Ethical Hacking and Countermeasures

Course Outline

(Version 12)

Module 01: Introduction to Ethical Hacking

Information Security Overview

- Elements of Information Security
- Motives, Goals, and Objectives of Information Security Attacks
- Classification of Attacks
- Information Warfare

Hacking Methodologies and Frameworks

- CEH Hacking Methodology (CHM)
- Cyber Kill Chain Methodology
- Tactics, Techniques, and Procedures (TTPs)
- Adversary Behavioral Identification
- Indicators of Compromise (IoCs)
  - Categories of Indicators of Compromise
- MITRE ATT&CK Framework
- Diamond Model of Intrusion Analysis

Hacking Concepts

- What is Hacking?
- Who is a Hacker?
- Hacker Classes

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)
- Continual/Adaptive Security Strategy
- Defense-in-Depth
- What is Risk?
  - Risk Management
- Cyber Threat Intelligence
  - Threat Intelligence Lifecycle
- Threat Modeling
- Incident Management
  - Incident Handling and Response
- Role of AI and ML in Cyber Security
  - How Do AI and ML Prevent Cyber Attacks?

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)
- The Federal Information Security Management Act (FISMA)
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- Cyber Law in Different Countries

Module 02: Footprinting and Reconnaissance

Footprinting Concepts

- What is Footprinting?
- Information Obtained in Footprinting
- Footprinting Methodology

Footprinting through Search Engines

- Footprinting through Search Engines
- Footprint Using Advanced Google Hacking Techniques
- Google Hacking Database
- VPN Footprinting through Google Hacking Database
- Other Techniques for Footprinting through Search Engines
  - Google Advanced Search
  - Advanced Image Search
  - Reverse Image Search
  - Video Search Engines
  - Meta Search Engines
  - FTP Search Engines
  - IoT Search Engines

Footprinting through Web Services

- Finding a 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
- Harvesting Email Lists
- Footprinting through Job Sites
- Deep and Dark Web Footprinting
- Determining the Operating System
- VoIP and VPN Footprinting through SHODAN
- Competitive Intelligence Gathering
- Other Techniques for Footprinting through Web Services
  - Finding the Geographical Location of the Target

- Gathering Information from Financial Services
- Gathering Information from Business Profile Sites
- Monitoring Targets Using Alerts
- Tracking the Online Reputation of the Target
- Gathering Information from Groups, Forums, and Blogs
- Gathering Information from NNTP Usenet Newsgroups
- Gathering Information from Public Source-Code Repositories

Footprinting through Social Networking Sites

- Collecting Information through Social Engineering on Social Networking Sites
- General Resources for Locating Information from Social Media Sites
- Conducting Location Search on Social Media Sites
- Constructing and Analyzing Social Network Graphs
- Tools for Footprinting through Social Networking Sites

Website Footprinting

- Website Footprinting
- Website Footprinting using Web Spiders
- Mirroring Entire Website
- Extracting Website Information from https://archive.org
- Other Techniques for Website Footprinting
  - Extracting Website Links
  - Gathering the Wordlist from the Target Website
  - Extracting Metadata of Public Documents
  - Monitoring Web Pages for Updates and Changes
  - Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website
  - Searching for Web Pages Posting Patterns and Revision Numbers
  - Monitoring Website Traffic of the Target Company

Email Footprinting

- Tracking Email Communications
- Email Tracking Tools

Whois Footprinting

- Whois Lookup
- Finding IP Geolocation Information

DNS Footprinting

- Extracting DNS Information
- Reverse DNS Lookup

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, Dumpster Diving, and Impersonation

Footprinting Tools

- Footprinting Tools: Maltego and Recon-ng
- Footprinting Tools: FOCA and OSRFramework
- Footprinting Tools: OSINT Framework
- Footprinting Tools: Recon-Dog and BillCipher
- Footprinting Tools: Spyse

Footprinting Countermeasures

- Footprinting Countermeasures

Module 03: Scanning Networks

Network Scanning Concepts

- Overview of Network Scanning
- TCP Communication Flags
- TCP/IP Communication

Scanning Tools

- Scanning Tools: Nmap

- Scanning Tools: Hping3
  - Hping Commands
- Scanning Tools
- Scanning Tools for Mobile

Host Discovery

- Host Discovery Techniques
  - ARP Ping Scan
  - UDP Ping Scan
  - ICMP ECHO Ping Scan
  - ICMP ECHO Ping Sweep
  - ICMP Timestamp Ping Scan
  - ICMP Address Mask Ping Scan
  - TCP SYN Ping Scan
  - TCP ACK Ping Scan
  - IP Protocol Ping Scan
  - Ping Sweep Tools

Port and Service Discovery

- Port Scanning Techniques
  - TCP Scanning
    - TCP Connect/Full Open Scan
    - Stealth Scan (Half-open Scan)
    - Inverse TCP Flag Scan
      - ✓ Xmas Scan
      - ✓ FIN Scan
      - ✓ NULL Scan
      - ✓ TCP Maimon Scan
    - ACK Flag Probe Scan
      - ✓ TTL-Based Scan
      - ✓ Window-Based Scan
    - IDLE/IPID Header Scan
  - UDP Scan

- SCTP INIT Scan
- SCTP COOKIE ECHO Scan
- SSDP and List Scan
- IPv6 Scan

- Service Version Discovery
- Nmap Scan Time Reduction Techniques

OS Discovery (Banner Grabbing/OS Fingerprinting)

- OS Discovery/Banner Grabbing
- How to Identify Target System OS
  - OS Discovery using Wireshark
  - OS Discovery using Nmap and Unicornscan
  - OS Discovery using Nmap Script Engine
  - OS Discovery using IPv6 Fingerprinting

Scanning Beyond IDS and Firewall

- IDS/Firewall Evasion Techniques
  - Packet Fragmentation
  - Source Routing
  - Source Port Manipulation
  - IP Address Decoy
  - IP Address Spoofing
  - MAC Address Spoofing
  - Creating Custom Packets
  - Randomizing Host Order and Sending Bad Checksums
  - Proxy Servers
    - Proxy Chaining
    - Proxy Tools
    - Proxy Tools for Mobile
  - Anonymizers
    - Censorship Circumvention Tools: Alkasir and Tails

