Certified Penetration Testing Professional

Course Outline

Module 01: Introduction to Penetration Testing and Methodologies

Penetration Testing Concepts

- What is Penetration Testing?
- Benefits of Conducting a Penetration Test
- Penetration Testing Service Delivery Models: Conventional vs. Next Generation
- ROI for Penetration Testing
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
- Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented
- Strategies of Penetration Testing
  - Black-box Penetration Testing
  - White-box Penetration Testing
  - Gray-box Penetration Testing
- Penetration Testing: Cost and Comprehensiveness
- Selection of Appropriate Testing Type
- Different Methods of Penetration Testing
- Selecting the Appropriate Method of Penetration Testing
- Common Areas of Penetration Testing
- Penetration Testing Process
- Penetration Testing Phases
- Penetration Testing Methodologies
  - Need for a Methodology

LPT Penetration Testing Methodology

- EC-Council's LPT Methodology
- Qualities of a Licensed Penetration Tester
  - Modus Operandi
  - Preparation

Guidelines and Recommendations for Penetration Testing

- Characteristics of a Good Penetration Test
- When should Pen Testing be Performed?
- Ethics of a Penetration Tester
- Evolving as a Penetration Tester
- Qualification, Experience, Certifications, and Skills Required for a Pen Tester
  - Communication Skills of a Penetration Tester
  - Profile of a Good Penetration Tester
  - Responsibilities of a Penetration Tester
- Risks Associated with Penetration Testing
  - Types of Risks Arising from Penetration Testing
  - Addressing Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions

Module 02: Penetration Testing Scoping and Engagement

- Penetration Testing: Pre-engagement Activities

Request for Proposal

- Initiation of a Pen Testing Engagement Process
- Proposal Submission
- Common Evaluation Criteria for Proposals

Preparing Response Requirements for Proposal Submission

- Preparing for Proposal Submission
  - Identifying Scope, Approach, and Methodology
    - Sending a Preliminary Information Request Document to the Client
    - Listing the Goals of Penetration Testing
    - Scoping the Penetration Test

- Pen Test Scoping Meeting
- Sample Questionnaires
- Identifying the Types of Penetration Testing Assessment to Perform
- Identifying the Testing Strategy
- Identifying the Areas of Infrastructure to Test
- Identifying the Targets to Test
  - ✓ Identifying the Internal/External Targets to Test Within/Outside the Organization
  - ✓ Identifying any Targets that Require Dealing with Third Parties
  - ✓ Identifying any Targets that Require Dealing with Other Countries
- Understanding Client Assessment Requirements
- Listing Tests That Will Not be Performed
  - ✓ Obtaining a Detailed Proposal of Tests to Conduct and Not Conduct
- Deciding on the Desired Depth for Penetration Testing

o Determining Project Deliverables

- Identifying How the Final Report will be Delivered
- Identifying the Reports to Deliver after the Pen Test

o Determining the Project Schedule

- Specifying the Test Duration

o Understanding Staffing Requirements

- Project Team Staffing

o Proposing Detailed and Itemized Pricing

- Estimating the Cost of the Pen Test Engagement

o Submitting the Proposal

Setting the Rules of Engagement

- Rules of Engagement
- Brainstorming Sessions with the Top Management and Technical Teams

Establishing Communication Lines

- Listing Contacts at the Client Organization in Charge of the Pen Testing Project
- Obtaining the Details of Personnel to Contact at the Client Organization in Case of an Emergency

- Points-of-Contact Template
- Initial Teleconference with Target Point of Contact

Timeline

- Estimating the Timeline for the Engagement
- Metrics for Time Estimation
- Drafting a Timeline for the Pen Testing Project
- Work Breakdown Structure or Task List
- Penetration Testing Schedule

Time/Location

- Identify the Reporting Time Scales
- Identifying the Office Space/Location where the Team will Work

Frequency of meetings

- Meeting with the Client

Time of Day

- Deciding the Time of Day for the Test

Identifying Personnel for Assistance

- Identifying the Local Human Resources Required for the Pen Test
- Identifying the Client's IT Security Admin
- Selecting Other Internal Employees
- ROE Document
  - XSECURITY: Sample ROE Document
  - Sample ROE Template
- Obtaining the Engagement Letter from the Client

Handling Legal Issues in Penetration Testing Engagement

- Hiring a Lawyer
- Penetration Testing Contract
  - Drafting Contracts
  - Sample Penetration Testing Contract
- Penetration Testing "Rules of Behavior"
- Create a Get-Out-of-Jail-Free Card
- Listing the Permitted Items in the Legal Agreement

- Confidentiality and Nondisclosure Agreement Clauses
- Preparing a Nondisclosure Agreement and Having the Client Sign
- Defining Liability Issues
- Defining a Negligence Claim
- Defining Contract Limitations
- Having the Engagement Letter Vetted by a Lawyer
- Obtaining Liability Insurance from a Local Insurance Firm
- Independence Check of Team Members
- Listing Known Waivers/Exemptions
- Listing Contractual Constraints in the Penetration Testing Agreement

Preparing for the Test

- Reviewing the Engagement Letter
- Creating an Engagement Log
- Kickoff Meeting
- Preparing a Statement of Work
- Identifying the Security Tools Required for the Penetration Test
- Identifying Hardware and Software Configurations Required for the Penetration Test
- Preparing the Test Plan
  - Test Plan
  - Content of a Test Plan
  - Building a Penetration Test Plan
  - Test Plan Identifier
  - XSECURITY: Test Plan Checklist
- Penetration Testing Hardware/Software Requirements
- Assign Resources
- Sending Internal Control Questionnaires to the Client
- Requesting for Previous Penetration Testing/Vulnerability Assessment Reports
- Creating a Data Use Agreement
- Working Teleconference
- Sending the Final Engagement Control Documents to the Client for Signature
- Obtaining the Penetration Testing Permission from the Company's Stakeholders

- Obtaining Special Permission from the Local Law Enforcement Agency
- Obtaining Temporary Identification Cards from the Client for Team Members Involved in the Process
- Gathering Information on the Client Organization's History and Background
- Visiting and Becoming Familiar with the Client Organization's Premises and Environment
- Identifying the Local Equipment Required for the Pen Test
- Mission Briefing

Handling Scope Creeping During Pen Testing

- Scope Creeping

Module 03: Open Source Intelligence (OSINT)

OSINT through the WWW

- Finding the Domain and Sub-domains of the Target
  - Finding Similar or Parallel Domain Names
- Refining Web Searches using Advanced Operators
- Footprinting the Target using Shodan
- Finding the Geographical Location of a Company
- Listing Employees and their Email Addresses
  - Identifying Key Email Addresses through Email Harvesting
  - Enumerating Key Email Addresses from Pastebin and HaveIBeenPwned
- Listing Key Personnel of the Company
- Using People Search Online Services to Collect Information
- Browsing Social Network Websites to Find Information on the Company and Employees
- Using Web Investigation Tools to Extract Sensitive Data about the Company
- Identifying the Type of Network Devices used in the Organization
- Looking for Sensitive Information in Email Headers
- Looking for Valuable Information in NNTP Usenet Newsgroups
- Other Useful Footprinting Activities to Find Information about the Target

OSINT through Website Analysis

- Searching for Contact Information, Email Addresses, and Telephone Numbers from the Company Website
- Searching for Web-page Posting Patterns and Revision Numbers

- Searching Archive.org for Old Information about the Company
- Monitoring Web Updates using WebSite-Watcher
- Examining the HTML Source of Web Pages

OSINT through DNS Interrogation

- Performing Whois Lookups
- Finding the IP Address Block Allocated to the Organization
- Finding the DNS Records for the Domain
- Performing Reverse Lookups
- Performing DNS Zone Transfer
- Drawing a Network Diagram using Traceroute Analysis
    - Creating a Topological Map of the Network

Automating the OSINT Process using Tools/Frameworks/Scripts

- Maltego
- FOCA
- Fsociety
- PENTMENU
- Document the Result

Module 04: Social Engineering Penetration Testing

Social Engineering Penetration Testing Concepts

- Social Engineering Penetration Testing: An Overview
- Skills Required to Perform Social Engineering Pen Test
- Black-Box or White-Box Testing?
- Social Engineering Penetration Testing Modes
- Social Engineering Penetration Testing Process
    - Step 1: Test Planning and Scoping
        - Do Remember: Before Social Engineering Pen Test
    - Step 2: Target Identification
    - Step 3: Penetration Testing Attempts

Social Engineering Penetration Testing Using E-mail Attack Vector

- Attempt Social Engineering Using Email

- Example of Social Engineering Using Email
- Attempt Social Engineering Using Phishing
  - Examples of Phishing Emails
- Attempt Social Engineering Using Spear Phishing
- Attempt Social Engineering Using Whaling
- Attempt Social Engineering Using Pharming
- Launch a Phishing Campaign

