



TM

EC SA

EC-Council Certified Security Analyst

EC-Council Certified Security Analyst

Course Outline

(Version 10)

Module 00: Penetration Testing Essential Concepts

- Computer Network Fundamentals
 - Computer Network
 - TCP/IP Model
 - Comparing OSI and TCP/IP
 - Types of Networks
 - Local Area Network (LAN)
 - Wide Area Network (WAN)
 - Metropolitan Area Network (MAN)
 - Personal Area Network (PAN)
 - Campus Area Network (CAN)
 - Global Area Network (GAN)
 - Wireless Networks(WLAN)
 - Advantages
 - Disadvantages
 - Network Topologies
 - Physical Topology
 - Bus Topology

- Ring Topology
- Tree Topology
- Star Topology

- Mesh Topology

- Hybrid Topology

- Logical Topology

Network Hardware Components

Types of LAN Technology

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- Asynchronous Transfer Mode (ATM)
- Power over Ethernet (PoE)
- Specifications of LAN

Technology Types of cables

- Fiber Optic Cable
- Coaxial Cable
- CAT 3 and CAT 4
- CAT 5
- CAT 5e and CAT 6
- 10/100/1000BaseT (UTP Ethernet)

- 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?
Non-DNSSEC-Aware Lookups

- DNSSEC-Aware Lookups
 - Operation of DNSSEC
- Hypertext Transfer Protocol (HTTP)
- Secure HTTP
- Hyper Text Transfer Protocol Secure (HTTPS)
- File Transfer Protocol (FTP)
 - How FTP Works?
 - Hardening FTP Servers
 - FTP Anonymous Access and its Risk
- 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
 - Cisco Reverse 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) Transport Layer Protocols
- Transmission Control Protocol (TCP)

- TCP Header Format
- TCP Services
 - Simplex
 - Half-duplex
 - Full-duplex
- User Datagram Protocol (UDP)
 - UDP Operation
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

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
 - DNS Issues
 - Mobile IP
- 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) 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
 - Static Routing
 - Dynamic Routing
 - Network Address Translation (NAT)
 - Benefits of NAT
 - Port Address Translation (PAT) VLAN
 - Advantages ○
 - Disadvantages
 - Security implications of VLANs
 - Shared Media Network
 - Advantages ○
 - Disadvantages
 - Switched Media Network
 - Advantages
 - Disadvantages
- Network Security Controls
 - Access Control
 - Access Control Terminology
 - Access Control Principles ○
 - Access Control System
 - Administrative Access Control
 - Physical Access Controls
 - Technical Access Controls
 - Types of Access Control
 - Discretionary Access Control (DAC)
 - Mandatory Access Control (MAC)
 - Role-based Access
 - Network Access Control List
 - User Identification, Authentication, Authorization and Accounting
 - Types of Authentication
 - Password Authentication

- Two-factor Authentication
- Biometrics
 - Biometric Identification Techniques
 - Fingerprinting
 - Retinal Scanning
 - Iris Scanning
 - Vein Structure Recognition
 - Face Recognition
 - Voice Recognition
- Smart Card Authentication
- Single Sign-on (SSO)
- Types of Authorization Systems
 - Centralized Authorization
 - Implicit Authorization
 - Decentralized Authorization
 - Explicit Authorization
- Authorization Principles
 - Least privilege
 - Separation of duties
- Encryption
 - Types of Encryption
 - Symmetric Encryption
 - Asymmetric Encryption
 - Encryption Algorithms
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - RC4, RC5, RC6 Algorithms
- Hashing: Data Integrity
 - Message Digest Function
 - MD5
 - 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 Firewalls
- Circuit Level Gateways
- Application Level Gateways
- Stateful Multilayer Inspection Firewalls

Packet Filtering

- Address Filtering
- Network Filtering

Firewall Policy

Periodic Review of Information Security Policies

Firewall Implementation

- Appliance-based firewall
- Commercial operating system

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

- Network-Based Intrusion Detection Systems (NIDS)
- Host-Based Intrusion Detection Systems (HIDS)

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)
 - NFS Host and File Level Security
 - UID/GUID Manipulation
- Windows Security
 - Patch Management
 - Configuring an Update Method for Installing Patches
 - 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
 - ACL (Access Control list)
 - Secure Object Contain Two Types of ACL
 - Implementation Of ACL
 - Disabling Unused System Services
 - Finding Suspicious/Hidden/Interesting Files
 - File System Security
 - Setting Access Controls and Permission
 - 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)
 - Master Browser