Network Scanning Countermeasures

- Ping Sweep Countermeasures

- Port Scanning Countermeasures
- Banner Grabbing Countermeasures
- IP Spoofing Detection Techniques
  - Direct TTL Probes
  - IP Identification Number
  - TCP Flow Control Method
- IP Spoofing Countermeasures
- Scanning Detection and Prevention Tools

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)
- Enumerating SNMP using SnmpWalk
- Enumerating SNMP using Nmap
- SNMP Enumeration Tools

LDAP Enumeration

- LDAP Enumeration
- Manual and Automated LDAP Enumeration
- LDAP Enumeration Tools

NTP and NFS Enumeration

- NTP Enumeration
- NTP Enumeration Commands
- NTP Enumeration Tools
- NFS Enumeration
- NFS Enumeration Tools

SMTP and DNS Enumeration

- SMTP Enumeration
- SMTP Enumeration using Nmap
- SMTP Enumeration using Metasploit
- SMTP Enumeration Tools
- DNS Enumeration Using Zone Transfer
- DNS Cache Snooping
- DNSSEC Zone Walking
- DNS and DNSSEC Enumeration using Nmap

Other Enumeration Techniques

- IPsec Enumeration
- VoIP Enumeration
- RPC Enumeration
- Unix/Linux User Enumeration
- Telnet and SMB Enumeration
- FTP and TFTP Enumeration
- IPv6 Enumeration
- BGP Enumeration

Enumeration Countermeasures

- Enumeration Countermeasures
- DNS Enumeration Countermeasures

Module 05: Vulnerability Analysis

Vulnerability Assessment Concepts

- What is Vulnerability?

- Examples of Vulnerabilities
- Vulnerability Research
- Resources for Vulnerability Research
- What is Vulnerability Assessment?
- Vulnerability Scoring Systems and Databases
- Vulnerability-Management Life Cycle
  - Pre-Assessment Phase
  - Vulnerability Assessment Phase
  - Post Assessment Phase

Vulnerability Classification and Assessment Types

- Vulnerability Classification
  - Misconfigurations/Weak Configurations
  - Application Flaws
  - Poor Patch Management
  - Design Flaws
  - Third-Party Risks
  - Default Installations/Default Configurations
  - Operating System Flaws
  - Default Passwords
  - Zero-Day Vulnerabilities
  - Legacy Platform Vulnerabilities
  - System Sprawl/Undocumented Assets
  - Improper Certificate and Key Management
- Types of Vulnerability Assessment

Vulnerability Assessment Tools

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

- Best Practices for Selecting Vulnerability Assessment Tools
- Vulnerability Assessment Tools: Qualys Vulnerability Management
- Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard
- Vulnerability Assessment Tools: OpenVAS and Nikto
- Other Vulnerability Assessment Tools
- Vulnerability Assessment Tools for Mobile

Vulnerability Assessment Reports

- Vulnerability Assessment Reports
- Components of a Vulnerability Assessment Report

Module 06: System Hacking

Gaining Access

- Cracking Passwords
  - Microsoft Authentication
  - How Hash Passwords Are Stored in Windows SAM?
  - NTLM Authentication Process
  - Kerberos Authentication
  - Password Cracking
  - Types of Password Attacks
    - Non-Electronic Attacks
    - Active Online Attacks
      - ✓ Dictionary, Brute-Force, and Rule-based Attack
      - ✓ Password Spraying Attack and Mask Attack
      - ✓ Password Guessing
      - ✓ Default Passwords
      - ✓ Trojans/Spyware/Keyloggers
      - ✓ Hash Injection/Pass-the-Hash (PtH) Attack
      - ✓ LLMNR/NBT-NS Poisoning
      - ✓ Internal Monologue Attack
      - ✓ Cracking Kerberos Password
      - ✓ Pass the Ticket Attack

- ✓ Other Active Online Attacks
- Passive Online Attacks
  - ✓ Wire Sniffing
  - ✓ Man-in-the-Middle/Manipulator-in-the-Middle and Replay Attacks
- Offline Attacks
  - ✓ Rainbow Table Attack
  - ✓ Distributed Network Attack

- Password Recovery Tools
- Tools to Extract the Password Hashes
- Password Cracking using Domain Password Audit Tool (DPAT)
- Password-Cracking Tools: L0phtCrack and ophcrack
- Password-Cracking Tools
- Password Salting
- How to Defend against Password Cracking
- How to Defend against LLMNR/NBT-NS Poisoning
- Tools to Detect LLMNR/NBT-NS Poisoning

- Vulnerability Exploitation
  - Exploit Sites
  - Buffer Overflow
    - Types of Buffer Overflow: Stack-Based Buffer Overflow
    - Types of Buffer Overflow: Heap-Based Buffer Overflow
    - Simple Buffer Overflow in C
    - Windows Buffer Overflow Exploitation
  - Return-Oriented Programming (ROP) Attack
  - Exploit Chaining
  - Active Directory Enumeration Using PowerView
  - Domain Mapping and Exploitation with Bloodhound
  - Identifying Insecurities Using GhostPack Seatbelt
  - Buffer Overflow Detection Tools
  - Defending against Buffer Overflows

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
- Privilege Escalation Using Named Pipe Impersonation
- Privilege Escalation by Exploiting Misconfigured Services
- Pivoting and Relaying to Hack External Machines
- Privilege Escalation Using Misconfigured NFS
- Privilege Escalation Using Windows Sticky Keys
- Privilege Escalation by Bypassing User Account Control (UAC)
- Privilege Escalation by Abusing Boot or Logon Initialization Scripts
- Privilege Escalation by Modifying Domain Policy
- Retrieving Password Hashes of Other Domain Controllers Using DCSync Attack
- Other Privilege Escalation Techniques
    - Access Token Manipulation
    - Parent PID Spoofing
    - Application Shimming
    - Filesystem Permission Weakness
    - Path Interception
    - Abusing Accessibility Features
    - SID-History Injection
    - COM Hijacking
    - Scheduled Tasks in Windows
    - Scheduled Tasks in Linux
    - Launch Daemon
    - Plist Modification
    - Setuid and Setgid
    - Web Shell
    - Abusing Sudo Rights

