Ethical Hacking and Countermeasures

Course Outline

(Version 10)

Module 01: Introduction to Ethical Hacking

Information Security Overview

- Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds
- Essential Terminology
- Elements of Information Security
- The Security, Functionality, and Usability Triangle

Information Security Threats and Attack Vectors

- Motives, Goals, and Objectives of Information Security Attacks
- Top Information Security Attack Vectors
- Information Security Threat Categories
- Types of Attacks on a System
- Information Warfare

Hacking Concepts

- What is Hacking?
- Who is a Hacker?
- Hacker Classes
- Hacking Phases
    - Reconnaissance
    - Scanning

  - Gaining Access
  - Maintaining Access
  - Clearing Tracks

Ethical Hacking Concepts

- What is Ethical Hacking?
- Why Ethical Hacking is Necessary
- Scope and Limitations of Ethical Hacking
- Skills of an Ethical Hacker

Information Security Controls

- Information Assurance (IA)
- Information Security Management Program
- Enterprise Information Security Architecture (EISA)
- Network Security Zoning
- Defense-in-Depth
- Information Security Policies
  - Types of Security Policies
  - Examples of Security Policies
  - Privacy Policies at Workplace
  - Steps to Create and Implement Security Policies
  - HR/Legal Implications of Security Policy Enforcement
- Physical Security
  - Types of Physical Security Control
  - Physical Security Controls
- What is Risk?
  - Risk Management
  - Key Roles and Responsibilities in Risk Management
- Threat Modeling
- Incident Management
  - Incident Management Process
  - Responsibilities of an Incident Response Team
- Security Incident and Event Management (SIEM)

  - SIEM Architecture
- User Behavior Analytics (UBA)
- Network Security Controls
  - Access Control
  - Types of Access Control
  - User Identification, Authentication, Authorization and Accounting
- Identity and Access Management (IAM)
- Data Leakage
  - Data Leakage Threats
  - What is Data Loss Prevention (DLP)?
- Data Backup
- Data Recovery
- Role of AI/ML in Cyber Security

Penetration Testing Concepts

- Penetration Testing
- Why Penetration Testing
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
- Blue Teaming/Red Teaming
- Types of Penetration Testing
- Phases of Penetration Testing
- Security Testing Methodology

Information Security Laws and Standards

- Payment Card Industry Data Security Standard (PCI-DSS)
- ISO/IEC 27001:2013
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- The Digital Millennium Copyright Act (DMCA)
- Federal Information Security Management Act (FISMA)
- Cyber Law in Different Countries

Module 02: Footprinting and Reconnaissance

Footprinting Concepts

- What is Footprinting?
- Objectives of Footprinting

Footprinting through Search Engines

- Footprinting through Search Engines
- Footprint Using Advanced Google Hacking Techniques
- Information Gathering Using Google Advanced Search and Image Search
- Google Hacking Database
- VoIP and VPN Footprinting through Google Hacking Database

Footprinting through Web Services

- Finding Company’s Top-level Domains (TLDs) and Sub-domains
- Finding the Geographical Location of the Target
- People Search on Social Networking Sites and People Search Services
- Gathering Information from LinkedIn
- Gather Information from Financial Services
- Footprinting through Job Sites
- Monitoring Target Using Alerts
- Information Gathering Using Groups, Forums, and Blogs
- Determining the Operating System
- VoIP and VPN Footprinting through SHODAN

Footprinting through Social Networking Sites

- Collecting Information through Social Engineering on Social Networking Sites

Website Footprinting

- Website Footprinting
- Website Footprinting using Web Spiders
- Mirroring Entire Website
- Extracting Website Information from https://archive.org
- Extracting Metadata of Public Documents
- Monitoring Web Pages for Updates and Changes

Email Footprinting

- Tracking Email Communications
- Collecting Information from Email Header
- Email Tracking Tools

Competitive Intelligence

- Competitive Intelligence Gathering
- Competitive Intelligence - When Did this Company Begin? How Did it Develop?
- Competitive Intelligence - What Are the Company's Plans?
- Competitive Intelligence - What Expert Opinions Say About the Company
- Monitoring Website Traffic of Target Company
- Tracking Online Reputation of the Target

Whois Footprinting

- Whois Lookup
- Whois Lookup Result Analysis
- Whois Lookup Tools
- Finding IP Geolocation Information

DNS Footprinting

- Extracting DNS Information
- DNS Interrogation Tools

Network Footprinting

- Locate the Network Range
- Traceroute
- Traceroute Analysis
- Traceroute Tools

Footprinting through Social Engineering

- Footprinting through Social Engineering
- Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Footprinting Tools

- Maltego
- Recon-ng
- FOCA

- Recon-Dog
- OSRFramework
- Additional Footprinting Tools

Countermeasures

- Footprinting Countermeasures

Footprinting Pen Testing

- Footprinting Pen Testing
- Footprinting Pen Testing Report Templates

Module 03: Scanning Networks

Network Scanning Concepts

- Overview of Network Scanning
- TCP Communication Flags
- TCP/IP Communication
- Creating Custom Packet Using TCP Flags
- Scanning in IPv6 Networks

Scanning Tools

- Nmap
- Hping2 / Hping3
  - Hping Commands
- Scanning Tools
- Scanning Tools for Mobile

Scanning Techniques

- Scanning Techniques
  - ICMP Scanning - Checking for Live Systems
  - Ping Sweep - Checking for Live Systems
    - Ping Sweep Tools
  - ICMP Echo Scanning
  - TCP Connect / Full Open Scan
  - Stealth Scan (Half-open Scan)
  - Inverse TCP Flag Scanning

    - Xmas Scan
    - ACK Flag Probe Scanning
    - IDLE/IPID Header Scan
    - UDP Scanning
    - SSDP and List Scanning
- Port Scanning Countermeasures