Social Engineering Penetration Testing Using Telephone Attack Vector

- Attempt Social Engineering Using Phone (Vishing)
  - Example of Social Engineering Using the Phone
- Attempt Social Engineering Using SMiShing (SMS Phishing)

Social Engineering Penetration Testing Using Physical Attack Vector

- Visit the Company as an Inquirer and Extract Privileged Information
- Visit the Company Locality
- Attempt to Use Fake ID to Gain Access
- Attempt Piggybacking/Tailgating
- Listen to Employee Conversations in Communal Areas/Cafeteria
- Identify “Disgruntled Employees” and Engage Them in Conversation to Extract Sensitive Information
- Attempt Eavesdropping
- Try to Shoulder Surf Users Who Are Logging On
- Attempt Media Dropping/Baiting
- Attempt Dumpster Diving
- Attempt Reverse Social Engineering
- Attempt Elicitation
- Attempt Social Engineering Using Motivation Techniques

Reporting and Countermeasures/Recommendations

- Document the Result
- Step 4: Reporting
- Social Engineering Countermeasures and Recommendations

Module 05: Network Penetration Testing - External

- Network Penetration Testing
- External vs. Internal Penetration Testing
- External Network Penetration Testing
- Internal Network Penetration Testing
- Network Penetration Testing Process
- White, Black or Gray-box Network Penetration Testing?

Port Scanning

- Port Scanning
  - Scan the Network to Discover Live Hosts
  - Check for Live Systems - ICMP Scanning
  - Identify Default Open Ports
  - Use Connect Scan (Full Open Scan) on the Target and See the Response
  - Use SYN Scan (Half-open Scan) on the Target and See the Response
  - Use Illegal Flag Combinations to Scan the Target
  - Use ACK Flag Probe Scan on the Target and See the Response
  - Use UDP Scan on the Target and See the Response
  - Use Fragmentation Scanning and Examine the Response
  - List Open and Closed Ports

OS and Service Fingerprinting

- Fingerprint the OS
- Examine the Patches Applied to the Target OS
- Fingerprint the Services

Vulnerability Research

- External Vulnerability Assessment
- Search and Map the Target with the Associated Security Vulnerabilities
- Find Out the Security Vulnerability Exploits

Exploit Verification

- Run the Exploits against Identified Vulnerabilities
- Document the Result

Module 06: Network Penetration Testing - Internal

- Internal Network Penetration Testing
  - Why Internal Network Penetration Testing?

Footprinting

- Identify the Internal Domains
- Identify Hosts
- Identify the Internal IP Range of the Subnet

Network Scanning

- Scanning
- Scanning Analysis
- Scanning Methodology
  - Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan
  - Live Systems
    - Netdiscover
    - Passive option -p
  - Local Subnet Connection
    - Ettercap
  - Bash Script
  - Ruby Ping Sweep
  - Nmap Host Discovery
  - TCP Discovery
  - Scanning Tools
  - TCP Connection
  - Connect Scan and Sockets
  - Half Open Scan
  - Scanning using Scripts
    - Sockets in Python
    - Grab a Web Page in Python
  - Port Scanning
    - Source Port Scanning
  - ZMap

- Masscan
- Scan a Network: Live Host Scan
- Scan a Network: Port Scan
- Common Ports List
- Other Network Scanning Tools
- Scanning from within Metasploit
  - Prepare Database
  - Metasploit Databases
  - Workspaces
    - ✓ Connected Workspace Options
  - Gathering our data
  - db_nmap
  - Review the data
  - Backing up our data
- Working with Hosts
- Setting Up Modules
  - Import the Data into a Module
- TCP portscan from Metasploit

OS and Service Fingerprinting

- Identify the OS
- SMB OS Discovery
- Manual Banner Grabbing
  - Banner Grabbing with dmitry
  - Banner Grabbing with Python
  - Banner Grabbing with Ruby
  - Banner Grab with Metasploit Module
    - Testing Custom Metasploit Modules
- Identify the Services
- Displaying Services within Metasploit
- Services Data
- Services Port State

- Map the Internal Network

Enumeration

- Perform Service Enumeration
- Enumeration
  - Enumeration Targets
  - Enumeration Techniques and Tools
- Perform NetBIOS Enumeration
  - nbtscan
- SNMP
  - SNMP and Nmap
  - Perform SNMP Enumeration
- Perform LDAP Enumeration
  - Directory Services
  - Extract Directory Services Data
- Perform NTP Enumeration
- Perform SMTP Enumeration
- Perform IPSec Enumeration
- Perform VoIP Enumeration
- Perform SMB Enumeration
- Perform RPC Enumeration
- Perform Null Session Enumeration
- Perform Unix/Linux User Enumeration
  - enum4linux
- Perform IPv6 Enumeration
- Nmap Scripting Engine Categories
- Discovery
- Fuzzer
- Scripts Category Downside
- Nmap Server Message Block Scripts
- Enumerate Shares
- Enumerate Users

- HTTP Enumeration Auxiliary Scripts in Metasploit
- cert
- dir_scanner
- files_dir
- Sniff the Network
  - Tcpdump: Capture Traffic using Tcpdump

Vulnerability Assessment

- Perform Internal Vulnerability Assessment
- Vulnerability Scanning Objectives
- Network Vulnerability Scanning
- Host Vulnerability Scanner
- Scanner Configuration
- Scan Templates
- Scanner Configuration OpenVAS
  - OpenVAS
  - OpenVAS Scan Dashboard
- Nessus Scanners Listing
  - Plugins
  - Plugin Families
  - Sub-plugins
  - Built-in Policies
  - Available Plugins
- Custom Scan
- Tailoring Scans
- Discovery
- Assessment
- Report
- Advanced
- Scan Templates
- OpenVAS Port Configuration
- OpenVAS Scan Configs

- Perform Network Vulnerability Scanning using Network Vulnerability Scanners
  - Perform Vulnerability Scanning using Nmap
- Vulnerability Assessment Reports
- Map the Service Version with the Associated Security Vulnerabilities
  - Map the Windows Applications with the Associated Security Vulnerabilities
  - Map the Windows OS with the Associated Security Vulnerabilities
  - Map the Solaris with the Associated Security Vulnerabilities
  - Map the Unix/Linux with the Associated Security Vulnerabilities
- Scan Analysis Process
  - Scan Analysis at the Network Level
  - Nessus Scan Results
  - Attack Scripting
  - NASL Banner Grab
  - Nmap Vulnerability Scanning
  - Vulnerability Scripts
    - Windows Vulnerability Script Results
    - Linux Vulnerability Script Results
  - Vulnerability Scanning Efficiency
  - SMB Vulnerability Scanning
  - Heartbleed Vulnerability
  - Custom Vulnerability Script
  - Vulnerability States

Windows Exploitation

- Reality
- Operating Systems
- Exploitation
- Exploiting Targets
- Data Collection
- Banners
- Finding Exploits
- Exploit Publishers

- Exploit DB
- Packetstorm
- Exploit DB in Parrot

- Exploits
- Full Disclosure
- Questions to Ask About the Exploit
- Location
- Complexity
- What About Authentication
- You do not Always have to run an Exploit to own the box!
- Remote Password Attack
  - Patator
  - Ncrack
  - Medusa
  - rdesktop
- Wpscan for exploitation
- Exploit Frameworks
- Identify Local/Remote Exploit to Gain Access to Windows System
  - Try to Gain Access to Windows using Remote Shell
  - Try to Exploit Buffer Overflow Vulnerability on Windows
- Metasploit
  - Finding Exploits in Metasploit
  - Exploit Wordpress with Metasploit
  - Locate the Plugin Exploit
  - Exploiting InBoundio
  - Metasploit Auxiliary
  - Metasploit Ranking
  - Targets
  - Payload
  - Shell Options
    - Reverse Shell

- Meterpreter Shell
- Metasploit Staged Payloads
  - Metasploit Staged Payloads in Memory
  - Staged Payload Size
- Metasploit Stageless Payload
- Metasploit Architecture
- Metasploit Libraries
- Metasploit Skeleton Module
  - Sample Module
  - Module Breakdown Part One
  - Module Breakdown Part Two
  - Module Breakdown Part Three
  - Module Breakdown Part Four
- Metasploit Exploits
- Metasploit Mixins
- Initialization Method
- Add an Exploit to Metasploit
- Uploading into Metasploit
- Repetitive Tasks
- Resource Scripts

Unix/Linux Exploitation

- Identify Local/Remote Exploit to Gain Root Access
- Try to Gain Access to Linux using Remote Shell
- Extract User Accounts