- Abusing SUID and SGID Permissions
- Kernel Exploits

- Privilege Escalation Tools
- How to Defend Against Privilege Escalation
  - Tools for Defending against DLL and Dylib Hijacking
  - Defending against Spectre and Meltdown Vulnerabilities
  - Tools for Detecting Spectre and Meltdown Vulnerabilities

Maintaining Access

- Executing Applications
  - Remote Code Execution Techniques
    - Tools for Executing Applications
  - Keylogger
    - Types of Keystroke Loggers
    - Remote Keylogger Attack Using Metasploit
    - Hardware Keyloggers
    - Keyloggers for Windows
    - Keyloggers for macOS
  - Spyware
    - Spyware Tools: Spytech SpyAgent and Power Spy
    - Spyware Tools
  - How to Defend Against Keyloggers
    - Anti-Keyloggers
  - How to Defend Against Spyware
    - Anti-Spyware
- Hiding Files
  - Rootkits
    - Types of Rootkits
    - How a Rootkit Works
    - Popular Rootkits
      - ✓ Purple Fox Rootkit
      - ✓ MoonBounce

- ✓ Dubbed Demodex Rootkit
- Detecting Rootkits
- Steps for Detecting Rootkits
- How to Defend against Rootkits
- Anti-Rootkits

o NTFS Data Stream

- How to Create NTFS Streams
- NTFS Stream Manipulation
- How to Defend against NTFS Streams
- NTFS Stream Detectors

o 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
  - ✓ Other Types of Steganography
- Steganography Tools for Mobile Phones
- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Detecting Steganography (Text, Image, Audio, and Video Files)
- Steganography Detection Tools

▪ Establishing Persistence

o Maintaining Persistence by Abusing Boot or Logon Autostart Executions

o Domain Dominance through Different Paths

- Remote Code Execution

- Abusing DPAPI
- Malicious Replication
- Skeleton Key Attack
- Golden Ticket Attack
- Silver Ticket Attack

- Maintain Domain Persistence Through AdminSDHolder
- Maintaining Persistence Through WMI Event Subscription
- Overpass-the-Hash Attack
- Linux Post Exploitation
- Windows Post Exploitation
- How to Defend against Persistence Attacks

Clearing Logs

- Covering Tracks
- Disabling Auditing: Auditpol
- Clearing Logs
- Manually Clearing Event Logs
- Ways to Clear Online Tracks
- Covering BASH Shell Tracks
- Covering Tracks on a Network
- Covering Tracks on an OS
- Delete Files using Cipher.exe
- Disable Windows Functionality
- Hiding Artifacts in Windows, Linux, and macOS
- Track-Covering Tools
- Defending against Covering Tracks

Module 07: Malware Threats

Malware Concepts

- Introduction to Malware
- Different Ways for Malware to Enter a System
- Common Techniques Attackers Use to Distribute Malware on the Web

- Components of Malware
- Potentially Unwanted Application or Applications (PUAs)
  - Adware

APT Concepts

- What are Advanced Persistent Threats?
- Characteristics of Advanced Persistent Threats
- Advanced Persistent Threat Lifecycle

Trojan Concepts

- What is a Trojan?
- How Hackers Use Trojans
- Common Ports used by Trojans
- Types of Trojans
  - Remote Access Trojans
  - Backdoor Trojans
  - Botnet Trojans
  - Rootkit Trojans
  - E-banking Trojans
    - Working of E-banking Trojans
    - E-banking Trojan: Dreambot
  - Point-of-Sale Trojans
  - Defacement Trojans
  - Service Protocol Trojans
  - Mobile Trojans
  - IoT Trojans
  - Security Software Disabler Trojans
  - Destructive Trojans
  - DDoS Trojans
  - Command Shell Trojans
- How to Infect Systems Using a Trojan
  - Creating a Trojan
  - Employing a Dropper or Downloader

- Employing a Wrapper
- Employing a Crypter
- Propagating and Deploying a Trojan
- Exploit Kits

Virus and Worm Concepts

- Introduction to Viruses
- Stages of Virus Lifecycle
- Working of Viruses
  - How does a Computer Get Infected by Viruses?
- Types of Viruses
  - System or Boot Sector Viruses
  - File Viruses
  - Multipartite Viruses
  - Macro Viruses
  - Cluster Viruses
  - Stealth Viruses/Tunneling Viruses
  - Encryption Viruses
  - Sparse Infector Viruses
  - Polymorphic Viruses
  - Metamorphic Viruses
  - Overwriting File or Cavity Viruses
  - Companion/Camouflage Viruses
  - Shell Viruses
  - File Extension Viruses
  - FAT Viruses
  - Logic Bomb Viruses
  - Web Scripting Virus
  - E-mail Viruses
  - Armored Viruses
  - Add-on Viruses
  - Intrusive Viruses

- Direct Action or Transient Viruses
- Terminate and Stay Resident (TSR) Viruses
- Ransomware
  - BlackCat
  - BlackMatter

- How to Infect Systems Using a Virus: Creating a Virus
- How to Infect Systems Using a Virus: Propagating and Deploying a Virus
- Computer Worms
  - Worm Makers

Fileless Malware Concepts

- What is Fileless Malware?
- Taxonomy of Fileless Malware Threats
- How does Fileless Malware Work?
- Launching Fileless Malware through Document Exploits and In-Memory Exploits
- Launching Fileless Malware through Script-based Injection
- Launching Fileless Malware by Exploiting System Admin Tools
- Launching Fileless Malware through Phishing
- Maintaining Persistence with Fileless Techniques
- Fileless Malware
  - LemonDuck
- Fileless Malware Obfuscation Techniques to Bypass Antivirus

Malware Analysis

- What is Sheep Dip Computer?
- Antivirus 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