Scanning Beyond IDS and Firewall

- IDS/Firewall Evasion Techniques
    - Packet Fragmentation
    - Source Routing
    - IP Address Decoy
    - IP Address Spoofing
        - IP Spoofing Detection Techniques: Direct TTL Probes
        - IP Spoofing Detection Techniques: IP Identification Number
        - IP Spoofing Detection Techniques: TCP Flow Control Method
        - IP Spoofing Countermeasures
    - Proxy Servers
        - Proxy Chaining
        - Proxy Tools
        - Proxy Tools for Mobile
    - Anonymizers
        - Censorship Circumvention Tools: Alkasir and Tails
        - Anonymizers
        - Anonymizers for Mobile

Banner Grabbing

- Banner Grabbing
- How to Identify Target System OS
- Banner Grabbing Countermeasures

Draw Network Diagrams

- Drawing Network Diagrams
- Network Discovery and Mapping Tools

- Network Discovery Tools for Mobile

Scanning Pen Testing

- Scanning Pen Testing

Module 04: Enumeration

Enumeration Concepts

- What is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate

NetBIOS Enumeration

- NetBIOS Enumeration
- NetBIOS Enumeration Tools
- Enumerating User Accounts
- Enumerating Shared Resources Using Net View

SNMP Enumeration

- SNMP (Simple Network Management Protocol) Enumeration
- Working of SNMP
- Management Information Base (MIB)
- SNMP Enumeration Tools

LDAP Enumeration

- LDAP Enumeration
- LDAP Enumeration Tools

NTP Enumeration

- NTP Enumeration
- NTP Enumeration Commands
- NTP Enumeration Tools

SMTP and DNS Enumeration

- SMTP Enumeration
- SMTP Enumeration Tools
- DNS Enumeration Using Zone Transfer

Other Enumeration Techniques

- IPsec Enumeration
- VoIP Enumeration
- RPC Enumeration
- Unix/Linux User Enumeration

Enumeration Countermeasures

- Enumeration Countermeasures

Enumeration Pen Testing

- Enumeration Pen Testing

Module 05: Vulnerability Analysis

Vulnerability Assessment Concepts

- Vulnerability Research
- Vulnerability Classification
- What is Vulnerability Assessment?
- Types of Vulnerability Assessment
- Vulnerability-Management Life Cycle
    - Pre-Assessment Phase: Creating a Baseline
    - Vulnerability Assessment Phase
    - Post Assessment Phase

Vulnerability Assessment Solutions

- Comparing Approaches to Vulnerability Assessment
- Working of Vulnerability Scanning Solutions
- Types of Vulnerability Assessment Tools
- Characteristics of a Good Vulnerability Assessment Solution
- Choosing a Vulnerability Assessment Tool
- Criteria for Choosing a Vulnerability Assessment Tool
- Best Practices for Selecting Vulnerability Assessment Tools

Vulnerability Scoring Systems

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)

- National Vulnerability Database (NVD)
- Resources for Vulnerability Research

Vulnerability Assessment Tools

- Vulnerability Assessment Tools
    - Qualys Vulnerability Management
    - Nessus Professional
    - GFI LanGuard
    - Qualys FreeScan
    - Nikto
    - OpenVAS
    - Retina CS
    - SAINT
    - Microsoft Baseline Security Analyzer (MBSA)
    - AVDS - Automated Vulnerability Detection System
    - Vulnerability Assessment Tools
- Vulnerability Assessment Tools for Mobile

Vulnerability Assessment Reports

- Vulnerability Assessment Reports
- Analyzing Vulnerability Scanning Report

Module 06: System Hacking

System Hacking Concepts

- CEH Hacking Methodology (CHM)
- System Hacking Goals

Cracking Passwords

- Password Cracking
- Types of Password Attacks
    - Non-Electronic Attacks
    - Active Online Attack
        - Dictionary, Brute Forcing and Rule-based Attack
        - Password Guessing

        - Default Passwords
        - Trojan/Spyware/Keylogger
        - Example of Active Online Attack Using USB Drive
        - Hash Injection Attack
        - LLMNR/NBT-NS Poisoning
    - Passive Online Attack
        - Wire Sniffing
        - Man-in-the-Middle and Replay Attack
    - Offline Attack
        - Rainbow Table Attack
        - Tools to Create Rainbow Tables: rtgen and Winrtgen
        - Distributed Network Attack
- Password Recovery Tools
- Microsoft Authentication
- How Hash Passwords Are Stored in Windows SAM?
- NTLM Authentication Process
- Kerberos Authentication
- Password Salting
- Tools to Extract the Password Hashes
- Password Cracking Tools
- How to Defend against Password Cracking
- How to Defend against LLMNR/NBT-NS Poisoning

Escalating Privileges

- Privilege Escalation
- Privilege Escalation Using DLL Hijacking
- Privilege Escalation by Exploiting Vulnerabilities
- Privilege Escalation Using Dylib Hijacking
- Privilege Escalation using Spectre and Meltdown Vulnerabilities
- Other Privilege Escalation Techniques
- How to Defend Against Privilege Escalation

Executing Applications

- Executing Applications
    - Tools for Executing Applications
- Keylogger
    - Types of Keystroke Loggers
    - Hardware Keyloggers
    - Keyloggers for Windows
    - Keyloggers for Mac
- Spyware
    - Spyware
    - USB Spyware
    - Audio Spyware
    - Video Spyware
    - Telephone/Cellphone Spyware
    - GPS Spyware
- How to Defend Against Keyloggers
    - Anti-Keylogger
- How to Defend Against Spyware
    - Anti-Spyware

Hiding Files

- Rootkits
    - Types of Rootkits
    - How Rootkit Works
    - Rootkits
        - Horse Pill
        - GrayFish
        - Sirefef
        - Necurs
    - Detecting Rootkits
    - Steps for Detecting Rootkits
    - How to Defend against Rootkits