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
 - Host-based access control
 - User-based access control
 - Cookie-based access control

■ Virtualization

Introduction to Virtualization

Characteristics of Virtualization

Benefits of Virtualization

Common Virtualization Vendors

Virtualization Security 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
 - - 1xx: Informational
 - - 2xx: Success
 - - 3xx: Redirection
 - - 4xx: Client Error
 - - 5xx: Server Error
 - HTTP Header Fields
 - - General Header
 - - Request Header
 - - Response Header
 - - Entity Header

An overview to HTTPS Protocol

Encoding and Decoding

- Encoding Techniques
 - - ASCII
 - - Unicode
 - - HTML Encoding
 - - Hex/ Base 16 Encoding
 - - URL Encoding

- Base64
 - 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 Frameworks and their Vulnerabilities
 - .NET Framework
 - J2EE Framework
 - ColdFusion
 - RubyOnRail
 - AJAX
- Web API's
 - Common Gateway Interface (CGI)
 - Common Gateway Interface (CGI) Attacks
 - PHF Attack
 - Test Attack
 - Count Attack
 - JJ Attack
 - Compass Attack
 - CGI Request Attack

Application interfaces: ISAPI

Filters Apache Modules

- Web Sub Components

Web applications components

- Web browser (or client) ○

- Web application server ○

Database server

Thick and Thin

Clients ○ Thin clients

- Thick client

- Smart Clients (rich clients)

Applet

Servlet

ActiveX

Flash Application

- Web Application Security
Mechanisms Input Validation

- Why Input Validation?

Input Filtering

- Input Filtering Technique

- Black Listing

- White Listing

Authentication and Authorization

Session Management

- Session Tokens

- Authentication Tokens

Error Handling

Web Application Fuzz Testing

- Drawbacks of Fuzzing

Source Code Review

- Manual Code Review

- Automated Code Review

Threat Modeling

Threat Modeling Approaches

- Asset Centric
- Attack Centric
- Software/Design Centric
- Hybrid Centric

Threat Modeling Process

- Security Objectives ○

Application Overview

- Application Decomposition
- Identify Threats
- Identify and Prioritize Vulnerabilities

Web Application Connection with Underlying Databases

- SQL Sever
 - Data Controls used for SQL Server Connection
- MS ACCESS
- MySQL
- ORACLE

- Working of Most Common Information Security Attacks Parameter/Form Tampering

Directory Traversal

SQL Injection Attacks

Command Injection Attacks

- Shell Injection

File Injection Attack

What is LDAP Injection?

- How LDAP Injection Works?

Hidden Field Manipulation Attack

Cross-Site Scripting (XSS) Attacks

- Stored XSS (AKA Persistent or Type I)
- Reflected XSS (AKA Non-Persistent or Type II)

Course Outline

- DOM Based XSS (AKA Type-0)
 - Cross-site Scripting Attack Scenario
 - Attack through Phishing
 - Attack in Blog Posting
 - 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
 - Dictionary Attack
 - Brute Forcing Attacks
 - Hybrid Attack
 - Birthday Attack
 - Rainbow Table Attack

Network Sniffing

Man-in-the-Middle Attack

Replay Attack

Privilege Escalation

- Vertical Privilege Escalation
- Horizontal 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
 - Simple Buffer Overflow in C
 - 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)

Sarbanes Oxley Act (SOX)

Gramm-Leach-Bliley Act (GLBA)

The Digital Millennium Copyright Act (DMCA)

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

Module 01: Introduction to Penetration Testing and Methodologies

- What is Penetration Testing?
- Benefits of Conducting a Penetration Test
- ROI for Penetration Testing

Course Outline

- How Penetration Testing Differs from Ethical Hacking?
 - Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
 - Types of Penetration Testing
 - Black-box Penetration Testing
 - Blind Testing
 - Double-Blind Testing
 - White-box Penetration Testing
 - Announced Testing
 - Unannounced Testing
 - Grey-box Penetration Testing
- Penetration Testing: Cost and Comprehensiveness
 - Selecting an Appropriate Testing Type
- Different Ways of Penetration Testing
 - Automated Penetration Testing
 - Manual Penetration Testing
- Selecting the Appropriate Way of Penetration Testing
- Common Areas of Penetration Testing
 - Network Penetration Testing
 - Web Application Penetration Testing
 - Social Engineering Penetration Testing
 - Wireless Network Penetration Testing
 - Mobile Device Penetration Testing
 - Cloud Penetration Testing
- Penetration Testing Process
 - Defining the Scope
 - Performing the Penetration Test
 - Reporting and Delivering Results
- Penetration Testing Phases
 - Pre-Attack Phase
 - Attack Phase
 - Post-Attack Phase
- Penetration Testing Methodologies
 - Proprietary Methodologies