- Identifying Packing/Obfuscation Method of ELF Malware
- Finding the Portable Executables (PE) Information
- Identifying File Dependencies
- Malware Disassembly
- Analyzing ELF Executable Files
- Analyzing Mach Object (Mach-O) Executable Files
- Analyzing Malicious MS Office Documents
  - Finding Suspicious Components
  - Finding Macro Streams
  - Dumping Macro Streams
  - Identifying Suspicious VBA Keywords

- Dynamic Malware Analysis
  - Port Monitoring
  - Process Monitoring
  - Registry Monitoring
  - Windows Services Monitoring
  - Startup Programs Monitoring
  - Event Logs Monitoring/Analysis
  - Installation Monitoring
  - Files and Folders Monitoring
  - Device Drivers Monitoring
  - Network Traffic Monitoring/Analysis
  - DNS Monitoring/Resolution
  - API Calls Monitoring
  - System Calls Monitoring
- Virus Detection Methods
- Trojan Analysis: ElectroRAT
  - ElectroRAT Malware Attack Phases
    - Initial propagation and Infection
    - Deploying Malware
    - Exploitation

- Maintaining Persistence

- Virus Analysis: REvil Ransomware
  - REvil Ransomware Attack Stages
    - Initial Access
    - Download and Execution
    - Exploitation
    - Lateral Movement / Defense Evasion and Discovery
    - Credential Access and Exfiltration / Command and Control
- Fileless Malware Analysis: SockDetour
  - SockDetour Fileless Malware Attack Stages
    - Pre-exploitation
    - Initial infection
    - Exploitation
    - Post-exploitation
      - ✓ Client Authentication and C2 Communication After Exploitation
      - ✓ Plugin Loading Feature

Malware Countermeasures

- Trojan Countermeasures
- Backdoor Countermeasures
- Virus and Worm Countermeasures
- Fileless Malware Countermeasures

Anti-Malware Software

- Anti-Trojan Software
- Antivirus Software
- Fileless Malware Detection Tools
- Fileless Malware Protection Tools

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 a 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 Attacks
    - MAC Limiting Configuration on Juniper Switches
    - Configuring DHCP Filtering on a Switch

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
- VLAN Hopping
- STP Attack
- How to Defend Against MAC Spoofing
- How to Defend Against VLAN Hopping
- How to Defend Against STP Attacks

Sniffing Technique: DNS Poisoning

- DNS Poisoning Techniques
  - Intranet DNS Spoofing
  - Internet DNS Spoofing
  - Proxy Server DNS Poisoning
  - DNS Cache Poisoning
    - SAD DNS Attack
- DNS Poisoning Tools
- 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
  - RITA (Real Intelligence Threat Analytics)
- Packet Sniffing Tools for Mobile Phones

Sniffing Countermeasures

- How to Defend Against Sniffing
- How to Detect Sniffing
- Sniffer Detection Techniques

- Ping Method
- DNS Method
- ARP Method

- Promiscuous Detection Tools

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
  - Diversion Theft
  - Honey Trap
  - Baiting
  - Quid Pro Quo
  - Elicitation
- Computer-based Social Engineering
  - Phishing
    - Examples of Phishing Emails
    - Types of Phishing
      - ✓ Spear Phishing
      - ✓ Whaling

- ✓ Pharming
- ✓ Spimming
- ✓ Angler Phishing
- ✓ Catfishing Attack
- ✓ Deepfake Attacks

- Phishing Tools

- Mobile-based Social Engineering
  - Publishing Malicious Apps
  - Repackaging Legitimate Apps
  - Fake Security Applications
  - SMiShing (SMS Phishing)

Insider Threats

- Insider Threats/Insider Attacks
- Types of Insider Threats
- Behavioral Indications of an Insider Threat

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

Social Engineering Countermeasures

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

- Audit Organization's Security for Phishing Attacks using OhPhish

Module 10: Denial-of-Service

DoS/DDoS Concepts

- What is a DoS Attack?
- What is a DDoS Attack?

Botnets

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

DoS/DDoS Attack Techniques

- Basic Categories of DoS/DDoS Attack Vectors
  - Volumetric Attacks
    - UDP Flood Attack
    - ICMP Flood Attack
    - Ping of Death and Smurf Attacks
    - Pulse Wave and Zero-Day DDoS Attacks
  - Protocol Attacks
    - SYN Flood Attack
    - Fragmentation Attack
    - Spoofed Session Flood Attack
  - Application Layer Attacks
    - HTTP GET/POST and Slowloris Attacks
    - UDP Application Layer Flood Attack
- Multi-Vector Attack
- Peer-to-Peer Attack
- Permanent Denial-of-Service Attack
- TCP SACK Panic

- Distributed Reflection Denial-of-Service (DRDoS) Attack
- DDoS Extortion/Ransom DDoS (RDDoS) Attack
- DoS/DDoS Attack Tools
- DoS and DDoS Attack Tools for Mobiles

DDoS Case Study

- DDoS Attack
- Hackers Advertise Links for Downloading Botnets
- Use of Mobile Devices as Botnets for Launching DDoS Attacks
- DDoS Case Study: DDoS Attack on Microsoft Azure

DoS/DDoS Attack 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
- Additional DoS/DDoS Countermeasures
- DoS/DDoS Protection at ISP Level
- Enabling TCP Intercept on Cisco IOS Software
- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools
- DoS/DDoS Protection Services

Module 11: Session Hijacking

Session Hijacking Concepts

- What is Session Hijacking?
- Why is Session Hijacking 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/Manipulator-in-the-Middle Attack
- Compromising Session IDs Using Man-in-the-Browser/Manipulator-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 Attacks
- Compromising Session IDs Using Session Fixation
- Session Hijacking Using Proxy Servers
- Session Hijacking Using CRIME Attack
- Session Hijacking Using Forbidden Attack
- Session Hijacking Using Session Donation Attack
- PetitPotam Hijacking