Other Internal Network Exploitation Techniques

- Attempt Replay Attacks
- Attempt ARP Poisoning
- Attempt Mac Flooding
- Conduct a Man-in-the-Middle Attack
- Attempt DNS Poisoning
  - Example of a Normal Host File under DNS Poisoning Attack

- Try to Log into a Console Machine
- Boot the PC using Alternate OS and Steal the SAM File
- Try to Break Down the Desktop Lockdown
- Escalate User Privileges
- Hide Sensitive Data on Target Machines
  - Use Various Steganography Techniques to Hide Files on Target Machines
- Capture Communications between FTP Client and FTP Server
- Capture HTTPS Traffic (Even though it cannot be Decoded)
- Spoof the MAC address
- Poison the Victim's IE Proxy Server
- Test for Stack Overflow Vulnerability using OllyDbg Debugger
- Test for Format String Vulnerability using IDA Pro

Automating Internal Network Penetration Test Effort

- Automated Internal Network Penetration Testing Tool: Metasploit
- Automated Internal Network Penetration Testing Tool: Immunity CANVAS

Post Exploitation

- You got a shell! Now what?
  - Disable the Firewall
  - Disable Windows Defender
  - Kill Anti-virus
  - Local Assessment
  - Meterpreter Post Exploitation
    - Install a Backdoor
    - Setup the Backdoor at Boot
    - Windows Target
    - Testing our Access
    - Grab the Data
    - Grab the Credentials
    - View the Recent Files
    - Installed Applications
    - Ask for Exploit Suggestions

- usb_history
- evt_manager Information
- evt_manager Log Clearing
- mimikatz
- WMIC Commands
- Escalating Privileges
- Meterpreter Getsystem Escalation
- Impersonation
- Tokens

- WMIC
  - WMIC Analysis
- findstr
- Exploiting the Finding
- Find with searchsploit
- Privilege Escalation with Dirty Cow
- Ubuntu 16.04 Privilege Escalation bpf
- Finding Privilege Escalation Attacks
  - Privilege Escalation up to Ubuntu 15.04
  - overlayfs privilege escalation
  - Local overlayfs details
  - Search by Kernel
  - Initial Access
  - ssh_login
  - Create the First Session
  - Background the Session and Attempt 2nd
  - Overlayfs Exploit
  - Search for Data in Windows Shell
  - Search for Specific Data
  - Search in the Registry
  - Unattended Files

        - Other Files of Interest
    - Linux Privilege Escalation
    - Shell Limited?
    - Sticky Bits
    - Written to and Executed From
    - Dev Tools
    - File Transfer
    - User/Group Account Script
    - Powershell Script to Transfer a File
    - Checking Missing Security Patches and Patch Levels: Linux
    - Cleanup: Resetting into Prevision State

Advanced Tips and Techniques

- Pivoting
- Trust
- Dual Homed Machine
- Preparation
- New Attack
- Run from the Shell
- Port Forwarding
- Session Routing
    - Session Routing Diagram
- Pivoting in Action
- We have to Add the Route
- Search the Discovered Network
- OS Discovery
- Exploit through the Session
- Double Pivot
- Proxychains
- Steps to Setup
    - Metasploit Proxy Module
    - Usage

- Web Shells
  - b734k
- Create the Shell
  - Shell Interface
- Connect to the Shell
- Weevely
- Create a Custom Shell
- Create the Form
  - Focus
  - Basic PHP Shell
  - HTML Part
  - PHP Part

- Document the Result

Module 07: Network Penetration Testing - Perimeter Devices

Assessing Firewall Security Implementation

- Testing the Firewall from Both Sides
- Find Information about the Firewall
- Locate the Firewall by Conducting Traceroute
- Try to Pass through the Firewall using Hping
- Enumerate Firewall Access Control List using Nmap
- Scan the Firewall for Vulnerabilities
- Map Firewall Make and Version with Associated Vulnerabilities
- Try to Bypass the Firewall using Fragmented Packets
- Try to Bypass the Firewall by Spoofing Packets
- Try to Bypass the Firewall by Spoofed Source Port
- Try to Bypass Firewall by MAC Address Spoofing
- Try to Bypass the Firewall by IP Address Spoofing
- Try to Bypass the Firewall by Varying Packet Size
- Try to Bypass the Firewall by Sending Bad Checksums
- Try to Bypass the Firewall using Port Redirection

- Try to Bypass the Firewall using IP Address in Place of URL
- Try to Bypass the Firewall using Anonymous Website Surfing Sites
- Try to Bypass the Firewall using a Proxy Server
- Try to Bypass the Firewall using Source Routing
- Try to Bypass the Firewall using HTTP Tunneling Method
- Try to Bypass the Firewall using ICMP Tunneling Method
- Try to Bypass the Firewall using ACK Tunneling Method
- Try to Bypass the Firewall using SSH Tunneling Method
- Try to Bypass the Firewall through MITM Attack
- Try to Bypass the Firewall using Malicious Contents

Assessing IDS Security Implementation

- Why IDS Penetration Testing?
- Common Techniques Used to Evade IDS Systems
- Test for Resource Exhaustion
- Test the IDS by Sending an ARP Flood
- Test the IDS by MAC Spoofing
- Test the IDS by IP Spoofing
- Test the IDS by Sending SYN Floods
- Test the IDS by Editing and Replaying Captured Network Traffic
- Test the IDS for a Denial-of-Service (DoS) Attack
- Try to Bypass IDS using Anonymous Website Surfing Sites and a Proxy Server
- Try to Bypass the IDS using Botnet
- Test the IDS by Sending Inconsistent Packets
- Test the IDS for IP Packet Fragmentation
    - Packet Fragmentation
- Test the IDS for Polymorphic Shellcode
- Try to Evade the IDS by Obfuscating or Encoding the Attack Payload
- Check the IDS for False-Positive Generation
- Test the IDS for TTL Evasion
- Test the IDS by Sending a Packet to Port 0
- Test the IDS for UDP Checksum

- Test the IDS for TCP Retransmissions
- Test the IDS using Covert Channels
- Test the IDS for Reverse Traversal
- Test for Self-Referencing Directories
- Test for Premature Request Ending
- Test for the IDS Parameter Hiding
- Test the IDS for HTTP Misformatting
- Test the IDS for Long URLs
- Test for Null Method Processing
- Try to Bypass the IDS using Compressed Media Files
- Test Session Splicing
- Try to Bypass Invalid RST Packets through the IDS

Assessing Security of Routers

- Need for Router Testing
  - Router Testing Issues
- Identify the Router Hostname
- Port Scan the Router
- Identify the Router Operating System and its Version
- Identify Protocols Running
- Test for TFTP Connections
- Try to Retrieve the Router Configuration File
  - Test for Router Misconfigurations
  - Try to Recover Router Passwords from Config File
- Test for VTY/TTY Connections
- Try to Gain Access to the Router
  - Test for Router Running Modes
  - Privileged Mode Attacks
- Test for SNMP Capabilities
- Perform SNMP Bruteforcing
- Try to Log in using default SNMP Community String
- Test if Finger is Running on the Router

- Test for CDP Protocol Running on the Router
- Test for NTP Protocol
- Test for Loose and Strict Source Routing
- Test for IP Spoofing
- Test for IP Handling Bugs
- Test ARP Attacks
- Test BGP Protocol
- Test for EIGRP Protocol
- Test Router Denial-of-Service Attacks
- Test Router's HTTP Capabilities
- Test for HTTP Configuration Vulnerabilities in Cisco Routers
- Test through HSRP Attack
- Router Penetration Testing using Secure Cisco Auditor (SCA)

Assessing Security of Switches

- Look for Security Misconfigurations in Cisco Switch Configuration
- Test for Address of Cache Size
- Test for Data Integrity and Error Checking
- Test for Back-to-Back Frame Capacity
- Test for Frame Loss
- Test for Latency
- Test for Throughput
- Test for Frame Error Filtering
- Test for Fully Meshed Condition
- Functional Test for Stateless QoS
- Performance Test for Spanning Tree Network Convergence
- Test for OSPF Performance
- Test for VLAN Hopping
- Test for MAC Table Flooding
- Testing for ARP Attack
- Check for VTP Attack
- Router and Switch Security Auditing Tool: Traffic IQ Professional

- Document the Result

Module 08: Web Application Penetration Testing

- White-Box or Black-Box?
- Web Application Penetration Testing
- Web Application Security Frame
- Security Frame vs. Vulnerabilities vs. Attacks

Discover Web Application Default Content

- Identify Functionality
- Perform Basic Website Footprinting using Netcraft
- Perform Web Enumeration using Whatweb
  - WhatWeb Aggression
- Manually Browse the Target Website URL and Internal URLs
- Analyze the HTML Source Code
- Check the HTTP and HTML Processing by the Browser
- Identify Server-Side Technologies
- Identify the Technology used to Build Target Website