- Open-Source Methodologies
 - Need for a Methodology
 - LPT Penetration Testing Methodology
 - EC-Council's LPT Penetration Testing Methodology
 - What Makes a Licensed Penetration Tester? Modus Operandi
- Preparation
 - Penetration Testing Essentials
 - What Makes 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 Pen Tester
 - Communication Skills of a Penetration Tester
 - Profile of a Good Penetration Tester
 - Responsibilities of a Penetration Tester
 - Risk Associated with the Penetration Testing
 - Type of Risks Arises during Penetration Testing
 - Technical Risk
 - Organizational Risks
 - Legal Risks
 - Dealing with Risk Associated with Penetration Testing and Avoiding Potential DoS Conditions

Module 02: Penetration Testing Scoping and Engagement Methodology

- Penetration Testing: Pre-engagement Activities
 - Pre-engagement Activities
 - Request for Proposal (RFP)
 - How Pen Testing Engagement Process Initiates Proposal Submission
 - Common Evaluation Criteria for the Proposals
- Preparing Response Requirements for Proposal Submission

- Identifying scope, approach and methodology
 - Send Preliminary Information Request Document to the Client
 - List the Goals of Penetration Testing
 - Scoping a Penetration Test
 - Conduct Pen Test Scoping Meeting
 - Sample Questionnaires
 - Network Penetration
 - Test Social Engineering
 - Web Application Penetration Test
 - Wireless Network Penetration Test
 - Questions for Business Unit Managers
 - Questions for Systems Administrators
 - Identify the Type of Testing to Be Carried Out
 - Identify the Areas of Infrastructure to Tested
 - Identify the Targets to be Tested
 - Identify the Items to be Tested Within Organization
 - Identify the Targets that Requires Dealing with Third parties, if any
 - Identify the Targets that Requires Dealing with Other Countries, if any
 - Understand Client Assessment Requirements
 - List the Tests that will not be Carried Out
 - Obtain a Detailed Proposal of Tests to Be Carried Out and not Carried out
 - Decide on Desired Depth for Penetration Testing
- Determining project deliverables
 - Identify How the Final Report will be Delivered
 - Identify the Reports to Be Delivered after the Pen Test
- Determining project schedule
 - Specify finite duration for the test to be conducted
- Understanding staffing requirements
 - Project Team Staffing
- Proposing detailed and itemized pricing
 - Estimate Cost for Your Pen Test Engagement
- Submitting proposal
 - Submitting the Proposal

Course Outline

- Setting the Rules of Engagement
(ROE) Rules of Engagement (ROE)
Conduct brainstorming sessions with the top management and technical teams
- Establishing communication lines: Identify the Details of the Key Contact
List the Contacts at the Client Organization Who Will be in Charge of the Pen Testing Project
Obtain the Details of the Key Contact at the Client's Company, in case of an Emergency
Points-of-Contact Template
Conduct Initial Teleconference with Target Point of Contact (TPOC)
- Timeline
Estimating Timeline for the Engagement
Metrics for Time Estimation
Draft a Timeline for the Penetration Testing
Project Work Breakdown Structure or Task List
Penetration Testing Schedule
- Time/Location
Identify the Reporting Time Scales
Identify the Office Space/Location Where Your Team Will Work during This Project
- Frequency of meetings
Meeting with the Client
- Time of Day
Deciding Time of day for the test
- Identify who can help you?
Identify the Local Human Resources Required for the Pen Test
Identify the Client's IT Security Admin Who Will Help You with the Pen Test (if Possible)
Decide Other Internal Employees Who Will Help You in the Pen Test (if Possible)
- ROE Document
XSECURITY: Sample Rules of Engagement Document
Rules of Engagement Template (Sample)
Getting Engagement Letter from Client
- Handling Legal Issues in Penetration Testing Engagement
Hire a Lawyer Who Can Handle Your Penetration Testing Legal Documents
- Penetration Testing Contract

