Anti-Virus and Anti-Trojan Programs Are Working
- Step 11: Detect the Boot-Sector Virus
- Step 12: Use HijackThis to Scan for Spyware

- Anti-Trojan/Anti-Spyware Tool
    - Emsisoft Anti-Malware
    - TrojanHunter and Ad-Aware Pro
- Anti-Trojan/Anti-Spyware Tools
- Anti-Virus Tools: BitDefender Antivirus Plus 2012 and AVG Anti-Virus 2013
- Anti-Virus Tools
- Trojan Countermeasures
- Virus and Worms Countermeasures

35 MODULE 33: LOG MANAGEMENT PENETRATION TESTING

- Introduction
- Need for Log Management
- Challenges in Log Management
- Steps for Log Management Penetration Testing
  - Step 1: Add a New Line/Plain Text into the Log Files
  - Step 2: Add Separators (Single Pipe/Multiple Pipe Characters) into the Log Files
  - Step 3: Timestamp Injection
  - Step 4: Wrapping Words and Creating Unusual Log Entries
  - Step 5: Add HTML Tags into a Log (HTML Injection)
  - Step 6: Check the Log Viewing Interface (Terminal Injection)
  - Step 7: Scan for Log Files
  - Step 8: Try to Flood Syslog Servers with Bogus Log Data
  - Step 9: Try Malicious Syslog Message Attack (Buffer Overflow)
  - Step 10: Perform Man-in-the-Middle Attack
  - Step 11: Check Whether Logs Are Encrypted
  - Step 12: Check Whether Arbitrary Data Can Be Injected Remotely into the Microsoft ISA Server Log File (Only for Microsoft ISA Server)
  - Step 13: Perform DoS Attack Against the Check Point FW-1 Syslog Daemon (Only for Check Point Firewall)

- Step 14: Send Syslog Messages Containing Escape Sequences to the Syslog Daemon of Check Point FW-1 NG FP3 (Only for Check Point Firewall)

- Log Management Tools
  - GFI EventsManager
  - GFI EventsManager Screenshot
- Log Monitoring Tools
  - EventLog Analyzer
  - ELM Event Log Monitor
  - Lepide Event Log Manager
  - EventSentry
  - EventTracker Enterprise
  - EventReporter
- Checklist for Secure Log Management

36 MODULE 34: FILE INTEGRITY CHECKING

- File Integrity Checking
- Steps for Checking File Integrity
  - Step 1: Manually Check the File Properties/Attributes
  - Step 2: Check Integrity by Opening/ Unzipping the File
  - Step 3: Check for Integrity by Comparing CRC Checksum
    - Process to Check Integrity by Comparing CRC Checksum
    - Checking and Comparing CRC Value in Linux
    - Checking and Comparing CRC Value in Windows
  - Step 4: Check for Integrity by Comparing Hash Value
    - Hash Value Calculator: SlavaSoft HashCalc
    - Hash Value Calculator: HashMyFiles
    - Hash Value Calculation Tools
- Automated File Integrity Verification Tools
  - nCircle File Integrity Monitor
  - Verisys File Integrity Monitoring System
- Challenges in File Integrity Checking
- Recommendations

37 MODULE 35: MOBILE DEVICES PENETRATION TESTING

- Why Mobile Device Penetration Testing?
- Requirements for Mobile Device Penetration Testing
- Mobile Devices Market Share
- Penetration Testing Android-based Devices
- Pen Testing Android
- Android Architecture
- Penetration Testing Steps for Android-based Devices
    - Step 1: Try to Root an Android Phone
        - Rooting Android Using Superboot
    - Step 2: Try to Install Malicious Apps without User's Approval
    - Step 3: Perform a DoS Attack on Android Phone
    - Step 4: Check for Vulnerabilities in the Android Browser
    - Step 5: Check for Vulnerabilities in SQLite
    - Step 6: Check for Vulnerabilities in Intents
    - Step 7: Check for Android Wi-Fi Vulnerability
    - Step 8: Use the "Woodpecker" Tool to Detect Capability Leaks in Android Devices
    - Best Practices for Android-based Devices
- Penetration Testing iOS-based Devices
- iOS Architecture
- Major iOS Vulnerabilities and Attacks