- Anti-Rootkits

- NTFS Data Stream
  - How to Create NTFS Streams
  - NTFS Stream Manipulation
  - How to Defend against NTFS Streams
  - NTFS Stream Detectors
- What is Steganography?
  - Classification of Steganography
  - Types of Steganography based on Cover Medium
    - Whitespace Steganography
    - Image Steganography
      - ✓ Image Steganography Tools
    - Document Steganography
    - Video Steganography
    - Audio Steganography
    - Folder Steganography
    - Spam/Email Steganography
  - Steganography Tools for Mobile Phones
  - Steganalysis
  - Steganalysis Methods/Attacks on Steganography
  - Detecting Steganography (Text, Image, Audio, and Video Files)
  - Steganography Detection Tools

Covering Tracks

- Covering Tracks
- Disabling Auditing: Auditpol
- Clearing Logs
- Manually Clearing Event Logs
- Ways to Clear Online Tracks
- Covering BASH Shell Tracks
- Covering Tracks on Network
- Covering Tracks on OS

- Covering Tracks Tools

Penetration Testing

- Password Cracking
- Privilege Escalation
- Executing Applications
- Hiding Files
- Covering Tracks

Module 07: Malware Threats

Malware Concepts

- Introduction to Malware
- Different Ways a Malware can Get into a System
- Common Techniques Attackers Use to Distribute Malware on the Web
- Components of Malware

Trojan Concepts

- What is a Trojan?
- How Hackers Use Trojans
- Common Ports used by Trojans
- How to Infect Systems Using a Trojan
- Trojan Horse Construction Kit
- Wrappers
- Crypters
- How Attackers Deploy a Trojan
- Exploit Kits
- Evading Anti-Virus Techniques
- Types of Trojans
    - Remote Access Trojans
    - Backdoor Trojans
    - Botnet Trojans
    - Rootkit Trojans
    - E-banking Trojans

        - Working of E-banking Trojans
        - E-banking Trojan: ZeuS
    - Proxy Server Trojans
    - Covert Channel Trojans
    - Defacement Trojans
    - Service Protocol Trojans
    - Mobile Trojans
    - IoT Trojans
    - Other Trojans

Virus and Worm Concepts

- Introduction to Viruses
- Stages of Virus Life
- Working of Viruses
- Indications of Virus Attack
- How does a Computer Get Infected by Viruses
- Virus Hoaxes
- Fake Antiviruses
- Ransomware
- Types of Viruses
    - System and File Viruses
    - Multipartite and Macro Viruses
    - Cluster and Stealth Viruses
    - Encryption and Sparse Infector Viruses
    - Polymorphic Viruses
    - Metamorphic Viruses
    - Overwriting File or Cavity Viruses
    - Companion/Camouflage and Shell Viruses
    - File Extension Viruses
    - FAT and Logic Bomb Viruses
    - Web Scripting and E-mail Viruses
    - Other Viruses

- Creating Virus
- Computer Worms
- Worm Makers

Malware Analysis

- What is Sheep Dip Computer?
- Anti-Virus Sensor Systems
- Introduction to Malware Analysis
- Malware Analysis Procedure: Preparing Testbed
- Static Malware Analysis
  - File Fingerprinting
  - Local and Online Malware Scanning
  - Performing Strings Search
  - Identifying Packing/ Obfuscation Methods
  - Finding the Portable Executables (PE) Information
  - Identifying File Dependencies
  - Malware Disassembly
- Dynamic Malware Analysis
  - Port Monitoring
  - Process Monitoring
  - Registry Monitoring
  - Windows Services Monitoring
  - Startup Programs Monitoring
  - Event Logs Monitoring/Analysis
  - Installation Monitoring
  - Files and Folder Monitoring
  - Device Drivers Monitoring
  - Network Traffic Monitoring/Analysis
  - DNS Monitoring/ Resolution
  - API Calls Monitoring
- Virus Detection Methods
- Trojan Analysis: ZeuS/Zbot

- Virus Analysis: WannaCry

Countermeasures

- Trojan Countermeasures
- Backdoor Countermeasures
- Virus and Worms Countermeasures

Anti-Malware Software

- Anti-Trojan Software
- Antivirus Software

Malware Penetration Testing

- Malware Penetration Testing

Module 08: Sniffing

Sniffing Concepts

- Network Sniffing
- Types of Sniffing
- How an Attacker Hacks the Network Using Sniffers
- Protocols Vulnerable to Sniffing
- Sniffing in the Data Link Layer of the OSI Model
- Hardware Protocol Analyzers
- SPAN Port
- Wiretapping
- Lawful Interception

Sniffing Technique: MAC Attacks

- MAC Address/CAM Table
- How CAM Works
- What Happens When CAM Table Is Full?
- MAC Flooding
- Switch Port Stealing
- How to Defend against MAC Attacks

Sniffing Technique: DHCP Attacks

- How DHCP Works

- DHCP Request/Reply Messages
- DHCP Starvation Attack
- Rogue DHCP Server Attack
- How to Defend Against DHCP Starvation and Rogue Server Attack

Sniffing Technique: ARP Poisoning

- What Is Address Resolution Protocol (ARP)?
- ARP Spoofing Attack
- Threats of ARP Poisoning
- ARP Poisoning Tools
- How to Defend Against ARP Poisoning
- Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
- ARP Spoofing Detection Tools

Sniffing Technique: Spoofing Attacks

- MAC Spoofing/Duplicating
- MAC Spoofing Technique: Windows
- MAC Spoofing Tools
- IRDP Spoofing
- How to Defend Against MAC Spoofing

Sniffing Technique: DNS Poisoning

- DNS Poisoning Techniques
    - Intranet DNS Spoofing
    - Internet DNS Spoofing
    - Proxy Server DNS Poisoning
    - DNS Cache Poisoning
- How to Defend Against DNS Spoofing

Sniffing Tools

- Sniffing Tool: Wireshark
        - Follow TCP Stream in Wireshark
    - Display Filters in Wireshark
    - Additional Wireshark Filters
- Sniffing Tools

- Packet Sniffing Tools for Mobile

Countermeasures

- How to Defend Against Sniffing

Sniffing Detection Techniques

- How to Detect Sniffing
- Sniffer Detection Techniques
  - Ping Method
  - DNS Method
  - ARP Method
- Promiscuous Detection Tools