Drafting Contracts

Sample Penetration Testing Contract

Create Penetration Testing “Rules of Behavior”

Create a Get-Out-of-Jail-Free Card

List Permitted Items in Legal Agreement

- Create Confidentiality and Non-Disclosure Agreements (NDAs) Clauses

- Prepare a Non-Disclosure Agreement (NDA) and Have the Client Sign

- It Define Liability Issues

Define Negligence Claim

Define Limitations of the Contract

Have the Engagement Letter Vetted by Your Lawyer

- Obtain (if Possible) Liability Insurance from a Local Insurance

- Firm Conduct Independence, Check of the Team Members

List the Known Waivers/Exemptions

List the Contractual Constraints in the Penetration Testing Agreement

■ Preparing for Test

- Review Engagement Letter

- Create Engagement Log

Kickoff Meeting

Prepare Statement of Work (SOW)

Identify the List the Security Tools You Will Be required for the Penetration Test

- Identify the List the Hardware and Software Requirements for the Penetration

- Test Prepare 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

Send Internal Control Questionnaires (ICQ) to the Client (Provided by Client [PBC] Information)

Request Previous Penetration Testing/Vulnerability Assessment Reports (If Possible)

Create Data Use Agreement (DUA) (If Required)

Conduct a Working Teleconference

Send the Final Engagement Control Documents to the Client for Signature

Obtain Penetration Testing Permission from the Company's Stakeholders

Obtain Special Permission, If Required, from the Local Law Enforcement Agency

Obtain Temporary Identification Cards from the Client for Team Members Involved in the Process

Gather Information about the Client Organization's History and Background

Visit and Become Familiar with the Client Organization's Premises and Environment

Identify the Local Equipment Required for the Pen

Test Conduct a Mission Briefing

- Handling Scope Creeping during pen test
Scope Creeping

Module 03: Open-Source Intelligence (OSINT) Methodology

- OSINT Gathering Steps
- OSINT Through World Wide Web(WWW)
 - Find the Domain and Sub-domains of the Target Find Similar or Parallel Domain Names
 - Refine your Web Searches using Advanced Operators
 - Footprint the Target using Shodan
 - Find the Geographical Location of a Company
 - List Employees and their Email Addresses
 - Identify the Key Email Addresses through Email
 - Harvesting List Key Personnel of the Company
- Use People Search Online Services to Collect the Information
 - Browse Social Network Websites to Find Information about the Company and Employees Use Web Investigation Tools to Extract Sensitive Data about the Company
- Identify the Type of Network Devices used in Organization
- Example of Company's Job Postings
- Look for the Sensitive Information in Email Headers
- Look for the Valuable Information in the NNTP USENET Newsgroups

- Other Useful Footprinting Activities to find Information about Target
 - OSINT through Website Analysis
 - Search Contact Information, Email Addresses, and Telephone Numbers from Company Website
 - Search for Web Pages Posting Patterns and Revision Numbers
 - Search the Archive.org for Old Information about the Company
 - Monitor Web Updates Using Website-Watcher
 - Examine HTML Source of the Web Pages
 - OSINT Through DNS Interrogation
 - Perform Whois Lookup
 - Find IP Address Block Allocated to the Organization
 - Find the DNS Records for Domain
 - Perform Reverse Lookup
 - Perform DNS Zone Transfer
 - Draw A Network Diagram Using Traceroute
 - Analysis Create Topological Map of the Network
 - Automating your OSINT Effort Using Tools/Frameworks/Scripts
 - Maltego
 - FOCA
 - Fsociety
 - PENTMENU

Module 04: Social Engineering Penetration Testing Methodology

- Social Engineering Penetration Testing
 - Skills Required to Perform Social Engineering Pen Test
 - Common Targets of Social Engineering Pen Test
 - Do Remember: Before Social Engineering Pen Test
 - Black Box or White Box?
 - Social Engineering Penetration Testing Steps
- 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

Launch a Phishing Campaign

- Social Engineering Penetration testing using Telephone Attack Vector Attempt Social Engineering Using the Phone (Vishing)
 - Example of Social Engineering Using the Phone
- 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 Conversation in Communal Areas/ Cafeteria
 - Identify “Disgruntled Employees” and Engage in Conversation to Extract Sensitive Information
- Attempt Eavesdropping
 - Try to Shoulder Surf Users Logging On
 - Attempt Media Dropping
- Attempt Dumpster Diving