Discover Web Application Hidden Content

- Identify the Sitemap of Target Website
- Perform Web Spidering
- Mirror and Crawl a Website to Identify its Files, Directories, Folders
  - Website Mirroring Tools
- Perform Directory Brute Forcing using DirBuster
- Identify the Restricted Directories that Web Crawlers cannot Find
- Discover Hidden Content of the Target Website
- Extract Common Word List from the Target

Conduct Web Vulnerability Scanning

- Conduct Web Vulnerability Assessment
- Web Application Vulnerability Scanners: WebInspect
- Web Application Security Scanners: Qualys
- Web Vulnerability Scanning with Metasploit

- Perform Web Application Fuzz Testing
- Identify Entry Points for User Input

Test for SQL Injection Vulnerabilities

- Identify the Injection Points
- Identify the SQL Injectable Entry Points in the HTTP Request
- Entry Points in HTTP Requests
  - Example: Identify Injection Points using SQLMAP
- Perform Database Fingerprinting
  - Example: Identify Databases using SQLMAP
- Detect SQL Injection Vulnerabilities by Manipulating a Parameter
- Determine the Database Schema using Error-Based SQL Injection
- Determine Privileges, DB Structure and Column Names
  - Example: Identifying Tables using SQLMAP
  - Example: Identifying Columns using SQLMAP
  - Example: Extract Data from Database Tables using SQLMAP
  - Example: Extract Authentication Credentials using SQLMAP
- Insert, Update, and Delete Data from Database
- Attempt a DoS Attack using SQL Injection
- Evade IDS Detection using 'OR 1=1 Equivalents
- Evade IDS Detection using Char Encoding
- Evade IDS Detection by Manipulating White Spaces
- Evade IDS Detection using Inline Comments
- Evade IDS Detection using Obfuscated Code
- Bypass Website Authentication using SQL Injection
- Perform a Function-Call Injection Attack
- Perform a Buffer Overflow Attack
- Access System Files and Execute Remote Commands
- Use OPENROWSET to Escalate Privileges on the Microsoft SQL Server

Test for XSS Vulnerabilities

- Manual Test for XSS Vulnerabilities
- Automated Test for XSS Vulnerabilities

Test for Parameter Tampering

- Test for URL Parameter Tampering
- Test for Hidden Field Parameter Tampering
- Test for Unrestricted File Upload Vulnerability
- Perform HTTP Response Splitting/CRLF Injection Attack

Test for Weak Cryptography Vulnerabilities

- Check for Insufficient Transport Layer Protection
- Check for Weak SSL Ciphers
- Detect Use of Weak Encoding Techniques

Tests for Security Misconfiguration Vulnerabilities

- Test the Inner Workings of a Web Application
- Test the Database Connectivity
- Test the Application Code
- Test whether the Target Website is Protected using Web Application Firewall (WAF)
- Test for Debug Parameters
- Test for Improper Error Handling

Test for Client-Side Attack

- Identify the Technology Used at Client-side
- Test the Application's Reliance on Client Side Validation
- Test Client-side Controls Over User Input
- Test Transmission of Data via Client
- Test ActiveX Controls
- Test Shockwave Flash Objects
- Check for Frame Injection
- Test with User Protection via Browser Settings

Tests for Broken Authentication and Authorization Vulnerabilities

- Understand the Authentication and Authorization Mechanism
- Test Password Quality
- Test for Username Enumeration
- Test Resilience to Password Guessing
- Perform Password Brute-forcing

- Perform Authorization Attack
- Understand the Access Control Requirements
- Test with Multiple Accounts
- Test with Limited Access
- Test for Insecure Access Control Methods
- Test Segregation in Shared Infrastructures
- Test Segregation between ASP-hosted Applications

Tests for Broken Session Management Vulnerabilities

- Understand the Session Management Mechanism
- Test Tokens for Meaning
- Session Token Prediction (Test Tokens for Predictability)
- Perform Session Token Sniffing
- Check for Insecure Transmission of Tokens
- Check for Disclosure of Tokens in Logs
- Check Mapping of Tokens to Sessions
- Test Session Termination
- Test for Session Fixation Attack
- Test for Session Hijacking
- Check for XSRF
- Check Cookie Scope
- Test Cookie Attacks

Test for Web Services Security

- Perform Web Services Probing Attacks
- Test for XML Structure
- Test for XML Content-level
- Test for WS HTTP GET Parameters/REST Attacks
- Test for Suspicious SOAP Attachments
- Test for XPath Injection Attack
- Test for WS Replay

Test for Business Logic Flaws

- Test for Logic Flaws

- Identify the Key Attack Surface
- Test Multistage Processes
- Test Handling of Incomplete Input
- Test Trust Boundaries
- Test Transaction Logic

Test for Web Server Vulnerabilities

- Perform HTTP Service Discovery
- Perform Banner Grabbing to Identify the Target Web Server
- Perform Advanced Web Server Fingerprinting using HTTPRecon
- Test for Default Credentials
- Test for Dangerous HTTP Methods
- Enumerate Webserver Directories
- Test for Proxy Functionality
- Test for Virtual Hosting Misconfiguration
- Test for Web Server Software Bugs
- Web Sever Vulnerability Scanner: NIKTO

Test for Thick Clients Vulnerabilities

- Pen Testing Thick Clients
- Dynamic Testing
- System Testing
- Static Testing

Wordpress Testing

- Wpscan
  - Enumerate wpscan data
- Wordpress Enumeration in Metasploit
- Document the Result

Module 09: Wireless Penetration Testing

- Wireless Penetration Testing

Wireless Local Area Network (WLAN) Penetration Testing

- Discover the Wireless Networks

- Check Physical Security of AP
- Detect Wireless Connections
- Sniff Traffic between the AP and Linked Devices
- Create a Rogue Access Point and Try to Create a Promiscuous Client
- Use a Wireless Honeypot to Discover Vulnerable Wireless Clients
- Perform a Denial-of-Service Attack (De-authentication Attack)
- Attempt Rapid Traffic Generation
- Attempt Single-packet Decryption
- Perform an ARP Poisoning Attack
- Try to Inject the Encrypted Packet
- Crack WPA-PSK Keys
- Crack WPA/WPA2 Enterprise Mode
- Check for MAC Filtering
- Spoof the MAC Address
- Create a Direct Connection to the Wireless Access Point
- Additional Wireless Penetration Testing Tools: Kismet
- Additional Wireless Penetration Testing Tools: Extreme AirDefense

RFID Penetration Testing

- Introduction to RFID Penetration Testing
- Perform Reverse Engineering
- Perform Power Analysis Attack
- Perform Eavesdropping
- Perform an MITM Attack
- Perform a DoS Attack
- Perform RFID Cloning/Spoofing
- Perform an RFID Replay Attack
- Perform a Virus Attack
- Oscilloscopes, RFID Antennas and RFID Readers

NFC Penetration Testing

- Introduction to NFC Penetration Testing
- Perform Eavesdropping

- Perform a Data Modification Attack
- Perform Data Corruption Attack
- Perform a MITM Attack
- Document the Result

Module 10: IoT Penetration Testing

IoT Attacks and Threats

- IoT
- Popular IoT Hacks
  - Phillips Smart Home
  - LIFX Smart Bulb
  - The Jeep Hack
  - Belkin WeMo
  - Insulin Pump
  - Smart Door Locks
  - Hacking Smart Guns and Rifles
- IoT Challenges

IoT Penetration Testing

- IoT Penetration Testing
- Abstract IoT Testing Methodology
- Attack Surface Mapping
- IoT Architecture
- Typical IoT Vulnerabilities
- Steps to Analyzing the IoT Hardware
- Example IoT Components
- Firmware Attacks
- Mobile Application
- Web Application
- Radio Communication
- Attack Surface Map
- Sample Architecture Diagram

- The Firmware
- Sample Firmware Analysis Process
- Binwalk
- Binwalk to Extract the File System
- Exploring the File System
- Exploitation
- Firmware Emulation

Module 11: OT and SCADA Penetration Testing

OT/SCADA Concepts

- IT vs OT System Architecture
- ICS/SCADA Protocols
- Control Plane vs. Data Plane
  - Example of Control-plane and Data-plane Protocols

Modbus

- Modbus
  - Modbus Protocol Types
  - Modbus Protocol and Open Systems Interconnection Model
  - Modbus Recon

ICS and SCADA Pen Testing

- ICS and SCADA Pen Testing
- Sample SCADA Network
- Approach
- Attack Monitoring
- Testing Environment
- Penetration Testing Actions
- Host Attack Types
- Network Attack Types
- Ports of SCADA
- Nmap Scripting Engine
- Attack Modifications