Sniffing Pen Testing

- Sniffing Penetration Testing

Module 09: Social Engineering

Social Engineering Concepts

- What is Social Engineering?
- Phases of a Social Engineering Attack

Social Engineering Techniques

- Types of Social Engineering
- Human-based Social Engineering
  - Impersonation
  - Impersonation (Vishing)
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
- Computer-based Social Engineering
  - Phishing
- Mobile-based Social Engineering

    - Publishing Malicious Apps
    - Repackaging Legitimate Apps
    - Fake Security Applications
    - SMiShing (SMS Phishing)

Insider Threats

- Insider Threat / Insider Attack
- Type of Insider Threats

Impersonation on Social Networking Sites

- Social Engineering Through Impersonation on Social Networking Sites
- Impersonation on Facebook
- Social Networking Threats to Corporate Networks

Identity Theft

- Identity Theft

Countermeasures

- Social Engineering Countermeasures
- Insider Threats Countermeasures
- Identity Theft Countermeasures
- How to Detect Phishing Emails?
- Anti-Phishing Toolbar
- Common Social Engineering Targets and Defense Strategies

Social Engineering Pen Testing

- Social Engineering Pen Testing
    - Using Emails
    - Using Phone
    - In Person
- Social Engineering Pen Testing Tools

Module 10: Denial-of-Service

DoS/DDoS Concepts

- What is a Denial-of-Service Attack?
- What is Distributed Denial-of-Service Attack?

DoS/DDoS Attack Techniques

- Basic Categories of DoS/DDoS Attack Vectors
- UDP Flood Attack
- ICMP Flood Attack
- Ping of Death and Smurf Attack
- SYN Flood Attack
- Fragmentation Attack
- HTTP GET/POST and Slowloris Attacks
- Multi-Vector Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial-of-Service (DRDoS)

Botnets

- Organized Cyber Crime: Organizational Chart
- Botnet
- A Typical Botnet Setup
- Botnet Ecosystem
- Scanning Methods for Finding Vulnerable Machines
- How Malicious Code Propagates?
- Botnet Trojans

DDoS Case Study

- DDoS Attack
- Hackers Advertise Links to Download Botnet
- Use of Mobile Devices as Botnets for Launching DDoS Attacks
- DDoS Case Study: Dyn DDoS Attack

DoS/DDoS Attack Tools

- DoS/DDoS Attack Tools
- DoS and DDoS Attack Tool for Mobile

Countermeasures

- Detection Techniques
- DoS/DDoS Countermeasure Strategies

- DDoS Attack Countermeasures
    - Protect Secondary Victims
    - Detect and Neutralize Handlers
    - Prevent Potential Attacks
    - Deflect Attacks
    - Mitigate Attacks
    - Post-Attack Forensics
- Techniques to Defend against Botnets
- DoS/DDoS Countermeasures
- DoS/DDoS Protection at ISP Level
- Enabling TCP Intercept on Cisco IOS Software

DoS/DDoS Protection Tools

- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools

DoS/DDoS Penetration Testing

- Denial-of-Service (DoS) Attack Pen Testing

Module 11: Session Hijacking

Session Hijacking Concepts

- What is Session Hijacking?
- Why Session Hijacking is Successful?
- Session Hijacking Process
- Packet Analysis of a Local Session Hijack
- Types of Session Hijacking
- Session Hijacking in OSI Model
- Spoofing vs. Hijacking

Application Level Session Hijacking

- Application Level Session Hijacking
- Compromising Session IDs using Sniffing and by Predicting Session Token
    - How to Predict a Session Token
- Compromising Session IDs Using Man-in-the-Middle Attack

- Compromising Session IDs Using Man-in-the-Browser Attack
  - Steps to Perform Man-in-the-Browser Attack
- Compromising Session IDs Using Client-side Attacks
- Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack
- Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack
- Compromising Session IDs Using Session Replay Attack
- Compromising Session IDs Using Session Fixation
- Session Hijacking Using Proxy Servers
- Session Hijacking Using CRIME Attack
- Session Hijacking Using Forbidden Attack

Network Level Session Hijacking

- TCP/IP Hijacking
- IP Spoofing: Source Routed Packets
- RST Hijacking
- Blind Hijacking
- UDP Hijacking
- MiTM Attack Using Forged ICMP and ARP Spoofing

Session Hijacking Tools

- Session Hijacking Tools
- Session Hijacking Tools for Mobile

Countermeasures

- Session Hijacking Detection Methods
- Protecting against Session Hijacking
- Methods to Prevent Session Hijacking: To be Followed by Web Developers
- Methods to Prevent Session Hijacking: To be Followed by Web Users
- Session Hijacking Detection Tools
- Approaches Vulnerable to Session Hijacking and their Preventative Solutions
- Approaches to Prevent Session Hijacking
- IPSec
  - Components of IPsec
  - Benefits of IPsec

    - Modes of IPsec
    - IPsec Architecture
    - IPsec Authentication and Confidentiality
- Session Hijacking Prevention Tools

Penetration Testing

- Session Hijacking Pen Testing

Module 12: Evading IDS, Firewalls, and Honeypots

IDS, Firewall and Honeypot Concepts

- Intrusion Detection System (IDS)
    - How IDS Detects an Intrusion
    - General Indications of Intrusions
    - Types of Intrusion Detection Systems
    - Types of IDS Alerts
- Firewall
    - Firewall Architecture
    - DeMilitarized Zone (DMZ)
    - Types of Firewalls
    - Firewall Technologies
        - Packet Filtering Firewall
        - Circuit-Level Gateway Firewall
        - Application-Level Firewall
        - Stateful Multilayer Inspection Firewall
        - Application Proxy
        - Network Address Translation (NAT)
        - Virtual Private Network
    - Firewall Limitations
- Honeypot
    - Types of Honeypots