Module 05: Network Penetration Testing Methodology - External

- Network Penetration Testing
 - External vs. Internal Penetration Testing
 - External Network Penetration Testing
 - Internal Network Penetration Testing
 - Network Penetration Testing Process
- White, Black or Grey-box Network Penetration Testing? White Box Penetration Testing
 - Black Box Penetration Testing
 - Gray Box Penetration Testing
- External Network Penetration Testing Steps
 - Port Scanning
 - Scan the Network to Discover Live Hosts
 - Checking 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 XMAS Scan on the Target and See the Response

Use FIN Scan on the Target and See the Response

Use NULL Scan on the Target and See the Response

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 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 Test for X11 Ports (Port 6000)

Port Scan for Jet Direct Ports (Port 9100)

Port Scan for FTP Data (Port 20)

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)

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

Module 06: Network Penetration Testing Methodology - Internal

- Internal Network Penetration Testing
 - Why Internal Network Penetration Testing?
 - Internal Network Penetration Testing Steps
 - Footprinting
 - Identify the Internal Domains Identify Hosts
 - Identify the Internal IP Range of Your Subnet
 - Detect All the Other Available Subnets
- Network Scanning
 - Scan a Network
 - IP Addresses Scan
 - Multiple IP Addresses Scan
 - Subnet Scan
 - Live Host Scan
 - Port Scan
 - Common Ports List
 - Other Network Scanning Tools
- OS and Service Fingerprinting
 - Identify the OS
 - Identify the Services
 - Identify the services running on open ports
 - Identifying IPsec Enabled Devices and Hosts

- Identifying VoIP Enabled Devices and Hosts
- Perform SSH Fingerprinting

Map the Internal Network

- Enumeration

Perform Service Enumeration

Enumeration Tools

Enumeration Techniques and Tools

- Perform NetBIOS Enumeration
- Perform SNMP Enumeration
- Perform LDAP Enumeration
- 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
- Perform IPv6 Enumeration

Sniff the Network

- Sniffing Tool: Wireshark
 - Wireshark: Follow TCP Stream
 - Wireshark: Capture and Display Filters
- Tcpdump: Capture Traffic using tcpdump
 - 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

- Vulnerability Assessment

Perform Internal Vulnerability Assessment

Perform Network Vulnerability Scanning Using Network Vulnerability Scanners
Perform Vulnerability Scanning Using Nmap

Vulnerability Assessment Reports

- Sample Vulnerability Assessment Report
- Vulnerability Report Model
- Sample Security Vulnerability Report - 1
- Sample Security Vulnerability Report - 2
- Sample Security Vulnerability Report - 3

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

■ Windows Exploitation

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

■ Unix/Linux Exploitation

Identify Local/Remote Exploit to Gain Root Access
Try to Gain Access to Linux using Remote Shell

Extract User Accounts

Extract the Password Hashes
Crack the Password Hashes

Try to Gain Unauthorized Access through UID/GUID Manipulation

■ Other Internal Network Exploitation Techniques Attempt Replay Attacks

Attempt ARP Poisoning ○
ARP Poisoning Tools

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 Extract the Password Hashes
Try to Crack Password from Hashes
Try to Break-down the Desktop
Lockdown Escalate User Privileges
Reset the Local Administrator or Other User Account Passwords
Attempt to Plant a Software Keylogger to Steal Passwords
Attempt to Plant a Hardware Keylogger to Steal Passwords
Attempt to Plant Spyware on the Target Machine
Attempt to Plant a Trojan on the Target Machine
Attempt to Create a Backdoor Account on the Target Machine
 - Creating Backdoor in Windows System for Future Access and Remote Administration Attempt to Bypass Antivirus Software Installed on the Target Machine
 - Attempt to Send a Virus Using the Target Machine Attempt to Plant Rootkits on the Target Machine Hide Sensitive Data on Target Machines
 - Use Various Steganography Techniques to Hide Files on Target Machines Whitespace Steganography Tool: SNOW
 - 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
 - Attempt Session Hijacking on Telnet Traffic
 - Attempt Session Hijacking on FTP Traffic
 - Attempt Session Hijacking on HTTP Traffic
 - 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

- Kali Linux
- Immunity CANVAS
- Post Exploitation
 - Checking Missing Security Patches and Patch Levels: Linux
 - Checking Missing Security Patches and Patch levels: Windows
 - Cleanup: Resetting into Prevision State