- OT Testing Tools
- BACnet
- Commercial SCADA Fuzzing Tool
- Special Testing Consideration
- Danger of Port Scanning
  - Low-risk Scan
  - Medium-risk Scan
  - High-risk Scan
- Types of Vulnerability Scans
  - Example Nessus Scan
- Device Separation
- ICS Cyber Test Impact

Module 12: Cloud Penetration Testing

- Cloud Computing Security and Concerns
- Security Risks Involved in Cloud Computing
- Role of Penetration Testing in Cloud Computing
- Do Remember: Cloud Penetration Testing
- Scope of Cloud Pen Testing

Cloud Penetration Testing

- Understand Shared Responsibilities in Cloud
- Understand Penetration Testing Process, Policies, and Limitations
- Identify the Type of Cloud to be Tested
- Identify what is to be Tested in the Cloud Environment
- Identify Tools for Penetration Testing
- Perform Cloud Reconnaissance
- Check for Lock-in Problems
- Check for Governance Issues
- Check for Compliance Issues
- Check for Right Implementation of Security Management
- Check the Cloud for Resource Isolation

- Check whether Anti-Malware Applications are Installed and Updated on Every Device
- Check whether Firewalls are Installed at Every Network Entry Point
- Check that Strong Authentication is Deployed for Every Remote User
- Check the SSL Certificates for the Cloud Services in the URL
- Check whether Files Stored on the Cloud Servers are Encrypted
- Check the Data Retention Policy of Service Providers
- Check that all Users Follow Safe Internet Practices
- Perform a Detailed Vulnerability Assessment
- Try to Gain Passwords to Hijack the Cloud Service
- Test for Virtualization Management (VM) Security
- Check Audit and Evidence-Gathering Features in the Cloud Service
- Recommendations for Cloud Testing

AWS Specific Penetration Testing

- Understand AWS Shared Responsibility Model
- Shared Responsibility Model: Infrastructure Services
- Shared Responsibility Model: Container Services
- Shared Responsibility Model: Abstract Services
- Understand AWS Penetration Testing Policy and Procedures
- Attempt to Identify S3 Buckets
- Check for S3 Bucket Permissions
- Attempt to Create New Policy Version
- Attempt to Set an Existing Policy Version as Default
- Attempt to Obtain Access to the set of EC2 Instance/Role Permissions
- Attempt to Create a New User Access Key
- Attempt to Create a New Login Profile
- Attempt to Update an Existing Login Profile
- Attempt to Attach a Policy to a User
- Attempt to Attach a Policy to a Group
- Attempt to Attach a Policy to a Role
- Attempt to Create/Update an Inline Policy for a User
- Attempt to Create/Update an Inline Policy for a Group

- Attempt to Create/Update an Inline Policy for a Role
- Attempt to Add a User to a Group
- Attempt to Update AssumeRolePolicyDocument of a Role

Azure Specific Penetration Testing

- Understand Azure's Shared Responsibility Model
- Understand Azure Penetration Testing Policy and Procedures
- Assess Azure Environment with Azure Security Center
- Check Assigned Role of Users
- Check whether access to the Azure AD Portal is Restricted
- Check whether Multi-Factor Authentication (MFA) is Enabled for Every User
- Check whether WAF is installed on Microsoft Azure
- Check whether Data is Encrypted at Rest
- Check whether Azure SQL Databases are Encrypted
- Check the Data Retention Time in Microsoft Azure
- Check whether Network Security Groups Diagnostic logs are turned On
- Check whether Azure Network Watcher is Enabled
- Check whether JIT VM Access is Enabled

Google Cloud Platform Specific Penetration Testing

- Understand Google Cloud Shared Responsibility Model
- Google Cloud's Provision for Penetration Testing
- Check whether Security Health Analytics is Enabled
- Check whether Cloud Web Security Scanner is Enabled
- Check whether Cloud Anomaly Detection is Enabled
- Check whether Container Threat Detection is Enabled
- Check whether Event Threat Detection is Enabled
- Document The Result

Module 13: Binary Analysis and Exploitation

Binary Coding Concepts

- Machine Instructions
- Sample Stack Frame

- C program memory
- Analyzing Binaries
- 32-bit Assembly
- IA-32 Registers on Linux
- Registers
- Important IA-32 Instructions for Pen Testing
- Netwide Assembler
- Executable and Linkable Format
  - ELF Binary
  - Simple Code Injection Techniques For ELF
  - Limitations of Simple Code Injection Techniques
- Advanced Binary Analysis
- Obfuscation Challenges
- Framework
- Binary Instrumentation
- IA-64
  - IA-64 System Calls

Binary Analysis Methodology

- Binary Analysis Methodology
  - Binary Discovery
  - Information Gathering
  - Static Analysis
  - Dynamic Analysis
  - Iterating Each Step
- Sample Program
- Sample x86 C Program
- Shellcode
- Obstacles to Exploitation
- ASLR
- Return-to-libc vulnerability
- Sample Code

- Comparison
- Sample Code
- Defeating the No-execute Stack
- Return-to-libc Limitations
- 64-bit Fundamentals
- Why use ROP?
- Attack using ROP
  - Build a Custom ROP Gadget tool
  - Sample Code

Module 14: Report Writing and Post Testing Actions

Penetration Testing Report: An Overview

- Goal of the Penetration Testing Report
- Penetration Testing Deliverables
- Report Audience
- Report Formats
- Types of Pen Test Reports
- Characteristics of a Good Pen Testing Report
- Common Mistakes

Phases of Report Development

- Phases of Report Development
  - Plan the Report
  - Collect and Document the Information
  - Write a Draft Report
  - Review and Finalize the Report
- Sample Pen Testing Report Format

Report Components

- Report Components
  - Cover Letter
  - Document Properties/Version History
  - Table of Contents/Final Report

- Assessment Information/Contact Information
- Distribution List/Confidentiality Statement
- Executive Summary
  - Scope of the Project
  - Evaluation Purpose/System Description
  - Assumptions/Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Strengths and Weaknesses
  - Summary of Recommendations
  - Testing Methodology
  - Planning
  - Exploitation
  - Reporting
- Comprehensive Technical Report
- Result Analysis
- Recommendations
- Appendices
  - Sample Appendix

Penetration Testing Report Analysis

- Penetration Testing Report Analysis
- Sections of the Penetration Testing Report
- Pen Test Team Meeting
- Research Analysis
  - Pen Test Findings
  - Rating Findings
  - Detailed Findings Table
    - Example of Finding – I
    - Example of Finding – II
    - Example of Finding – III
  - Analyze

- Prioritize Recommendations

Penetration Testing Report Delivery

- Delivering Penetration Testing Report
- Letter of Attestation
- Cleanup and Restoration
- Report Retention
- Destroy the Report
- Sign-off Document
  - Sign-off Document Template

Post-Testing Actions for Organizations

- Develop an Action Plan
  - Points to Check in Action Plan
- Develop and Implement Data Backup Plan
- Create a Process for Minimizing Misconfiguration Chances
- Updates and Patches
- Capture Lessons Learned and Best Practices
- Create Security Policies
- Conduct Training

Appendix A: Penetration Testing Essential Concepts

Computer Network Fundamentals

- Computer Network
- TCP/IP Model
  - Comparing OSI and TCP/IP
- Types of Networks
  - Network Topologies
  - Network Hardware Components
- Types of LAN Technology
- Types of Cables: Fiber Optic Cable
- Types of Cables: Coaxial Cable
- Types of Cables: CAT 3 and CAT 4
- Types of Cables: CAT 5
- Types of Cables: CAT 5e and CAT 6
- Types of Cables: 10/100/1000BaseT (UTP Ethernet)

TCP/IP Protocol Suite

- TCP/IP Protocol Suite

TCP/IP Protocol Suite: 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
  - How DNSSEC Works?
  - Managing DNSSEC for your Domain Name
  - What is a DS Record?
  - How does DNSSEC Protect Internet Users?
  - Operation of DNSSEC
- Hypertext Transfer Protocol (HTTP)

- Secure HTTP
- Hyper Text Transfer Protocol Secure (HTTPS)

- File Transfer Protocol (FTP)
  - How FTP Works?
  - FTP Anonymous Access and its Risk
  - Hardening FTP Servers
- Secure File Transfer Protocol (SFTP)
- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transfer Protocol (SMTP)
- Sendmail
- Mail Relaying
- S/MIME
  - How it Works?
- Pretty Good Privacy (PGP)
- Difference between PGP and S/MIME
- Telnet
- SSH
- SOAP (Simple Object Access Protocol)
- Simple Network Management Protocol (SNMP)
- NTP (Network Time Protocol)
- RPC (Remote Procedure Call)
- Server Message Block (SMB) Protocol
- Session Initiation Protocol (SIP)
- RADIUS
- TACACS+
- Routing Information Protocol (RIP)
- OSPF (Open Shortest Path First)