Network-Level Session Hijacking

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

Session Hijacking Tools

- Session Hijacking Tools
- Session Hijacking Tools for Mobile Phones

Session Hijacking Countermeasures

- Session Hijacking Detection Methods
- Protecting against Session Hijacking
- Web Development Guidelines to Prevent Session Hijacking
- Web User Guidelines to Prevent Session Hijacking
- Session Hijacking Detection Tools
- Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions
- Approaches to Prevent Session Hijacking
  - HTTP Referrer Header
- Approaches to Prevent MITM Attacks
  - DNS over HTTPS
  - Password Manager
  - Zero-trust Principles
- IPsec
  - IPsec Authentication and Confidentiality
- Session Hijacking Prevention Tools

Module 12: Evading IDS, Firewalls, and Honeypots

IDS, IPS, Firewall, and Honeypot Concepts

- Intrusion Detection System (IDS)
  - How an IDS Detects an Intrusion?
  - General Indications of Intrusions
  - Types of Intrusion Detection Systems
  - Types of IDS Alerts
- Intrusion Prevention System (IPS)
- 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, IPS, Firewall, and Honeypot Solutions

- Intrusion Detection using YARA Rules
- Intrusion Detection Tools
  - 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
  - Intrusion Detection Tools for Mobile Devices
- Intrusion Prevention Tools
- Firewalls
  - Firewalls for Mobile Devices
- Honeypot Tools

Evading IDS

- IDS Evasion Techniques
  - Insertion Attack
  - Evasion
  - Denial-of-Service Attack (DoS)

- Obfuscating
- False Positive Generation
- Session Splicing
- Unicode Evasion Technique
- 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 an IP Address in Place of a URL
  - Bypass Blocked Sites Using Anonymous Website Surfing Sites
  - Bypass a Firewall Using a Proxy Server
  - Bypassing Firewalls through the ICMP Tunneling Method
  - Bypassing Firewalls through the ACK Tunneling Method
  - Bypassing Firewalls through the HTTP Tunneling Method
    - Why do I Need HTTP Tunneling?
    - HTTP Tunneling Tools
  - Bypassing Firewalls through the SSH Tunneling Method
    - SSH Tunneling Tools: Bitvise and Secure Pipes
  - Bypassing Firewalls through the DNS Tunneling Method

- Bypassing Firewalls through External Systems
- Bypassing Firewalls through MITM Attacks
- Bypassing Firewalls through Content
- Bypassing the WAF using an XSS Attack
- Other Techniques for Bypassing WAF
  - Using HTTP Header Spoofing
  - Using Blacklist Detection
  - Using Fuzzing/Bruteforcing
  - Abusing SSL/TLS ciphers
- Bypassing Firewalls through HTML Smuggling
- Bypassing Firewalls through Windows BITS

Evading NAC and Endpoint Security

- Bypassing NAC using VLAN Hopping
- Bypassing NAC using Pre-authenticated Device
- Bypassing Endpoint Security using Ghostwriting
- Bypassing Endpoint Security using Application Whitelisting
- Bypassing Endpoint Security using XLM Weaponization
- Bypassing Endpoint Security by Dechaining Macros
- Bypassing Endpoint Security by Clearing Memory Hooks
- Bypassing Antivirus using Metasploit Templates
- Bypassing Symantec Endpoint Protection
- Other Techniques for Bypassing Endpoint Security
  - Hosting Phishing Sites
  - Passing Encoded Commands
  - Fast Flux DNS Method
  - Timing-based Evasion
  - Signed Binary Proxy Execution

IDS/Firewall Evading Tools

- IDS/Firewall Evading Tools
- Packet Fragment Generator Tools

Detecting Honeypots

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

IDS/Firewall Evasion Countermeasures

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

Module 13: Hacking Web Servers

Web Server Concepts

- Web Server Operations
- Web Server Security Issues
- Why are Web Servers Compromised?

Web Server Attacks

- DNS Server Hijacking
- DNS Amplification Attack
- Directory Traversal Attacks
- Website Defacement
- Web Server Misconfiguration
- HTTP Response-Splitting Attack
- Web Cache Poisoning Attack
- SSH Brute Force Attack
- Web Server Password Cracking
- Other Web Server Attacks
  - DoS/DDoS Attacks
  - Man-in-the-Middle Attack
  - Phishing Attacks
  - 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 Password Hacking
- Using Application Server as a Proxy
- Web Server Attack Tools
  - Metasploit
    - Metasploit Exploit Module
    - Metasploit Payload and Auxiliary Modules
    - Metasploit NOPS Module
  - Web Server Attack Tools

Web Server Attack Countermeasures

- Place Web Servers in Separate Secure Server Security Segment on Network
- Countermeasures: Patches and Updates
- Countermeasures: Protocols and Accounts
- Countermeasures: 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
- Web Server Security Tools
  - Web Application Security Scanners
  - Web Server Security Scanners
  - Web Server Malware Infection Monitoring Tools

- Web Server Security Tools
- Web Server Pen Testing Tools

Patch Management

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

Module 14: Hacking Web Applications

Web Application Concepts

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

Web Application Threats

- OWASP Top 10 Application Security Risks - 2021
  - A01 - Broken Access Control
  - A02 - Cryptographic Failures/Sensitive Data Exposure
  - A03 - Injection Flaws
    - SQL Injection Attacks
    - Command Injection Attacks
      - ✓ Command Injection Example
    - File Injection Attack
    - LDAP Injection Attacks
    - Other Injection Attacks
      - ✓ JNDI Injection
    - Cross-Site Scripting (XSS) Attacks
      - ✓ Cross-Site Scripting Attack Scenario: Attack via Email
      - ✓ XSS Attack in Blog Posting
      - ✓ XSS Attack in Comment Field
  - A04 - Insecure Design

- A05 - Security Misconfiguration
  - XML External Entity (XXE)
- A06 - Vulnerable and Outdated Components/Using Components with Known Vulnerabilities
- A07 - Identification and Authentication Failures/Broken Authentication
- A08 - Software and Data Integrity Failures
  - Insecure Deserialization
- A09 - Security Logging and Monitoring Failures/Insufficient Logging and Monitoring
- A10 - Server-Side Request Forgery (SSRF)
  - Types of Server-Side Request Forgery (SSRF) Attack
    - ✓ Injecting SSRF payload
    - ✓ Cross-Site Port Attack (XSPA)