IDS, Firewall and Honeypot Solutions

- Intrusion Detection Tool

    - Snort
        - Snort Rules
        - Snort Rules: Rule Actions and IP Protocols
        - Snort Rules: The Direction Operator and IP Addresses
        - Snort Rules: Port Numbers
    - Intrusion Detection Tools: TippingPoint and AlienVault® OSSIM™
    - Intrusion Detection Tools
    - Intrusion Detection Tools for Mobile
- Firewalls
    - ZoneAlarm Free Firewall 2018 and Firewall Analyzer
    - Firewalls
    - Firewalls for Mobile
- Honeypot Tools
    - KFSensor and SPECTER
    - Honeypot Tools
    - Honeypot Tools for Mobile

Evading IDS

- IDS Evasion Techniques
    - Insertion Attack
    - Evasion
    - Denial-of-Service Attack (DoS)
    - Obfuscating
    - False Positive Generation
    - Session Splicing
    - Unicode Evasion
    - Fragmentation Attack
    - Overlapping Fragments
    - Time-To-Live Attacks
    - Invalid RST Packets
    - Urgency Flag
    - Polymorphic Shellcode

    - ASCII Shellcode
    - Application-Layer Attacks
    - Desynchronization
    - Other Types of Evasion

Evading Firewalls

- Firewall Evasion Techniques
    - Firewall Identification
    - IP Address Spoofing
    - Source Routing
    - Tiny Fragments
    - Bypass Blocked Sites Using IP Address in Place of URL
    - Bypass Blocked Sites Using Anonymous Website Surfing Sites
    - Bypass a Firewall Using Proxy Server
    - Bypassing Firewall through ICMP Tunneling Method
    - Bypassing Firewall through ACK Tunneling Method
    - Bypassing Firewall through HTTP Tunneling Method
        - Why do I Need HTTP Tunneling
        - HTTP Tunneling Tools
    - Bypassing Firewall through SSH Tunneling Method
        - SSH Tunneling Tool: Bitvise and Secure Pipes
    - Bypassing Firewall through External Systems
    - Bypassing Firewall through MITM Attack
    - Bypassing Firewall through Content
    - Bypassing WAF using XSS Attack

IDS/Firewall Evading Tools

- IDS/Firewall Evasion Tools
- Packet Fragment Generator Tools

Detecting Honeypots

- Detecting Honeypots
- Detecting and Defeating Honeypots
- Honeypot Detection Tool: Send-Safe Honeypot Hunter

IDS/Firewall Evasion Countermeasures

- How to Defend Against IDS Evasion
- How to Defend Against Firewall Evasion

Penetration Testing

- Firewall/IDS Penetration Testing
  - Firewall Penetration Testing
  - IDS Penetration Testing

Module 13: Hacking Web Servers

Web Server Concepts

- Web Server Operations
- Open Source Web Server Architecture
- IIS Web Server Architecture
- Web Server Security Issue
- Why Web Servers Are Compromised?
- Impact of Web Server Attacks

Web Server Attacks

- DoS/DDoS Attacks
- DNS Server Hijacking
- DNS Amplification Attack
- Directory Traversal Attacks
- Man-in-the-Middle/Sniffing Attack
- Phishing Attacks
- Website Defacement
- Web Server Misconfiguration
- HTTP Response Splitting Attack
- Web Cache Poisoning Attack
- SSH Brute Force Attack
- Web Server Password Cracking
- Web Application Attacks

Web Server Attack Methodology

- Information Gathering
  - Information Gathering from Robots.txt File
- Web Server Footprinting/Banner Grabbing
  - Web Server Footprinting Tools
  - Enumerating Web Server Information Using Nmap
- Website Mirroring
  - Finding Default Credentials of Web Server
  - Finding Default Content of Web Server
  - Finding Directory Listings of Web Server
- Vulnerability Scanning
  - Finding Exploitable Vulnerabilities
- Session Hijacking
- Web Server Passwords Hacking
- Using Application Server as a Proxy

Web Server Attack Tools

- Metasploit
  - Metasploit Exploit Module
  - Metasploit Payload and Auxiliary Module
  - Metasploit NOPS Module
- Web Server Attack Tools

Countermeasures

- Place Web Servers in Separate Secure Server Security Segment on Network
- Countermeasures
  - Patches and Updates
  - Protocols
  - Accounts
  - Files and Directories
- Detecting Web Server Hacking Attempts
- How to Defend Against Web Server Attacks
- How to Defend against HTTP Response Splitting and Web Cache Poisoning

- How to Defend against DNS Hijacking

Patch Management

- Patches and Hotfixes
- What is Patch Management
- Installation of a Patch
- Patch Management Tools

Web Server Security Tools

- Web Application Security Scanners
- Web Server Security Scanners
- Web Server Security Tools

Web Server Pen Testing

- Web Server Penetration Testing
- Web Server Pen Testing Tools

Module 14: Hacking Web Applications

Web App Concepts

- Introduction to Web Applications
- Web Application Architecture
- Web 2.0 Applications
- Vulnerability Stack

Web App Threats

- OWASP Top 10 Application Security Risks – 2017
    - A1 - Injection Flaws
        - SQL Injection Attacks
        - Command Injection Attacks
            - ✓ Command Injection Example
        - File Injection Attack
        - LDAP Injection Attacks
    - A2 - Broken Authentication
    - A3 - Sensitive Data Exposure
    - A4 - XML External Entity (XXE)

    - A5 - Broken Access Control
    - A6 - Security Misconfiguration
    - A7 - Cross-Site Scripting (XSS) Attacks
        - Cross-Site Scripting Attack Scenario: Attack via Email
        - XSS Attack in Blog Posting
        - XSS Attack in Comment Field
        - Websites Vulnerable to XSS Attack
    - A8 - Insecure Deserialization
    - A9 - Using Components with Known Vulnerabilities
    - A10 - Insufficient Logging and Monitoring
- Other Web Application Threats
    - Directory Traversal
    - Unvalidated Redirects and Forwards
    - Watering Hole Attack
    - Cross-Site Request Forgery (CSRF) Attack
    - Cookie/Session Poisoning
    - Web Services Architecture
    - Web Services Attack
    - Web Services Footprinting Attack
    - Web Services XML Poisoning
    - Hidden Field Manipulation Attack