TCP/IP Protocol Suite: Transport Layer Protocols

- Transmission Control Protocol (TCP)
  - TCP Header Format
  - TCP Services

- User Datagram Protocol (UDP)
  - UDP Operation
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

TCP/IP Protocol Suite: Internet Layer Protocols

- Internet Protocol (IP)
  - IP Header: Protocol Field
- What is Internet Protocol v6 (IPv6)?
  - IPv6 Header
  - IPv4/IPv6 Transition Mechanisms
  - IPv6 Security Issues
  - IPv6 Infrastructure Security Issues
- IPv4 vs. IPv6
- Internet Protocol Security (IPsec)
- IPsec Authentication and Confidentiality
- 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
- Address Resolution Protocol (ARP)
  - ARP Packet Format
  - ARP Packet Encapsulation
  - ARP Packet Analysis
- IGRP (Interior Gateway Routing Protocol)

- EIGRP (Enhanced Interior Gateway Routing Protocol)

TCP/IP Protocol Suite: Link Layer Protocols

- Fiber Distributed Data Interface (FDDI)
- Token Ring
- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 Encryption
- WEP vs. WPA vs. WPA2
- TKIP
- EAP (Extensible Authentication Protocol)
  - How EAP Works?
- Understanding LEAP / PEAP
- CDP (Cisco Discovery Protocol)
- HSRP (Hot Standby Router Protocol)
- Virtual Router Redundancy Protocol (VRRP)
- VLAN Trunking Protocol (VTP)
- STP (Spanning Tree Protocol)

IP Addressing and Port Numbers

- Internet Assigned Numbers Authority (IANA)
- IP Addressing
- Classful IP Addressing
- Address Classes
- Subnet Masking
- Subnetting
- Supernetting
- IPv6 Addressing
- Difference between IPv4 and IPv6
- Port Numbers

Network Terminology

- Routing
- Network Address Translation (NAT)

- Port Address Translation (PAT)
- VLAN
- Shared Media Network
- Switched Media Network

Network Security Controls

- Network Security Controls
- Access Control
  - Access Control Terminology
  - Access Control Principles
  - Access Control System: Administrative Access Control
  - Access Control System: Physical Access Controls
  - Access Control System: Technical Access Controls
  - Types of Access Control
  - Network Access Control List
- User Identification, Authentication, Authorization, and Accounting
- Types of Authentication: Password Authentication
- Types of Authentication: Two-factor Authentication
- Types of Authentication: Biometrics
- Types of Authentication: Smart Card Authentication
- Types of Authentication: Single Sign-on (SSO)
- Types of Authorization Systems
- Authorization Principles
- Encryption
  - Symmetric Encryption
  - Asymmetric Encryption
- Encryption Algorithms: Data Encryption Standard (DES)
- Encryption Algorithms: Advanced Encryption Standard (AES)
- Encryption Algorithms: RC4, RC5, RC6 Algorithms
- Hashing: Data Integrity
- Message Digest Function: MD5
- Message Digest Function: Secure Hashing Algorithm (SHA)

- Hash-based Message Authentication Code (HMAC)
- Digital Signatures
- Digital Certificates
- Public Key Infrastructure (PKI)

Network Security Devices

- 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
- Egress Filtering and its Importance
- Ingress Filtering and its Importance
- Firewall Rulebase Review
- Maintenance and Management of Firewall
- 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)
- Common Techniques Used to Evade IDS Systems
- Proxy Server
- Virtual Private Network (VPN)
- VPN Security

Network File System (NFS)

- Network File System (NFS)
  - NFS Host and File Level Security
- UID/GUID Manipulation

Windows Security

- Patch Management
- System Management Server: SMS
- Microsoft Software Update Services: SUS
- Windows Software Update Services: WSUS
- Microsoft Baseline Security Analyzer (MBSA)
- Windows Registry
- Identifying Running Process and its Associated Sockets
- Analyzing Registry ACLs
- Disabling Unused System Services
- Finding Suspicious/Hidden/Interesting Files
- File System Security: Setting Access Controls and Permission
- File System Security: Setting Access Controls and Permission to Files and Folders
- Creating and Securing a Windows File Share
- Desktop Locked Down
- Active Directory(AD)
  - Active Directory Roles: Global Catalog (GC)
  - Active Directory Roles: Master Browser
  - Active Directory Roles: FSMO
  - How AD Relies on DNS
  - How AD Relies on LDAP Group Policy
- Windows Passwords: Password Policy
- Account Lockout Policy
- Microsoft Authentication
- Security Accounts Manager (SAM) Database
- Microsoft Exchange Server and its Concerns

Unix/Linux Security

- Linux Baseline Security Checker: buck-security

- Password Management
- Disabling Unnecessary Services
- Killing Unnecessary Processes
- Linux Patch Management
- File System Security: Unix/Linux
- Understanding and Checking Linux File Permissions
- Changing File Permissions
- Check and Verify Permissions for Sensitive Files and Directories
- R Services
- X Windows
    - X Windows: Access Controls

Virtualization

- Introduction to Virtualization
- Characteristics of Virtualization
- Benefits of Virtualization
- Common Virtualization Vendors
- Virtualization Security and Concerns

Web Server

- Web Server Operations
- Apache
- IIS Web Server Architecture
- Web Server Security Issue
- Common Web Server Security Issues

Web Application

- Overview of Web Application Architecture
    - Web Application Architecture
- HTTP Communication
    - Exchange of HTTP Request and Response Messages
    - HTTP Request Message Format
    - HTTP Response Message Format
    - HTTP Message Parameters

- HTTP Request Methods
- HTTP GET and POST Request Method
- HTTP Response Status Codes and Phrases
- HTTP Header Fields: General Header
- HTTP Header Fields: Request Header
- HTTP Header Fields: Response Header
- HTTP Header Fields: Entity Header

- An Overview to HTTPS Protocol
- Encoding and Decoding
- Encoding Techniques
- Differences between Encryption and Encoding
- ASCII Control Characters Encoding
- Non-ASCII Control Characters Encoding
- Reserved Characters Encoding
- Unsafe Characters Encoding

Web Markup and Programming Languages

- HTML
- Extensible Markup Language (XML)
- Java
- .Net
- Java Server Pages (JSP)
- Active Server Pages (ASP)
- PHP: Hypertext Preprocessor (PHP)
- Practical Extraction and Report language (Perl)
- JavaScript
- Bash Scripting

Application Development Framework and their Vulnerabilities

- .NET Framework
- J2EE Framework
- ColdFusion
- Ruby On Rails

- AJAX

Web API's

- Common Gateway Interface (CGI)
- Common Gateway Interface (CGI) Attacks
- Application Interfaces: ISAPI Filters
- Apache Modules

Web Sub Components

- Web Sub Components
- Thick and Thin Clients
- Applet
- Servlet
- ActiveX
- Flash Application

Web Application Security Mechanisms

- Input Validation
  - Why Input Validation?
- Input Filtering
  - Input Filtering Technique: Black Listing
  - Input Filtering Technique: White Listing
- Authentication and Authorization
- Session Management
- Error Handling
- Web Application Fuzz Testing
- Drawbacks of Fuzzing
- Source Code Review
- Threat Modeling
  - Threat Modeling Approaches
  - Threat Modeling Process
    - Threat Modeling Process: Security Objectives
    - Threat Modeling Process: Application Overview
    - Threat Modeling Process: Application Decomposition

- Threat Modeling Process: Identify Threats
- Threat Modeling Process: Identify and Prioritize Vulnerabilities

- Web Application Connection with Underlying Databases: SQL Sever
- Data Controls used for SQL Server Connection
- Web Application Connection with Underlying Databases: MS ACCESS
- Web Application Connection with Underlying Databases: MySQL
- Web Application Connection with Underlying Databases: ORACLE

Working of Most Common Information Security Attacks

- Parameter/Form Tampering
- Directory Traversal
- SQL Injection Attacks
- Command Injection Attacks
- Command Injection Example
- File Injection Attack
- What is LDAP Injection?
  - How LDAP Injection Works?
- Hidden Field Manipulation Attack
- Cross-Site Scripting (XSS) Attacks
  - Cross-site Scripting Attack Scenario: Attack through Phishing
  - Cross-site Scripting Attack Scenario: XSS Attack in Blog Posting
  - Cross-site Scripting Attack Scenario: XSS Attack in Comment Field
- Cross-site Request Forgery (CSRF) Attack
- Denial-of-Service (DoS) Attack
  - Denial-of-Service (DoS) Examples
- Distributed Denial-of-Service Attack (DDoS)
- Cookie/Session Poisoning Attacks
- Session Fixation Attack
- Social Engineering Attacks
- Password Attacks
  - Password Attack Techniques
- Network Sniffing