- Jailbreaking
- Penetration Testing Steps for iOS-based Devices
    - Step 1: Try to Jailbreak the iPhone
        - Jailbreaking Using iFuntastic
    - Step 2: Try to Unlock the iPhone
    - Step 3: Try to Activate the Voicemail Button on Your Unlocked iPhone
    - Step 4: Try to Bypass the Smart Cover
    - Step 5: Exploit Siri to Get Unauthorized Access
    - Step 6: Try to Hack the iPhone Using Metasploit
    - Step 7: Check for an Access Point with the Same Name and Encryption Type
    - Step 8: Check iOS Device Data Transmission on Wi-Fi Networks
    - Step 9: Check Whether the Malformed Data Can Be Sent to the Device
    - Step 10: Check for Code Signing Vulnerabilities on iOS Devices
    - Step 11: Check Whether Hardware Encryption/Backup Recovery Can Be Done
    - Best Practices for iOS-based Devices
- Penetration Testing BlackBerry-based Devices
- BlackBerry Network Architecture
- Vulnerabilities in BlackBerry
- Penetration Testing Steps for BlackBerry-based Devices
    - Step 1: Try Blackjacking on the BlackBerry

- Step 2: Perform a Metaspolit Exploit with Blackjacking
- Step 3: Try IDS Evasion on the BlackBerry Enterprise Network
- Step 4: Perform DNS Spoofing
- Step 5: Check for Flaws in the Application Code Signing Process
- Step 6: Use Trojans to Extract Information
- Step 7: Perform a DoS Attack
- Step 8: Check for Vulnerabilities in the BlackBerry Browser
- Step 9: Check for Flaws in Attachment Services
- Step 10: Try to Attack by Sending TIFF Image Files
- Step 11: Search for Password-protected Files in BlackBerry Devices
- Best Practices for BlackBerry-based Devices

- Penetration Testing Bluetooth Connections
- Introduction to Bluetooth Devices
- Bluetooth Stack
- Penetration Testing Steps for Bluetooth-enabled Devices
  - 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
- Step 10: Try a BlueBug Attack
- Step 11: Try a BlueSpam Attack
- Step 12: Try Denial-of-Service Attacks
- Best Practices for Bluetooth Connections

Recommendations

- Mobile Devices Best Practices

38 MODULE 36: TELECOMMUNICATION AND BROADBAND COMMUNICATION PENETRATION TESTING

- Broadband Communication
- Risks in Broadband Communication
- Steps for Broadband Communication Penetration Testing
  - Step 1.1: Check Whether the Firewall Device Is Installed on the Network
  - Step 1.2: Check Whether Personal and Hardware Firewalls Are Installed
  - Step 1.3: Check Whether These Firewalls Prevent Intruders or Detect Any Rogue Software
  - Step 1.4: Check Whether the Logging is Enabled on the Firewall
  - Step 1.5: Check Whether the Firewall Is in Stealth Mode
  - Step 2.1: Check Whether the Browser Has Default Configuration
  - Step 2.2: Check for the Browser Plug-ins
  - Step 2.3: Check Whether the Active Code Is Enabled
  - Step 2.4: Check Whether the Browser Version Is Updated
  - Step 2.5: Check Whether Cookies Are Enabled
    - Cookies Analysis Tool: IECookiesView
  - Step 2.6: Check Whether the Scripting Languages Are Enabled
  - Step 3.1: Check Whether the 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 4.1: Check for VPN Policy Configurations
- Step 4.2: Try for Wiretapping
- Step 4.3: Try to Perform Wardriving
    - Wardriving Tools
- Step 4.4: Check Whether the Wireless Base Station Is in Default Configuration
- Step 4.5: Check Whether WEP Is Implemented
- Step 4.6: Try to Crack the WEP Key
    - WEP Cracking Tools
- 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