- Other Web Application Threats
  - Directory Traversal
  - Unvalidated Redirects and Forwards
    - Open Redirection
    - Header-Based Open Redirection
    - JavaScript-Based Open Redirection
  - Watering Hole Attack
  - Cross-Site Request Forgery (CSRF) Attack
  - Cookie/Session Poisoning
  - Web Service Attack
  - Web Service Footprinting Attack
  - Web Service XML Poisoning
  - Hidden Field Manipulation Attack
  - Web-based Timing Attacks
  - MarioNet Attack
  - Clickjacking Attack
  - DNS Rebinding Attack
  - Same-Site Attack
  - Pass-the-cookie Attack

Web Application Hacking Methodology

- Web Application 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
  - Detect Load Balancers
- Analyze Web Applications
  - Identify Entry Points for User Input
  - Identify Server-Side Technologies
  - Identify Server-Side Functionality
  - Identify Files and Directories
  - Identify Web Application Vulnerabilities
  - Map the Attack Surface
- Bypass Client-side Controls
  - Attack Hidden Form Fields
  - Attack Browser Extensions
    - Attack Google Chrome Browser Extensions
  - Perform Source Code Review
  - Evade XSS Filters
- Attack Authentication Mechanism
  - Design and Implementation Flaws in Authentication Mechanism
  - Username Enumeration
  - Password Attacks: Password Functionality Exploits
  - Password Attacks: Password Guessing and Brute-forcing
  - Password Attacks: Attack Password Reset Mechanism
  - Session Attacks: Session ID Prediction/Brute-forcing
  - Cookie Exploitation: Cookie Poisoning
  - Bypass Authentication: Bypass SAML-based SSO

- Attack Authorization Schemes
  - Authorization Attack: HTTP Request Tampering
  - Authorization Attack: 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
  - Perform Local File Inclusion (LFI)
- Attack Application Logic Flaws
- Attack Shared Environments
- Attack Database Connectivity
  - Connection String Injection
  - Connection String Parameter Pollution (CSPP) Attacks
  - Connection Pool DoS
- Attack Web Application Client
- Attack Web Services
  - Web Services Probing Attacks
  - Web Service Attacks: SOAP Injection
  - Web Service Attacks: SOAPAction Spoofing
  - Web Service Attacks: WS-Address Spoofing
  - Web Service Attacks: XML Injection
  - Web Services Parsing Attacks
  - Web Service Attack Tools
- Additional Web Application Hacking Tools

Web API, Webhooks, and Web Shell

- What is Web API?
  - Web Services APIs
- What are Webhooks?
- OWASP Top 10 API Security Risks
- API Vulnerabilities

- Web API Hacking Methodology
  - Identify the Target
  - Detect Security Standards
  - Identify the Attack Surface
    - Analyze Web API Requests and Responses
  - Launch Attacks
    - Fuzzing and Invalid Input Attacks
    - Malicious Input Attacks
    - Injection Attacks
    - Exploiting Insecure Configurations
    - Login/ Credential Stuffing Attacks
    - API DDoS Attacks
    - Authorization Attacks on API: OAuth Attacks
      - ✓ SSRF using Dynamic Client Registration endpoint
      - ✓ WebFinger User Enumeration
      - ✓ Exploit Flawed Scope Validation
    - Other Techniques to Hack an API
  - REST API Vulnerability Scanning
  - Bypassing IDOR via Parameter Pollution
- Web Shells
  - Web Shell Tools
- How to Prevent Installation of a Web Shell
- Web Shell Detection Tools
- Secure API Architecture
  - Implementing Layered Security in an API
- API Security Risks and Solutions
- Best Practices for API Security
- Best Practices for Securing Webhooks

Web Application Security

- Web Application Security Testing
- Web Application Fuzz Testing

- Source Code Review
- Encoding Schemes
- Whitelisting vs. Blacklisting Applications
  - Application Whitelisting and Blacklisting Tools
- How to Defend Against Injection Attacks
- Web Application Attack Countermeasures
- How to Defend Against Web Application Attacks
- RASP for Protecting Web Servers
- Bug Bounty Programs
- Web Application Security Testing Tools
- Web Application Firewalls

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
    - Blind SQL Injection: No Error Message 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

- Information Gathering and SQL Injection Vulnerability Detection
  - Information Gathering
  - Identifying Data Entry Paths
  - Extracting Information through Error Messages
  - SQL Injection Vulnerability Detection: 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
- 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
- HTTP Header-Based SQL Injection
- DNS Exfiltration using SQL Injection
- MongoDB Injection/NoSQL Injection Attack
- Case Study: SQL Injection Attack and Defense

SQL Injection Tools

- SQL Injection Tools
- SQL Injection Tools for Mobile Devices

Evasion Techniques

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

SQL Injection Countermeasures

- How to Defend Against SQL Injection Attacks

- Use Type-Safe SQL Parameters
- Defenses in the Application
  - LIKE Clauses
  - Wrapping Parameters with QUOTENAME() and REPLACE()

- Detecting SQL Injection Attacks
- SQL Injection Detection Tools
  - OWASP ZAP and Damn Small SQLi Scanner (DSSS)
  - Snort
  - SQL Injection Detection Tools

Module 16: Hacking Wireless Networks

Wireless Concepts

- Wireless Terminology
- 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
  - Wired Equivalent Privacy (WEP) Encryption
  - Wi-Fi Protected Access (WPA) Encryption
  - WPA2 Encryption
  - WPA3 Encryption
- Comparison of WEP, WPA, WPA2, and WPA3
- Issues in WEP, WPA, and WPA2

Wireless Threats

- Wireless Threats
  - Rogue AP Attack
  - Client Mis-association

- Misconfigured AP Attack
- Unauthorized Association
- Ad-Hoc Connection Attack
- Honeypot AP Attack
- AP MAC Spoofing
- Denial-of-Service Attack
- Key Reinstallation Attack (KRACK)
- Jamming Signal Attack
  - Wi-Fi Jamming Devices
- aLTEr Attack
- Wormhole and Sinkhole Attacks
- Inter-Chip Privilege Escalation/Wireless Co-Existence Attack
- GNSS Spoofing