Module 07: Network Penetration Testing Methodology - Perimeter Devices

- Steps for Firewall Penetration Testing
- Steps for IDS Penetration Testing
- Steps for Router Penetration Testing
- Steps for Switch Penetration Testing
- Assessing Firewall Security Implementation
 - Testing the Firewall from Both Sides
 - Find Information about the Firewall
 - Locate the Firewall by Conducting Traceroute
 - Detect Open Ports and Services Allowed through on Firewall using Firewalking
 - Try to pass through 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 Firewall by Spoofing Packets
 - Try to Bypass Firewall by Spoofed Source Port
 - Try to Bypass Firewall by MAC Address Spoofing
 - Try to Bypass Firewall by IP Address Spoofing
 - Try to Bypass Firewall by Varying Packet Size
 - Try to Bypass Firewall by Sending Bad Checksums
 - Try to Bypass 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
 - Try to Bypass the Firewall Using a Proxy Server

Try to Bypass the Firewall Using Source Routing

Try to Bypass Firewall using HTTP Tunneling Method

Try to Bypass Firewall using ICMP Tunneling Method

Try to Bypass Firewall using ACK Tunneling Method Try

to Bypass Firewall using SSH Tunneling Method Try to

Bypass Firewall through MITM Attack

Try to Bypass 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 IDS Using Botnet

Test the Insertion on the IDS

Test the IDS by Sending a Packet to the Broadcast

Address Test the IDS by Sending Inconsistent Packets

Test the IDS for IP Packet Fragmentation

Packet Fragmentation

Test the IDS for Overlapping Fragments

Test the IDS for Ping of Death

Test the IDS for Unicode Evasion

Test the IDS for Polymorphic Shellcode

Try to Evade the IDS by Obfuscating or Encoding the Attack

Payload Check IDS for False-Positive Generation

Test the IDS Using URL Encoding

Test the IDS Using Double Slashes

Test IDS for TTL Evasion

Test the IDS by Sending a Packet to Port

0 Test IDS for UDP Checksum

Test IDS for TCP Retransmissions

Test the IDS by TCP Flag

Manipulation TCP Flags

○ (none) ○

SYN/FIN ○

SYN/RST ○

All Flags

○ SYN/RST/ACK

○ SYN/FIN/ACK

Test IDs for Initial Sequence Number

Prediction Test ID for Backscatter

Test the IDS Using Covert Channels

Test the IDS Using Method Matching

Test the IDS for Reverse Traversal

Test for Self-Referencing Directories

Test for Premature Request Ending

Test for IDS Parameter Hiding

Test IDS for HTTP Misformatting

Test IDS for Long URLs

Test for Win Directory Syntax

Test for Null Method Processing

Test for Case Sensitivity

Try to Bypass 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

Testing for Package Leakage at the

Router 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 Access to Router Console Port

Test for Loose and Strict Source

Routing Test for IP Spoofing

Test for IP Handling

Bugs Test ARP Attacks

Test for Routing Protocol

(RIP) Test for OSPF Protocol

Test BGP Protocol

Test for EIGRP Protocol

Test Router Denial-of-Service Attacks

- Malformed Packet Attack

- Packet Flood Attacks

Test Router's HTTP Capabilities

Test for HTTP Configuration Vulnerabilities in Cisco Routers

Course Outline

- 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
 - Connectivity and Performance Monitoring software for Switch and Router: Switch Center
 - Router and Switch Security Auditing Tool: Traffic IQ Professional

Module 08: Web Application Penetration Testing Methodology

- White Box or Black Box?
 - Web Application Penetration Testing
 - Web Application Security Frame
 - Security Frame vs. Vulnerabilities vs. Attacks
 - Web Application Penetration Testing Steps
- Discover Web Application Default Content
 - Identify Functionality
 - Perform Basic Website Footprinting Using Netcraft
 - Perform Web Enumeration Using Whatweb