39 MODULE 37: EMAIL SECURITY PENETRATION TESTING

- Introduction to Email Security
- Commonly Used Email Service Protocols
- Prerequisites for Email Penetration Testing
- Steps for Email Penetration Testing
    - Step 1: Perform SMTP Service Fingerprinting
    - Step 2: Perform Directory Harvest Attacks
    - Step 3: Enumerate Enabled SMTP Subsystems and Features
    - Step 4: Perform SMTP Password Brute-Forcing
    - Step 5: Perform NTLM Overflows Attack Through SMTP Authentication
    - Step 6: Test for SMTP Open Relay
        - SMTP Enumeration Tool: NetScanTools Pro
    - Step 7: Perform SMTP User Enumeration
    - Step 8: Perform POP3 Password Brute-Forcing
    - Step 9: Perform IMAP Brute-Forcing
    - Step 10: Test for IMAP Process Manipulation Attack
    - Step 11: Check for Known Vulnerabilities in Mail Servers and Hosts
        - Vulnerability Scanning Tool: Netsparker
        - Vulnerability Scanning Tool: SAINT
        - Vulnerability Scanners

- Step 12: Check the Patch Status of Mail Servers and Hosts
    - Patch Management Tool: GFI LanGuard
    - Patch Management Tools
- Step 13: Try to Crack Email Passwords
- Step 14: Check Whether Anti-Phishing Software Is Enabled
    - Anti-Phishing Tool: Netcraft
    - Anti-Phishing Tools
- Step 15: Check Whether Anti-Spamming Tools Are Enabled
    - Common Spam Techniques
    - Anti-Spamming Tools: GFI MailEssentials
    - Anti-Spamming Tools: Spamihilator
    - Anti-Spamming Tools
- Step 16: Try to Perform Email Bombing
- Step 17: Perform CLSID Extension Vulnerability Test
- Step 18: Perform VBS Attachment Vulnerability Test
- Step 19: Perform Double File Extension Vulnerability Test
- Step 20: Perform Long File Name Vulnerability Test
- Step 21: Perform Malformed File Extension Vulnerability Test
- Step 22: Perform Access Exploit Vulnerability Test
- Step 23: Perform Fragmented Message Vulnerability Test

- Step 24: Perform Long Subject Attachment Checking Test
- Step 25: Perform No File Attachment Vulnerability Test

- Recommendations for Email Security Penetration Testing

40 MODULE 38: SECURITY PATCHES PENETRATION TESTING

- Patch Management
- Patch and Vulnerability Group (PVG)
- Steps for Security Patches Penetration Testing
  - Step 1: Check if the Organization Has a PVG in Place
  - Step 2: Check Whether the Security Environment Is Updated
  - Step 3: Check Whether the Organization Uses Automated Patch Management Tools
  - Step 4: Check the Last Date/Timing Process of Patch Management
  - Step 5: Check the Patches on Non-Production Systems
  - Step 6: Check the Vendor Authentication Mechanism
  - Step 7: Check the Probability of Patches Containing Malicious Code
  - Step 8: Check for Dependency of New Patches
  - Step 9: Check the Compliance of Change Management
- Security Patches Penetration Testing Tools
  - Patch Management Tools: Ecora Patch Manager
  - Patch Management Tool: GFI LanGuard
  - Patch Management Tool: Desktop Central
  - Patch Management Tools
- Recommendations for Sound Patch Management Process

41 MODULE 39: DATA LEAKAGE PENETRATION TESTING

- Data Leakage
- Data Leakage Statistics
- Data Leakage Statistics – Types of Incidents
- How Data Can Be Leaked
- What to Protect?
- Data Leakage Penetration Testing Steps
  - 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 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 the 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 the 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

42 MODULE 40: SAP PENETRATION TESTING

- SAP World
- Introduction to SAP Penetration Testing
- The SAP RFC Library
- Methodology and Goals
- Setting Up the Assessment Platform
- Sapyto: An SAP Penetration Testing Framework
- Sapyto Architecture
- Connectors and Targets
  - Plugins
  - Shells
  - SapytoAgents
- Installation of Sapyto on Windows
- Installation of Sapyto on Linux
- Using Sapyto
  - The Console Interface
  - Plugin Configuration and Selection of Sapyto
- SAP Penetration Testing
  - Discovery Phase
  - Exploration Phase
  - Exploration Phase: Discovering Available Clients
  - Vulnerability Assessment Phase