Hacking Methodology

- Web App Hacking Methodology
- Footprint Web Infrastructure
    - Server Discovery
    - Service Discovery
    - Server Identification/Banner Grabbing
    - Detecting Web App Firewalls and Proxies on Target Site
    - Hidden Content Discovery
    - Web Spidering Using Burp Suite
    - Web Crawling Using Mozenda Web Agent Builder

- Attack Web Servers
- Analyze Web Applications
  - Identify Entry Points for User Input
  - Identify Server- Side Technologies
  - Identify Server- Side Functionality
  - Map the Attack Surface
- Bypass Client-Side Controls
  - Attack Hidden Form Fields
  - Attack Browser Extensions
  - Perform Source Code Review
- Attack Authentication Mechanism
  - User Name Enumeration
  - Password Attacks: Password Functionality Exploits
  - Password Attacks: Password Guessing and Brute-forcing
  - Session Attacks: Session ID Prediction/Brute-forcing
  - Cookie Exploitation: Cookie Poisoning
- Attack Authorization Schemes
  - HTTP Request Tampering
  - Cookie Parameter Tampering
- Attack Access Controls
- Attack Session Management Mechanism
  - Attacking Session Token Generation Mechanism
  - Attacking Session Tokens Handling Mechanism: Session Token Sniffing
- Perform Injection/Input Validation Attacks
- Attack Application Logic Flaws
- Attack Database Connectivity
  - Connection String Injection
  - Connection String Parameter Pollution (CSPP) Attacks
  - Connection Pool DoS
- Attack Web App Client
- Attack Web Services

    - Web Services Probing Attacks
    - Web Service Attacks: SOAP Injection
    - Web Service Attacks: XML Injection
    - Web Services Parsing Attacks
    - Web Service Attack Tools

Web App Hacking Tools

- Web Application Hacking Tools

Countermeasures

- Web Application Fuzz Testing
- Source Code Review
- Encoding Schemes
- How to Defend Against Injection Attacks
- Web Application Attack Countermeasures
- How to Defend Against Web Application Attacks

Web App Security Testing Tools

- Web Application Security Testing Tools
- Web Application Firewall

Web App Pen Testing

- Web Application Pen Testing
    - Information Gathering
    - Configuration Management Testing
    - Authentication Testing
    - Session Management Testing
    - Authorization Testing
    - Data Validation Testing
    - Denial-of-Service Testing
    - Web Services Testing
    - AJAX Testing
- Web Application Pen Testing Framework

Module 15: SQL Injection

SQL Injection Concepts

- What is SQL Injection?
- SQL Injection and Server-side Technologies
- Understanding HTTP POST Request
- Understanding Normal SQL Query
- Understanding an SQL Injection Query
- Understanding an SQL Injection Query – Code Analysis
- Example of a Web Application Vulnerable to SQL Injection: BadProductList.aspx
- Example of a Web Application Vulnerable to SQL Injection: Attack Analysis
- Examples of SQL Injection

Types of SQL Injection

- Types of SQL injection
  - In-Band SQL Injection
    - Error Based SQL Injection
    - Union SQL Injection
  - Blind/Inferential SQL Injection
    - No Error Messages Returned
    - Blind SQL Injection: WAITFOR DELAY (YES or NO Response)
    - Blind SQL Injection: Boolean Exploitation and Heavy Query
  - Out-of-Band SQL injection

SQL Injection Methodology

- SQL Injection Methodology
  - Information Gathering and SQL Injection Vulnerability Detection
    - Information Gathering
    - Identifying Data Entry Paths
    - Extracting Information through Error Messages
    - Testing for SQL Injection
    - Additional Methods to Detect SQL Injection
    - SQL Injection Black Box Pen Testing
    - Source Code Review to Detect SQL Injection Vulnerabilities

- Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL

- Launch SQL Injection Attacks
  - Perform Union SQL Injection
  - Perform Error Based SQL Injection
  - Perform Error Based SQL Injection using Stored Procedure Injection
  - Bypass Website Logins Using SQL Injection
  - Perform Blind SQL Injection – Exploitation (MySQL)
  - Blind SQL Injection - Extract Database User
  - Blind SQL Injection - Extract Database Name
  - Blind SQL Injection - Extract Column Name
  - Blind SQL Injection - Extract Data from ROWS
  - Perform Double Blind SQL Injection – Classical Exploitation (MySQL)
  - Perform Blind SQL Injection Using Out of Band Exploitation Technique
  - Exploiting Second-Order SQL Injection
  - Bypass Firewall using SQL Injection
  - Perform SQL Injection to Insert a New User and Update Password
  - Exporting a Value with Regular Expression Attack
- Advanced SQL Injection
  - Database, Table, and Column Enumeration
  - Advanced Enumeration
  - Features of Different DBMSs
  - Creating Database Accounts
  - Password Grabbing
  - Grabbing SQL Server Hashes
  - Extracting SQL Hashes (In a Single Statement
  - Transfer Database to Attacker's Machine
  - Interacting with the Operating System
  - Interacting with the File System
  - Network Reconnaissance Using SQL Injection
  - Network Reconnaissance Full Query

        - Finding and Bypassing Admin Panel of a Website
        - PL/SQL Exploitation
        - Creating Server Backdoors using SQL Injection

SQL Injection Tools

- SQL Injection Tools
    - SQL Power Injector and sqlmap
    - The Mole and jSQL Injection
- SQL Injection Tools
- SQL Injection Tools for Mobile

Evasion Techniques

- Evading IDS
- Types of Signature Evasion Techniques
    - In-line Comment
    - Char Encoding
    - String Concatenation
    - Obfuscated Codes
    - Manipulating White Spaces
    - Hex Encoding
    - Sophisticated Matches
    - URL Encoding
    - Null Byte
    - Case Variation
    - Declare Variable
    - IP Fragmentation