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
 - 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 Can Not Find
 - Discover Hidden Content of the Target Website
 - Extracting Common Word List from the Target
- Conduct Web Vulnerability Scanning
 - Conduct Web Vulnerability Assessment
 - Web Application Vulnerability Scanners
 - WebInspect
 - IBM Security AppScan
 - Qualys
 - Perform Web Application Fuzz Testing
- Identify the Attack Surface Area
 - Identify Entry Points for User Input
 - Map the Attack Surface
- Tests 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 the Database Schema Using UNION-Based SQL Injection
- Determine the Database Schema Using Blind SQL Injection
- Determine Privileges, DB Structure and Column Names
- Example: Identifying Tables Using SQLMAP
- Example: Identifying Columns Using SQLMAP
- Extract Data Using Blind SQL Injection
- Extract the First Table Entry Using Blind SQL Injection
- Extract Data from Rows Using Blind SQL Injection
- Example: Extract Data From Database Tables Using SQLMAP
- Example: Extract Authentication Credentials Using SQLMAP
- Insert, Update, 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
- Replicate the Database Structure and Data
- Use OPENROWSET to Escalate Privileges on The Microsoft SQL Server
- Extract SQL-Server Password Hashes
- Tests for XSS Vulnerabilities
- Manual Test for XSS Vulnerabilities
- Automated Test for XSS Vulnerabilities
- Tests for Parameter Tampering
- Test for URL Parameter Tampering
- Test for Hidden Field Parameter
- Tampering Test for Directory Traversal

- Check for Unvalidated Redirects and Forwards
- Test for Unrestricted File Upload Vulnerability
- Perform HTTP Response Splitting/CRLF Injection Attack
- Tests for Weak Cryptography Vulnerabilities
 - Check for Insufficient Transport Layer Protection
 - Check for Weak SSL Ciphers
 - Check for Insecure Cryptographic Storage
 - 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
- Tests for Client-Side Scripting 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
 - Test Any Account Recovery Function and Remember Me Function
 - Perform Password Brute-forcing
 - Perform Session ID Prediction/Brute-forcing

Perform Authorization Attack

Perform HTTP Request Tampering

Perform Authorization Attack – Cookie Parameter Tampering

Understand the Access Control Requirements

Testing with Multiple Accounts

Testing with Limited Access

Test for Insecure Access Control Methods

Test Segregation in Shared Infrastructures

Test Segregation between ASP-hosted Applications

Connection String Injection

Test for Connection String Parameter Pollution (CSPP) Attacks

Test for Connection Pool DoS

- 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 Footprinting Attack

Perform Web Services Probing Attacks

Test for XML Structure

Test for XML Content-level

Test for Web Services XML Poisoning

Test for WS HTTP GET Parameters/REST
Attacks Test for Suspicious SOAP Attachments

Test for XPath Injection Attack

Test for WS Replay

- Tests 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
- Tests for Web Server Vulnerabilities
 - Perform HTTP Service Discovery
 - Perform Banner Grabbing to Identify the Target Web Server
 - Perform Web Server Fingerprinting using httprint
 - 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
- Tests for Thick Clients Vulnerabilities
 - Pen Testing Thick Clients
 - Dynamic Testing
 - System Testing
 - Static Testing

Module 09: Database Penetration Testing Methodology

- Database Penetration Testing Steps
- 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
 - Attempt to Brute-Force Password Hashes from the Oracle Database
- Database Exploitation: MS SQL SERVER
 - Test for Buffer Overflow in the pwencrypt() Function
 - Test for Heap/Stack Buffer Overflow in SSRS
 - Test for Buffer Overflows in the Extended Stored Procedures
 - Test for Service Account Registry Key
 - Test the Stored Procedure to Run Web Tasks
 - Brute Force SA Account

Course Outline

- Database Exploitation: MySQL
 - Try to Log in Using Default/ Common Passwords
 - Brute Force Accounts Using Dictionary Attack
 - Database Password Cracking Tool
 - Cain & Abel
 - HexorBase
 - Database Password Cracking Tools

Module 10: Wireless Penetration Testing Methodology

- Wireless Penetration Testing
 - WLAN Penetration Testing Steps
 - RFID Penetration Testing Steps
 - NFC Penetration Testing Steps
 - Mobile Device Penetration Testing Steps
 - IoT Penetration Testing Steps
- Wireless Local Area Network (WLAN) Penetration Testing
 - Discover the Wireless Networks
 - Detect Hidden SSIDs
 - Check Physical Security of AP
 - Detect Wireless Connections
 - Types of scanning methodologies
 - Active Scanning
 - Passive Scanning
 - Active Wireless Scanner: inSSIDer Office
 - Sniff Traffic Between the AP and Linked Devices
 - Create Ad Hoc Associations with an Unsecured AP
 - Create a Rogue Access Point and Try to Create a Promiscuous Client
 - Use a Wireless Honeytrap to Discover Vulnerable Wireless Clients
 - Perform a Denial-of-Service Attack (De-authentication Attack)
 - Attempt Rapid Traffic Generation Jam the Signal
 - Attempt Single-Packet Decryption