- Exploitation Phase

- Recommendations for SAP Penetration Testing

43 MODULE 41: STANDARDS AND COMPLIANCE

- Incident Handling
- Incident Response
- Need for Incident Response
- Goals of Incident Response
- Parameters of Investigations
- Laws
- GLBA Compliance Checklist
- HIPAA Compliance Checklist
- Sarbanes-Oxley Compliance Checklist
- FISMA Compliance Checklist
- FERPA Compliance Checklist
- Intellectual Property Rights
- Privacy Act
- ECPA Compliance Checklist
- Standards of Conduct
- Legal Issues Affecting Information Assurance

44 MODULE 42: INFORMATION SYSTEM SECURITY PRINCIPLES

- Defense in Depth
- Examples of Defense in Depth
- System Interconnection
- Monitoring Systems Interconnection
- System Interconnection Policy
- Aggregation
- Inference and Object Reuse
- Polyinstantiation
- Security Affected by Assurance and Confidence
- Security Affected by Covert Channels
- Security Affected by Countermeasures
- Security Affected by Emanations
- Security Affected by Maintenance Hooks and Privileged Programs
- Security Affected by Resource Misuse Prevention
- Security Affected by States Attack (e.g., Time of Check/Time of Use)
- Security Affected by Timing Attacks
- Threat from Aggregation
- Basic Security Requirements
- Information Valuation
- States of Information
- Protection Profiles
- Security Target
- Account Management

- Account Management Principles
- Security Policy for Account Administration
- Peer-to-Peer Security
- Peer-to-Peer Security Policy
- Configuration Management
- Configuration Management Requirements
- Steps for Configuration Management Training
- Steps for Configuration Management Training to SA/Staff
- Change Control
- Steps Involved in Change Control Process
- Change Control Process
- Configuration Management Plan
- Monitoring Configuration Plan Training
- Cryptanalysis
- Digital Signature
- Steganography and Watermarking
- Non-Repudiation
- Message Digest
- Message Digest Tools
- Key Management
- Electronic Key Management System (EKMS)
- EKMS Requirements
- Public Key Infrastructure (PKI)
- Need for Public Key Infrastructure (PKI)
- Public Key Infrastructure Requirements
- Email Security

- Key Escrow
- Life Cycle Security
- System Security Plan (SSP)
- Life Cycle Security Planning
- Incorporating Life Cycle Security Planning in Information Systems
- Monitoring Life Cycle Security Acquisition Process
- Life Cycle Security Plan
- Access Control Models
- Business Aspects of Information Security
- Information Warfare (INFOWAR)
- Intellectual Property Rights
- COMSEC
- COMSEC Policy
- System Security Authorization Agreement (SSAA)
- System Security Architecture
- Software Piracy
- Addressing Account Management
- Policy for Redeploying Classified Systems
- Hardware Asset Management Program
- Key Management Infrastructure (KMI)
- Development of Configuration Control Policies
- Assess the System Configuration Control Plan
- Report to the DAA the Deficiencies/Discrepancies in the Configuration Control Policy
- Improvements to the Security Plans Developed by Site Personnel
- Security Domains

- Administrative Security Procedures Appropriate for the System Certification
- Security Features Necessary to Support Site Operations
- Maintenance Procedures to Ensure Security against Unauthorized Access
- Procedures to Counter Potential Threats from Insiders or Outsiders of the Organization
- Physical Security
- How the System Handles Error Conditions
- Principles of Information Security
- Practices of Information Security