Countermeasures

- How to Defend Against SQL Injection Attacks
    - Use Type-Safe SQL Parameters
- SQL Injection Detection Tools
    - IBM Security AppScan and Acunetix Web Vulnerability Scanner
    - Snort Rule to Detect SQL Injection Attacks
- SQL Injection Detection Tools

Module 16: Hacking Wireless Networks

Wireless Concepts

- Wireless Terminologies
- Wireless Networks
- Wireless Standards
- Service Set Identifier (SSID)
- Wi-Fi Authentication Modes
- Wi-Fi Authentication Process Using a Centralized Authentication Server
- Types of Wireless Antennas

Wireless Encryption

- Types of Wireless Encryption
  - WEP (Wired Equivalent Privacy) Encryption
  - WPA (Wi-Fi Protected Access) Encryption
  - WPA2 (Wi-Fi Protected Access 2) Encryption
- WEP vs. WPA vs. WPA2
- WEP Issues
- Weak Initialization Vectors (IV)

Wireless Threats

- Wireless Threats
  - Rogue Access Point Attack
  - Client Mis-association
  - Misconfigured Access Point Attack
  - Unauthorized Association
  - Ad Hoc Connection Attack
  - Honeypot Access Point Attack
  - AP MAC Spoofing
  - Denial-of-Service Attack
  - Key Reinstallation Attack (KRACK)
  - Jamming Signal Attack
    - Wi-Fi Jamming Devices

Wireless Hacking Methodology

- Wireless Hacking Methodology
  - Wi-Fi Discovery
    - Footprint the Wireless Network
    - Find Wi-Fi Networks in Range to Attack
    - Wi-Fi Discovery Tools
    - Mobile-based Wi-Fi Discovery Tools
  - GPS Mapping
    - GPS Mapping Tools
    - Wi-Fi Hotspot Finder Tools
    - How to Discover Wi-Fi Network Using Wardriving
  - Wireless Traffic Analysis
    - Choosing the Right Wi-Fi Card
    - Wi-Fi USB Dongle: AirPcap
    - Wi-Fi Packet Sniffer
    - Perform Spectrum Analysis
  - Launch Wireless Attacks
    - Aircrack-ng Suite
    - How to Reveal Hidden SSIDs
    - Fragmentation Attack
    - How to Launch MAC Spoofing Attack
    - Denial-of-Service: Disassociation and Deauthentication Attacks
    - Man-in-the-Middle Attack
    - MITM Attack Using Aircrack-ng
    - Wireless ARP Poisoning Attack
    - Rogue Access Points
    - Evil Twin
    - How to Set Up a Fake Hotspot (Evil Twin)
  - Crack Wi-Fi Encryption
    - How to Break WEP Encryption

  - How to Crack WEP Using Aircrack-ng
  - How to Break WPA/WPA2 Encryption
  - How to Crack WPA-PSK Using Aircrack-ng
  - WEP Cracking and WPA Brute Forcing Using Cain & Abel

Wireless Hacking Tools

- WEP/WPA Cracking Tools
- WEP/WPA Cracking Tool for Mobile
- Wi-Fi Sniffer
- Wi-Fi Traffic Analyzer Tools
- Other Wireless Hacking Tools

Bluetooth Hacking

- Bluetooth Stack
- Bluetooth Hacking
- Bluetooth Threats
- How to BlueJack a Victim
- Bluetooth Hacking Tools

Countermeasures

- Wireless Security Layers
- How to Defend Against WPA/WPA2 Cracking
- How to Defend Against KRACK Attacks
- How to Detect and Block Rogue AP
- How to Defend Against Wireless Attacks
- How to Defend Against Bluetooth Hacking

Wireless Security Tools

- Wireless Intrusion Prevention Systems
- Wireless IPS Deployment
- Wi-Fi Security Auditing Tools
- Wi-Fi Intrusion Prevention System
- Wi-Fi Predictive Planning Tools
- Wi-Fi Vulnerability Scanning Tools
- Bluetooth Security Tools

- Wi-Fi Security Tools for Mobile

Wireless Pen Testing

- Wireless Penetration Testing
- Wireless Penetration Testing Framework
  - Pen Testing for General Wi-Fi Network Attack
  - Pen Testing WEP Encrypted WLAN
  - Pen Testing WPA/WPA2 Encrypted WLAN
  - Pen Testing LEAP Encrypted WLAN
  - Pen Testing Unencrypted WLAN

Module 17: Hacking Mobile Platforms

Mobile Platform Attack Vectors

- Vulnerable Areas in Mobile Business Environment
- OWASP Top 10 Mobile Risks - 2016
- Anatomy of a Mobile Attack
- How a Hacker can Profit from Mobile when Successfully Compromised
- Mobile Attack Vectors and Mobile Platform Vulnerabilities
- Security Issues Arising from App Stores
- App Sandboxing Issues
- Mobile Spam
- SMS Phishing Attack (SMiShing) (Targeted Attack Scan)
  - SMS Phishing Attack Examples
- Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

Hacking Android OS

- Android OS
  - Android Device Administration API
- Android Rooting
  - Rooting Android Using KingoRoot
  - Android Rooting Tools
- Blocking Wi-Fi Access using NetCut
- Hacking with zANTI

- Hacking Networks Using Network Spoofer
- Launching DoS Attack using Low Orbit Ion Cannon (LOIC)
- Performing Session Hijacking Using DroidSheep
- Hacking with Orbot Proxy
- Android-based Sniffers
- Android Trojans
- Securing Android Devices
- Android Security Tool: Find My Device
- Android Security Tools
- Android Vulnerability Scanner
- Android Device Tracking Tools

Hacking iOS

- Apple iOS
- Jailbreaking iOS
  - Jailbreaking Techniques
  - Jailbreaking of iOS 11.2.1 Using Cydia
  - Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang
  - Jailbreaking Tools
- iOS Trojans
- Guidelines for Securing iOS Devices
- iOS Device Tracking Tools
- iOS Device Security Tools