Wireless Hacking Methodology

- Wireless Hacking Methodology
- Wi-Fi Discovery
  - Wireless Network Footprinting
  - Finding Wi-Fi Networks in Range to Attack
  - Finding WPS-Enabled APs
  - Wi-Fi Discovery Tools
  - Mobile-based Wi-Fi Discovery Tools
- GPS Mapping
  - GPS Mapping Tools
  - Wi-Fi Hotspot Finder Tools
  - Wi-Fi Network Discovery Through WarDriving
- Wireless Traffic Analysis
  - Choosing the Optimal Wi-Fi Card
  - Sniffing Wireless Traffic
  - Perform Spectrum Analysis
- Launch of Wireless Attacks
  - Aircrack-ng Suite

- Detection of Hidden SSIDs
- Fragmentation Attack
- MAC Spoofing Attack
- Denial-of-Service: Disassociation and De-authentication Attacks
- Man-in-the-Middle Attack
- MITM Attack Using Aircrack-ng
- Wireless ARP Poisoning Attack
  - ARP Poisoning Attack Using Ettercap
- Rogue APs
  - Creation of a Rogue AP Using MANA Toolkit
- Evil Twin
  - Set Up of a Fake Hotspot (Evil Twin)
- aLTEr Attack
- Wi-Jacking Attack
- RFID Cloning Attack

- Wi-Fi Encryption Cracking
  - WEP Encryption Cracking
  - Cracking WEP Using Aircrack-ng
  - WPA/WPA2 Encryption Cracking
  - Cracking WPA-PSK Using Aircrack-ng
  - Cracking WPA/WPA2 Using Wifiphisher
  - Cracking WPS Using Reaver
  - WPA3 Encryption Cracking
  - WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker

Wireless Hacking Tools

- WEP/WPA/WPA2 Cracking Tools
- WEP/WPA/WPA2 Cracking Tools for Mobile
- Wi-Fi Packet Sniffers
- Wi-Fi Traffic Analyzer Tools
- Other Wireless Hacking Tools

Bluetooth Hacking

- Bluetooth Stack
- Bluetooth Hacking
- Bluetooth Threats
- Bluejacking
- Bluetooth Reconnaissance Using Bluez
- Btlejacking Using BtleJack
- Cracking BLE Encryption Using crackle
- Bluetooth Hacking Tools

Wireless Attack Countermeasures

- Wireless Security Layers
- Defense Against WPA/WPA2/WPA3 Cracking
- Defense Against KRACK and aLTEr Attacks
- Detection and Blocking of Rogue APs
- Defense Against Wireless Attacks
- Defense Against Bluetooth Hacking

Wireless Security Tools

- Wireless Intrusion Prevention Systems
- WIPS Deployment
- Wi-Fi Security Auditing Tools
- Wi-Fi IPSs
- Wi-Fi Predictive Planning Tools
- Wi-Fi Vulnerability Scanning Tools
- Bluetooth Security Tools
- Wi-Fi Security Tools for Mobile

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 Devices that are 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
- Agent Smith Attack
- Exploiting SS7 Vulnerability
- Simjacker: SIM Card Attack
- OTP Hijacking/Two-Factor Authentication Hijacking
- Camera/Microphone Capture Attacks
  - Camfecting Attack
  - Android Camera Hijack Attack

Hacking Android OS

- Android OS
  - Android Device Administration API
- Android Rooting
  - Rooting Android Using KingoRoot
  - Android Rooting Tools
- Hacking Android Devices
  - Blocking Wi-Fi Access Using NetCut
  - Identifying Attack Surfaces Using drozer
  - Hacking with zANTI and Network Spoofer
  - Launch DoS Attack using Low Orbit Ion Cannon (LOIC)
  - Session Hijacking Using DroidSheep
  - Hacking with Orbot Proxy
  - Exploiting Android Device through ADB Using PhoneSploit
  - Android-based Sniffers
  - Launching Man-in-the-Disk Attack

- Launching Sphearphone Attack
- Exploiting Android Devices Using Metasploit
- Other Techniques for Hacking Android Devices
- Android Trojans

- OTP Hijacking Tools
- Camera/Microphone Hijacking Tools
- Android Hacking Tools
- Securing Android Devices
- Android Security Tools
  - Android Device Tracking Tools: Google Find My Device
  - Android Device Tracking Tools
  - Android Vulnerability Scanners
  - Online Android Analyzers

Hacking iOS

- Apple iOS
- Jailbreaking iOS
  - Jailbreaking Techniques
  - Jailbreaking iOS Using Hexxa Plus
  - Jailbreaking Tools
- Hacking iOS Devices
  - Hacking using Spyzie
  - Hacking Network using Network Analyzer Pro
  - iOS Trustjacking
  - Analyzing and Manipulating iOS Applications
    - Manipulating an iOS Application Using cycript
    - iOS Method Swizzling
    - Extracting Secrets Using Keychain Dumper
    - Analyzing an iOS Application Using objection
  - iOS Malware
  - iOS Hacking Tools
- Securing iOS Devices

- iOS Device Security Tools
- iOS Device Tracking Tools

Mobile Device Management

- Mobile Device Management (MDM)
- Mobile Device Management Solutions: IBM MaaS360
  - Mobile Device Management Solutions
- Bring Your Own Device (BYOD)
  - BYOD Risks
  - BYOD Policy Implementation
  - BYOD Security Guidelines

Mobile Security Guidelines and Tools

- OWASP Top 10 Mobile Controls
- General Guidelines for Mobile Platform Security
- Mobile Device Security Guidelines for Administrator
- SMS Phishing Countermeasures
- Critical Data Storage in Android and iOS: KeyStore and Keychain Recommendations
- Mobile Security Tools
  - Source Code Analysis Tools
  - Reverse Engineering Tools
  - App Repackaging Detector
  - Mobile Protection Tools
  - Mobile Anti-Spyware
  - Mobile Pen Testing Toolkit: ImmuniWeb® MobileSuite