- Man-in-the-Middle Attack
- Replay Attack
- Privilege Escalation
- DNS Poisoning
- DNS Cache Poisoning
- ARP Poisoning
- DHCP Starvation Attacks
- DHCP Spoofing Attack
- Switch Port Stealing
- MAC Spoofing/Duplicating
- Malware Attacks
- Buffer Overflow Attacks
  - Stack-based Buffer Overflow
  - Heap-based Buffer Overflow
- Shellcode
- No Operations (NOPs)
- Buffer Overflow Steps
- Attacking a Real Program
- Format String Problem
- Overflow using Format String
- Smashing the Stack
- Once the Stack is Smashed...
- Buffer Overflow Examples: Simple Uncontrolled Overflow
- Buffer Overflow Examples: Simple Buffer Overflow in C
- Buffer Overflow Examples: Exploiting Semantic Comments in C (Annotations)

Information Security Standards, Laws and Acts

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Acts: Sarbanes Oxley Act (SOX)
- Information Security Acts: Gramm-Leach-Bliley Act (GLBA)

- Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Police and Justice Act 2006
- Other Information Security Acts and Laws
- Cyber Law in Different Countries

Appendix B: Fuzzing

- Fuzzing Concepts
- No Source Code
- Fuzzing Steps
- Types of Fuzzers
- Bugs Detected by Fuzzing
- Sample Source File
- Protections
- Python Simple Fuzzer
  - Python Simple Fuzzer in Action
  - Python Fuzzer with Network Connection
- Bad Characters
- Basic Debugging
- Crashing the Application
- Sending Input
- Using BASH for input
- Verifying Data
- Debugging the Crash
- Fuzzing Tools
- Python
  - Python FTP Fuzzer
- AFL

- AFL Steps
- Getting Started
- zzuf
- Address Sanitizer
- Peach Framework
- SPIKE

Appendix C: Mastering Metasploit Framework

- Metasploit
- Metasploit 5
- Metasploit Components
- Anatomy and Structure
- Auxiliaries
- Payloads
- Exploits
- Encoders
- NOPs
- Post
- Evasion
- connect
- help
- tips
- route
- save
- sessions
- Other commands
- jobs
- Variables
  - Assigning Variables
- Metasploit Scanners
  - Metasploit SMB Scanners

- Metasploit HTTP Scanners
- Metasploit SSH Scanners

- Identify Vulnerabilities
- Metasploit Databases
  - Customizing Databases
- Workspace
- Import scans
  - db_nmap
- Extracting the data
- Exploitation
- Ranking Explained
- Establishing Persistence
- Backdoor a Binary Stage One
- Backdoor a Binary Stage Two
- Post Exploitation
- Credential Harvesting
- Enumerate Applications
- Enumeration Modules
- msf utilities
- exe2vbs
- exe2vba
- pdf2xdp
- msf_irb
- pattern_create
- Egghunt
- msfrop
- Payload Obfuscation
- New Evasion Module
- Using Encryption
- Certificate Impersonation

Appendix D: PowerShell Scripting

- PowerShell
  - PowerShell Features
- PowerShell cmdlet
  - Cmdlet vs. Command
- Important Commands
- Special Variables
- PowerShell Scripts
- PowerShell Integrated Scripting Environment
- PowerShell vs. Command Prompt
- PowerShell Administrative
- Netsh
  - Netsh as a Sniffer
  - Netsh Examples
  - Replace netsh with Powershell
- Net-Adapter Commands
- Basic PowerShell Commands
- PowerShell Pen Testing
- Execution Policies
- Interaction with Windows
- Control of Processes and Services
- Working with Event Logs
- Sending and Receiving Files
- Interacting with the Registry
- PowerShell and Metasploit

Appendix E: BASH Environment and Scripting

- BASH
- Shebang
- Variables
- Parameter Expansion

- Input, Output, and Error Redirections
- Functions
- Numeric and String Comparisons
- Conditional Statements
- Positional Parameters
- Loops
- BASH Data Collection
- find
- Data Processing
  - awk
  - join
  - sed
  - tail
- Data Analysis
  - sort
  - uniq
- File Analysis
  - cURL
  - xxd
- Extracting Strings
- Log Analysis
- tail
- tr
- Bash script with awk

Appendix F: Python Environment and Scripting

- Python Basics
  - Variable Names
  - Python Keywords
  - Viewing Python Keywords
  - Python Data Types

- String Operations
- Substrings and String Slicing
- String Concatenation and Replication
- The strip(), lstrip(), and rstrip() Methods
- The split() Method
- List Types
  - List Operations
- The in and not in Methods
- Tuple
- Python Operators
- Building Python Scripts
- Indentation
- Conditional Statements
- While Loops
- For Loops
- Functions and Methods
- Modules
- Packages
- Advanced Python Modules
- Multitasking with Threads
- Multitasking with Processes
  - Subprocesses
- Socket Programming
  - Server
  - Client
  - Reverse TCP Shell
- Python Nmap Module
- Python Pen Testing Libraries
- Windows Enumeration
- Web Scraping
- The urlopen Function

- Beautiful Soup
  - Beautiful Soup in Action
  - Extracting Links with Beautiful Soup
  - Reviewing the Extracted Data
  - Review the Sections that Use div
  - The find all() Method
- XSS Sniper

Appendix G: Perl Environment and Scripting

- Perl
- Regular Expressions
- Perl String Functions and Operators
- Regular Expressions and grep()
- CPAN Perl Modules
- Socket in Perl
- CPAN Minus
- Input/Output Streams
- Forking Processes
- BASH Command Execution
- Internal Footprinting
- Port Scanner
- Packet Disassembly
- SMB Scanner
- NetworkInfo::Discovery
- SQL Injection with Perl
- Enumerate Data from Websites
- String SQL Injection
- SQL Column Counting
- Using Perl to Find Exploits
- Creating Reports Using Perl
- Graphing with Perl

- Creating PDF Files

Appendix H: Ruby Environment and Scripting

- Ruby
- Two Methods for Script Execution
  - Hello World in Ruby
- Conversion
- Simple Script
- Variables
  - Constants, Integers, and Floats
  - Arrays and Hashes
- Control Statements
- Grabbing a Web Banner
- Building Classes with Ruby
- Accessing Class Data
- File Manipulation
- Databases and Ruby
  - Ruby DBI Modules
  - Active Record
- Sockets: Client
- Sockets: Server

Appendix I: Active Directory Penetration Testing

- Steps
  - Reconnaissance
    - ADRecon
      - ✓ ADRecon - User Account Details
      - ✓ ADRecon - Groups
    - Active Directory - Kerberos Attacks
      - ✓ Active Directory - Kerberos Attacks Examples
    - Silver Ticket

- ✓ Mimikatz Silver Ticket
- ✓ Silver Ticket Required Parameters
- ✓ Silver Ticket Default Groups

- Golden Ticket
  - ✓ Golden Ticket Requirements
  - ✓ Golden Ticket Limitations
  - ✓ Golden Ticket + SID History
- Service Principal Names (SPNs)
- Kerberoasting via PowerShell
  - ✓ ADRecon - Kerberoast

- Brute Force AD

Appendix J: Database Penetration Testing

Information Reconnaissance

- Scan for Default Ports Used by Databases
- Sniff Database-related Traffic on the Local Wire
- Discover Databases on Network

Database Enumeration: Oracle

- Scan for other Default Ports Used by the Oracle Database
- Scan for Non-Default Ports Used by the Oracle Database
- Check the Status of the TNS Listener Running at the Oracle Server
- Enumerate the Database

Database Enumeration: MS SQL Server

- Scan for Other Default Ports Used by the SQL Server Database
- Enumerate the Database using Nmap Scripts
- Enumerate the Database using Standard SQL Queries
- Enumerate the Database using SQL Server Resolution Service (SSRS)

Database Enumeration: MySQL

- Enumerate the Database

Vulnerability and Exploit Research

- Conduct Exploit Research for Known Vulnerabilities

- Perform Vulnerability Scanning on Target Database
- Database Vulnerability Assessment Tool: AppDetectivePro

Database Exploitation: Oracle

- Try to Log in using Default Account Passwords
- Try to Brute Force Oracle Logins
- Test whether Execution of Privileges is Allowed
- Try to Bypass the Protections Provided by the Oracle Database Vault

Database Exploitation: MS SQL Server

- Test the Stored Procedure to Run Web Tasks
- Brute Force SA Account

Database Exploitation: MySQL

- Try to Log in using Default/Common Passwords
- Brute Force Accounts using Dictionary Attack
- Database Password Cracking Tool: Cain & Abel
- Database Password Cracking Tool: HexorBase
- Document the Result
- Databases Security Countermeasures and Recommendations