Mobile Spyware

- Mobile Spyware
- Mobile Spyware: mSpy
- Mobile Spywares

Mobile Device Management

- Mobile Device Management (MDM)
- Mobile Device Management Solutions
- Bring Your Own Device (BYOD)
  - BYOD Risks

  - BYOD Policy Implementation
  - BYOD Security Guidelines

Mobile Security Guidelines and Tools

- General Guidelines for Mobile Platform Security
- Mobile Device Security Guidelines for Administrator
- SMS Phishing Countermeasures
- Mobile Protection Tools
- Mobile Anti-Spyware

Mobile Pen Testing

- Android Phone Pen Testing
- iPhone Pen Testing
- Mobile Pen Testing Toolkit: Hackode

Module 18: IoT Hacking

IoT Concepts

- What is IoT
- How IoT Works
- IoT Architecture
- IoT Application Areas and Devices
- IoT Technologies and Protocols
- IoT Communication Models
- Challenges of IoT
- Threat vs Opportunity

IoT Attacks

- IoT Security Problems
- OWASP Top 10 IoT Vulnerabilities and Obstacles
- IoT Attack Surface Areas
- IoT Threats
- Hacking IoT Devices: General Scenario
- IoT Attacks
  - DDoS Attack

  - Exploit HVAC
  - Rolling Code Attack
  - BlueBorne Attack
  - Jamming Attack
  - Hacking Smart Grid / Industrial Devices: Remote Access using Backdoor
  - Other IoT Attacks
- IoT Attacks in Different Sectors
- Case Study: Dyn Attack

IoT Hacking Methodology

- What is IoT Device Hacking?
- IoT Hacking Methodology
  - Information Gathering Using Shodan
  - Information Gathering using MultiPing
  - Vulnerability Scanning using Nmap
  - Vulnerability Scanning using RIoT Vulnerability Scanner
  - Sniffing using Foren6
  - Rolling code Attack using RFCrack
  - Hacking Zigbee Devices with Attify Zigbee Framework
  - BlueBorne Attack Using HackRF One
  - Gaining Remote Access using Telnet
  - Maintain Access by Exploiting Firmware

IoT Hacking Tools

- Information Gathering Tools
- Sniffing Tools
- Vulnerability Scanning Tools
- IoT Hacking Tools

Countermeasures

- How to Defend Against IoT Hacking
- General Guidelines for IoT Device Manufacturing Companies
- OWASP Top 10 IoT Vulnerabilities Solutions
- IoT Framework Security Considerations

- IoT Security Tools

IoT Pen Testing

- IoT Pen Testing

Module 19: Cloud Computing

Cloud Computing Concepts

- Introduction to Cloud Computing
- Separation of Responsibilities in Cloud
- Cloud Deployment Models
- NIST Cloud Deployment Reference Architecture
- Cloud Computing Benefits
- Understanding Virtualization

Cloud Computing Threats

- Cloud Computing Threats

Cloud Computing Attacks

- Service Hijacking using Social Engineering Attacks
- Service Hijacking using Network Sniffing
- Session Hijacking using XSS Attack
- Session Hijacking using Session Riding
- Domain Name System (DNS) Attacks
- Side Channel Attacks or Cross-guest VM Breaches
- SQL Injection Attacks
- Cryptanalysis Attacks
- Wrapping Attack
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Man-in-the-Cloud Attack

Cloud Security

- Cloud Security Control Layers
- Cloud Security is the Responsibility of both Cloud Provider and Consumer
- Cloud Computing Security Considerations
- Placement of Security Controls in the Cloud

- Best Practices for Securing Cloud
- NIST Recommendations for Cloud Security
- Organization/Provider Cloud Security Compliance Checklist

Cloud Security Tools

- Cloud Security Tools

Cloud Penetration Testing

- What is Cloud Pen Testing?
- Key Considerations for Pen Testing in the Cloud
- Cloud Penetration Testing
- Recommendations for Cloud Testing

Module 20: Cryptography

Cryptography Concepts

- Cryptography
    - Types of Cryptography
- Government Access to Keys (GAK)

Encryption Algorithms

- Ciphers
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- RC4, RC5, and RC6 Algorithms
- Twofish
- The DSA and Related Signature Schemes
- Rivest Shamir Adleman (RSA)
- Diffie-Hellman
- Message Digest (One-Way Hash) Functions
    - Message Digest Function: MD5
    - Secure Hashing Algorithm (SHA)
    - RIPEMD - 160
    - HMAC

Cryptography Tools

- MD5 Hash Calculators
- Hash Calculators for Mobile
- Cryptography Tools
  - Advanced Encryption Package 2017
  - BCTextEncoder
  - Cryptography Tools
- Cryptography Tools for Mobile

Public Key Infrastructure (PKI)

- Public Key Infrastructure (PKI)
  - Certification Authorities
  - Signed Certificate (CA) Vs. Self Signed Certificate

Email Encryption

- Digital Signature
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Cryptography Toolkit
  - OpenSSL
  - Keyczar
- Pretty Good Privacy (PGP)

Disk Encryption

- Disk Encryption
- Disk Encryption Tools
  - VeraCrypt
  - Symantec Drive Encryption
  - Disk Encryption Tools

Cryptanalysis

- Cryptanalysis Methods
  - Linear Cryptanalysis
  - Differential Cryptanalysis
  - Integral Cryptanalysis

- Code Breaking Methodologies
- Cryptography Attacks
  - Brute-Force Attack
  - Birthday Attack
    - Birthday Paradox: Probability
  - Meet-in-the-Middle Attack on Digital Signature Schemes
  - Side Channel Attack
  - Hash Collision Attack
  - DUHK Attack
  - Rainbow Table Attack
- Cryptanalysis Tools
- Online MD5 Decryption Tools

Countermeasures

- How to Defend Against Cryptographic Attacks