Perform Fragmentation Attack

Perform an ARP Poisoning Attack

Try to Inject the Encrypted

Packet Crack Static WEP Keys

Crack WPA-PSK Keys

Crack WPA/WPA2 Enterprise

Mode Crack WPS PIN

Check for MAC Filtering

Spoof the MAC Address

Create a Direct Connection to the Wireless Access Point

Attempt an MITM Attack

Test for Wireless Driver Vulnerabilities

Additional Wireless Penetration Testing

Tools: ○ Aircrack-ng Suite

○ Kismet

○ AirMagnet WiFi Analyzer

○ 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

RFID Hacking Tool ○

Tastic RFID Thief ○

RFDump

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 an MITM Attack

- 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
 - 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

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

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 Penetration Testing Using Smartphone Pentest Framework
- 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
- IoT Penetration Testing
 - Introduction to IoT Penetration
 - Testing IoT Attack Surface
- Testing an IoT Device for an Insecure Web Interface
 - Testing an IoT Device for Poor Authentication/Authorization
 - Testing an IoT Device for Poor Insecure Network Services
 - Testing an IoT Device for Lack of Transport Encryption
 - Testing an IoT Device for Privacy Concerns

Testing an IoT Device for an Insecure Cloud Interface
Testing an IoT Device for Insecure Mobile Interface
Testing an IoT Device for Insufficient Security Configurability
Testing an IoT Device for Insecure Software/Firmware
Testing an IoT Device for Poor Physical Security
IoT Penetration Testing Tool: HardSploit

Module 11: Cloud Penetration Testing Methodology

- Distribution of Public Cloud Services: AWS, Azure, Google Clouds Are on TOP Among Others
 - 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 Limitations
 - Cloud Specific Penetration Testing
 - Cloud Reconnaissance
 - Identify the Type of Cloud to be Tested
 - Identify What to be Tested in Cloud Environment
 - Identify the Tools for Penetration Test
 - Identify What Allowed to be Tested in Cloud Environment
 - Identify Which Tests are Prohibited
 - AWS's Provision for Penetration Testing
 - Azure's Provision for Penetration Testing
 - Google Cloud's Provision for Penetration Testing
 - Identify Date and Time for Penetration Test
- Cloud Specific Penetration Testing
 - 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 Cloud Services in the URL
- Check whether Files Stored on 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 Cloud Service
- Test for Virtualization Management (VM) Security
 - Check Audit and Evidence-Gathering Features in the Cloud Service
 - Perform Automated Cloud Security Testing
- Recommendations for Cloud Testing

Module 12: Report Writing and Post Testing Actions

- Penetration Testing Deliverables
 - Goal of the Penetration Testing Report
- Types of Pen Test Reports
 - Executive Report
 - Host Report
 - Client-Side Test
 - Report User Report
 - Vulnerability Report
 - Activity Report
- Characteristics of a Good Pen Testing Report
- Writing the Final Report
 - Plan the Report
 - Collect and Document the Information
 - Write a Draft Report
 - Review and Finalize the Report
 - Sample Pen Testing Report Format
 - Report Format – Cover Letter
- Document Properties/Version History

Course Outline

- **Table of Contents/Final Report**
 - Summary of Execution
 - Scope of the Project
 - Evaluation Purpose/System Description
 - Assumptions/Timeline
 - Summary of Evaluation, Findings, and Recommendations
 - Methodologies
 - Planning
 - Exploitation
 - Reporting
 - Comprehensive Technical Report
 - Result Analysis
 - Recommendations
 - Appendices
 - Sample Appendix
 - Penetration Testing Report Analysis
 - Report on Penetration Testing
 - Pen Test Team Meeting
 - Research Analysis
 - Pen Test Findings
 - Rating Findings

High Criticality Findings

Medium Criticality Findings

Low Criticality Findings

Example of Finding – I

Example of Finding – II

- **Analyze**
 - Prioritize Recommendations
 - Delivering Penetration Testing Report
 - Cleanup and Restoration
 - Report Retention

Destroy the Report

Sign-off Document

Course Outline

- Sign-off Document Template
- Post-testing Actions for Organizations
 - 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