Appendix K: Mobile Device Penetration Testing

- Why Mobile Device Penetration Testing?
- Requirements for Mobile Device Penetration Testing
- Rooting the Android Phones
- Jailbreaking iPhones
- Mobile Penetration Testing Methodology

Communication Channel Penetration Testing

- Mobile Penetration Testing: Communication Channel Penetration Testing
- Intercept HTTP Requests Sent from Phone Browser/Applications
- Intercept HTTP Request using Proxy when using Android Emulator
- Intercept HTTP Request using Proxy on iPhone
- Intercept HTTP Request using Proxy on iOS Simulator
- Intercept iOS Traffic using Burp Suite

- Sniff the Traffic using Wireshark
- Sniff the Traffic using FaceNiff

Server-side Infrastructure Penetration Testing

- Mobile Penetration Testing: Server-side Infrastructure Pen Testing

Application Penetration Testing

- Mobile Penetration Testing: Application Penetration Testing
- Setting Up the Environment for Android Apps Penetration Testing
- Identify whether Android is Rooted or not
- Android Browser-based Applications Penetration Testing
- Android Platform-based Applications Penetration Testing
- Test for Application Least Privilege
- Explore Installed Packages on Android Phone with Package Play
- Perform Intent Sniffing
  - Test Android App using Intent Fuzzer
- Test whether Application Stores any Sensitive Information
- Test whether Log of Application Reveals any Sensitive Information
- Try to Reverse Engineer the Android Application
- Try to Discover the Processes Running on the Android Device
- Try to Discover the System Calls Made by Processes
- Check for Sensitive Data on SD Card
- Test whether SQLite Database Reveals any Sensitive Data
- Perform a DoS Attack on Android Phone
- Find and Exploit Android App Vulnerabilities using Drozer
- Conduct Vulnerability Scanning using zANTI
- Perform Android Penetration Testing using dSploit
- Setting Up the Environment for iOS Apps Penetration Testing
- Before IPA Penetration Testing
- Identify whether iPhone is Jailbroken or not
- Inspect the Plist for Sensitive Information
- Investigate the Keychain Data Storage
- Check the iPhone Logs for Leakage of Sensitive Information (Insecure Logging)

- Explore and Look for Sensitive Files in iOS File System
- Inspecting SQLite Databases
- Inspect Error Application Logs
- Inspect Device Logs
- Look for Sensitive Data Cached in Snapshots
- Inspect Keyboard Cache
- Inspect cookies.binarycookies File for Leakage of Sensitive Information
- Check URL Schemes Used by Applications
- Check for Broken Cryptography
- Try to Reverse Engineer the iOS Applications
- Document the Result
- Mobile Device Security Countermeasures and Recommendations

Appendix L: CEH Refresher

Network Penetration Testing: External

- Port Scanning
  - Port Scan DNS Servers (TCP/UDP 53)
  - Port Scan TFTP Servers (Port 69)
  - Port Scan for NTP Ports (Port 123)
  - Port Scan for SNMP Ports (Port 161)
  - Port Scan for Telnet Ports (Port 23)
  - Port Scan for LDAP Ports (Port 389)
  - Port Scan for Netbios Ports (Ports 135-139, 445)
  - Port Scan for Citrix Ports (Port 1495)
  - Port Scan for Oracle Ports (Port 1521)
  - Port Scan for NFS Ports (Port 2049)
  - Port Scan for Compaq, HP Inside Manager Ports (Ports 2301, 2381)
  - Port Scan for Remote Desktop Ports (Port 3389)
  - Port Scan for Sybase Ports (Port 5000)
  - Port Scan for SIP Ports (Port 5060)
  - Port Scan for VNC Ports (Ports 5900/5800)

- Port Scan for X11 Ports (Port 6000)
- Port Scan for Jet Direct Ports (Port 9100)
- Port Scan for FTP Port (Port 21)
- Port Scan for Web Servers (Port 80)
- Port Scan for SSL Servers (Port 443)
- Port Scan for Kerberos-Active Directory (Port TCP/UDP 88)
- Port Scan for SSH Servers (Port 22)

- External Network Security Countermeasures and Recommendations

Network Penetration Testing: Internal

- Enumeration
  - Perform SMTP Enumeration
  - Sniffing Tool: Wireshark
    - Wireshark: Follow TCP Stream
    - Wireshark: Capture and Display Filters
  - Try to Capture HTTP Traffic
  - Try to Capture FTP Traffic
  - Try to Capture TELNET Traffic
  - Try to Capture POP3 Traffic
  - Try to Capture SMTP Traffic
  - Try to Capture IMAP Email Traffic
  - Try to Capture RDP Traffic
  - Try to Capture VoIP Traffic
  - Wireshark
  - Nessus in Wireshark
  - Wireshark Statistics
  - HTTP Statistics
- OpenVAS Scan Tasks
  - OpenVAS NVTs
  - OpenVAS CVE
  - OpenVAS OS Listing
  - OpenVAS Host Listing

- OpenVAS Topology
- OpenVAS Update
- OpenVAS Results
- OpenVAS Reports

- Vulnerability Report Model
  - Nessus Scan Results
  - Remediation's
  - History
- Sample Vulnerability Assessment Report
  - Sample Security Vulnerability Report - 1
  - Sample Security Vulnerability Report - 2
  - Sample Security Vulnerability Report - 3

Windows Exploitation

- Metasploit File Structure

Other Internal Network Exploitation Techniques

- Attempt to Create a Backdoor Account on the Target Machine
  - Creating Backdoor in Windows System for Future Access and Remote Administration
- Attempt to Plant Rootkits on the Target Machine
- Whitespace Steganography Tool: SNOW
- ARP Poisoning Tools

Advanced Tips and Techniques

- autoroute
- autoroute -s
- Internal Network Security Countermeasures and Recommendations

Network Penetration Testing: Perimeter Devices

- Test the Insertion on the IDS
- Test the IDS using URL Encoding
- Test the IDS using Double Slashes
- Test the IDS using Method Matching
- Test for Win Directory Syntax
- Test for Case Sensitivity

- Connectivity and Performance Monitoring Software for Switch and Router: Switch Center
- Firewall Security Countermeasures and Recommendations
- IDS Security Countermeasures and Recommendations
- Router Security Countermeasures and Recommendations
- Switch Security Countermeasures and Recommendations

Web Application Penetration Testing

- Discover Web Application Default Content
  - Perform Basic Website Footprinting using Netcraft
  - Identify Server-Side Technologies
- Identify the Attack Surface Area
  - Map the Attack Surface
- Test for SQL Injection Vulnerabilities
  - Perform Database Fingerprinting
  - Detect SQL Injection Vulnerabilities by Manipulating a Parameter
  - Determine the Database Schema using UNION-Based SQL Injection
  - Determine the Database Schema using Blind SQL Injection
  - Extract Data using Blind SQL Injection
  - Extract the First Table Entry using Blind SQL Injection
  - Extract Data from Rows using Blind SQL Injection
  - Replicate the Database Structure and Data
  - Extract SQL-Server Password Hashes
  - Test for Hidden Field Parameter Tampering
- Test for Parameter Tampering
  - Test for Directory Traversal
  - Check for Unvalidated Redirects and Forwards
- Test for Weak Cryptography Vulnerabilities
  - Check for Insecure Cryptographic Storage
  - Test Any Account Recovery Function and Remember Me Function
- Tests for Broken Authentication and Authorization Vulnerabilities
  - Perform Session ID Prediction/Brute-forcing

- Perform HTTP Request Tampering
- Perform Authorization Attack – Cookie Parameter Tampering
- Connection String Injection
- Test for Connection String Parameter Pollution (CSPP) Attacks
- Test for Connection Pool DoS

- Test for Web Services Security
  - Perform Web Services Footprinting Attack
  - Test for Web Services XML Poisoning
- Test for Web Server Vulnerabilities
  - Perform Web Server Fingerprinting using httprint
- Web Application Security Countermeasures and Recommendations

Wireless Penetration Testing

- Wireless Local Area Network (WLAN) Penetration Testing
  - Detect Hidden SSIDs
  - Create Ad Hoc Associations with an Unsecured AP
  - Jam the Signal
  - Perform Fragmentation Attack
  - Crack Static WEP Keys
  - Crack WPA-PSK Keys
  - Attempt an MITM Attack
  - Additional Wireless Penetration Testing Tools: Aircrack-ng Suite
  - Create a Direct Connection to the Wireless Access Point
- WLAN Security Countermeasures and Recommendations

Cloud Penetration Testing

- Cloud Security Countermeasures and Recommendations