45 MODULE 43: INFORMATION SYSTEM INCIDENT HANDLING AND RESPONSE

- EMSEC/TEMPEST
- Emergency/Incident Response Team
- Education, Training, and Awareness (ETA)
- ETA Policy
- Contingency Plan
- Contingency Planning Considerations
- Write Contingency Plan
- Present Contingency Plan
- Concept of Operations (CONOP)
- Concept of Operations Policy
- Information Covered by CONOP
- Business Continuity Plan (BCP)
- Business Organization Analysis
- Disaster Recovery Planning (DRP)
- Business Continuity Plan Development and Planning
- Resource Requirements for Business Continuity Plan
- Security Policy for Backup Procedures
- Backup Plan
- Business Resumption Plan
- Communication Plan
- Documentation Plan
- Emergency Response Plan
- Fire Protection Plan

- Personnel Notification Plan
- Develop Recovery Strategy
- Develop Contingency Plan
- Contingency Plan Training
- Reconstitution Process
- Recovery Process
- Develop Business Continuity Plan
- Security Policy
- Criminal Prosecution
- Due Care
- Generally Accepted Systems Security Principles (GASSP)
- Industrial Security
- Security Awareness for Users of the Information System
- Security Awareness Plan for Users of the Information System
- Security Education
- Security Training for Information System Users
- Personal Information Security Breaches
- Investigation of Personal Information Security Breaches
- Role-Based Access Control
- Unauthorized Access Attempts
- Train Staff to Get Unauthorized Access
- Security Incident Investigation Process
- Rules of Evidence Acceptability
- Evidence Collection and Preservation
- Security Incident Reporting
- Process of Responding to and Reporting Security Incidents

- Computer Incident Reporting Form
- Agency Specific Security Policies and Procedures

46 MODULE 44: INFORMATION SYSTEM AUDITING AND CERTIFICATION

- Certification and Accreditation
- Common Criteria (CC)
- Common Criteria Key Concepts
- National Information Assurance Partnership (NIAP)
- Information Technology Security Evaluation Criteria (ITSEC)
- International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799
- Discuss the Concepts of Availability, Integrity, Confidentiality, Authentication, and Non- repudiation
- Security Models
- Confidentiality Models (Bell-La Padula Model)
- Integrity Models (Clark-Wilson)
- Integrity Models (Biba)
- Information Flow Models
- Components of Information Systems Evaluation Models
- Key Participants of the Certification and Accreditation Process
- Protection Profiles
- Protection Profile Policy
- Validated Products
- Audit Collection Requirements
- Audit Policy
- Information System Security Auditing and Logging
- Information System Security Auditing Policy

- Information Systems Security Auditing Plan
- Steps for Training Given to Auditing and Logging Management Personnel
- Audit Trails
- Information Systems Monitoring Process
- Information Systems Monitoring Policy
- Steps for Training Given to Monitoring Management Personnel
- Certification Advocacy Group
- Approval to Operate
- Evaluation Assurance Levels (EALs)
- Need for System Certification
- Waive Policy to Continue Operation
- Need-to-Know Control
- Auditing Report
- Assessment Use During Certification of Information Systems
- Post Accreditation
- Systems Security Plan (SSP)
- Systems Security Plan for Simple Information System
- C&A Accreditation Objects
- Certification and Accreditation Process for Information System
- Certification Statement
- Interim Approval to Operate (IATO)
- Re-certification and Re-accreditation
- Security Test and Evaluation (ST&E)
- Security Test and Evaluation Plan
- Example of Security Test and Evaluation Report
- System Security Authorization Agreement (SSAA)

- Contents of SSAA
- Documentation Policies of SSAA
- Type Accreditation
- Security Disciplines
- Steps to Understand Mission
- Understand Mission Risk
- System Certification Memorandum of Understanding (MOU)
- Criteria for Personnel Selection for Certification Team
- Roles and Responsibilities of Certification Team
- Certification Process Boundaries
- Setting Certification Process Boundaries
- Budget/Resources Allocation/ Scheduling
- Information System Security Certification Requirements
- System Architectural Description Document
- Agency-specific C&A Guidelines
- Steps to Audit the Information System to Perform Certification Analysis
- Security Processing Mode
- Change Control Management Process
- Change Control Policies
- Accreditation Decision
- Security Accreditation Package
- Life Cycle Security Planning