Module 18: IoT and OT Hacking

IoT Hacking

IoT Concepts

- What is the IoT?
- How the 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 Threats
- OWASP IoT Attack Surface Areas
- IoT Vulnerabilities
- 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
  - SDR-Based Attacks on IoT
  - Identifying and Accessing Local IoT Devices
  - Fault Injection Attacks
  - Other IoT Attacks
- IoT Attacks in Different Sectors
- Case Study: Enemybot

IoT Hacking Methodology

- What is IoT Device Hacking?
- IoT Hacking Methodology
  - Information Gathering Using Shodan
  - Information Gathering using MultiPing
  - Information Gathering using FCC ID Search
  - Discovering IoT Devices with Default Credentials using IoTSeeker

- Vulnerability Scanning using Nmap
- Vulnerability Scanning using RIoT Vulnerability Scanner
- Sniffing using Foren6
- Sniffing using Wireshark
- Analyzing Spectrum and IoT Traffic
- Rolling code Attack using RFCrack
- Hacking Zigbee Devices with Attify Zigbee Framework
- BlueBorne Attack Using HackRF One
- Replay Attack using HackRF One
- SDR-Based Attacks using RTL-SDR and GNU Radio
- Side Channel Attack using ChipWhisperer
- Identifying IoT Communication Buses and Interfaces
- NAND Glitching
- Gaining Remote Access using Telnet
- Maintain Access by Exploiting Firmware
  - Firmware Analysis and Reverse Engineering
    - ✓ Emulate Firmware for Dynamic Testing

- IoT Hacking Tools
  - Information-Gathering Tools
  - Sniffing Tools
  - Vulnerability-Scanning Tools
  - Tools to Perform SDR-Based Attacks
  - IoT Hacking Tools

IoT Attack 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 Hardware Security Best Practices
- IoT Device Management
- IoT Security Tools

OT Hacking

OT Concepts

- What is OT?
- Essential Terminology
- IT/OT Convergence (IIOT)
- The Purdue Model
- Challenges of OT
- Introduction to ICS
- Components of an ICS
  - Distributed Control System (DCS)
  - Supervisory Control and Data Acquisition (SCADA)
  - Programmable Logic Controller (PLC)
  - Basic Process Control System (BPCS)
  - Safety Instrumented Systems (SIS)
- OT Technologies and Protocols

OT Attacks

- OT Vulnerabilities
- MITRE ATT&CK for ICS
- OT Threats
- OT Attacks
  - HMI-based Attacks
  - Side-Channel Attacks
  - Hacking Programmable Logic Controller (PLC)
  - Hacking Industrial Systems through RF Remote Controllers
  - OT Malware
- OT Malware Analysis: INDUSTROYER.V2

OT Hacking Methodology

- What is OT Hacking?
- OT Hacking Methodology
  - Identifying ICS/SCADA Systems using Shodan
  - Gathering Default Passwords using CRITIFENCE

- Scanning ICS/SCADA Systems using Nmap
- Vulnerability Scanning using Nessus
- Vulnerability Scanning using Skybox Vulnerability Control
- Fuzzing ICS Protocols
- Sniffing using NetworkMiner
- Analyzing Modbus/TCP Traffic Using Wireshark
- Discovering ICS/SCADA Network Topology using GRASSMARLIN
- Hacking ICS Hardware
- Hacking Modbus Slaves using Metasploit
- Hacking PLC using modbus-cli
- Gaining Remote Access using DNP3

- OT Hacking Tools
  - Information-Gathering Tools
  - Sniffing and Vulnerability-Scanning Tools
  - OT Hacking Tools

OT Attack Countermeasures

- How to Defend Against OT Hacking
- OT Vulnerabilities and Solutions
- How to Secure an IT/OT Environment
- Implementing a Zero-Trust Model for ICS/SCADA
- International OT Security Organizations and Frameworks
  - OTCSA
  - OT-ISAC
  - NERC
  - Industrial Internet Security Framework (IISF)
  - ISA/IEC-62443
- OT Security Solutions
- OT Security Tools

Module 19: Cloud Computing

Cloud Computing Concepts

- Introduction to Cloud Computing
- Types of Cloud Computing Services
  - Infrastructure-as-a-Service (IaaS)
  - Platform-as-a-Service (PaaS)
  - Software-as-a-Service (SaaS)
  - Identity-as-a-Service (IDaaS)
  - Security-as-a-Service (SECaaS)
  - Container-as-a-Service (CaaS)
  - Function-as-a-Service (FaaS)
  - Anything-as-a-Service (XaaS)
  - Firewalls-as-a-Service (FWaaS)
  - Desktop-as-a-Service (DaaS)
  - Mobile Backend-as-a-Service (MBaaS)
  - Machines-as-a-Service (MaaS) Business Model
- Separation of Responsibilities in Cloud
- Cloud Deployment Models
  - Public Cloud
  - Private Cloud
  - Community Cloud
  - Hybrid Cloud
  - Multi Cloud
  - Distributed Cloud
  - Poly Cloud
- NIST Cloud Deployment Reference Architecture
- Cloud Storage Architecture
- Role of AI in Cloud Computing
- Virtual Reality and Augmented Reality on Cloud
- Fog Computing
- Edge Computing

- Cloud vs. Fog Computing vs. Edge Computing
- Cloud Computing vs. Grid Computing
- Cloud Service Providers

Container Technology

- What is a Container?
- Containers Vs. Virtual Machines
- What is Docker?
  - Microservices Vs. Docker
  - Docker Networking
- Container Orchestration
- What is Kubernetes?
  - Kubernetes Vs. Docker
- Clusters and Containers
- Container Security Challenges
- Container Management Platforms
- Kubernetes Platforms

Serverless Computing

- What is Serverless Computing?
- Serverless Vs. Containers
- Serverless Computing Frameworks

Cloud Computing Threats

- OWASP Top 10 Cloud Security Risks
- OWASP Top 10 Serverless Security Risks
- Cloud Computing Threats
- Container Vulnerabilities
- Kubernetes Vulnerabilities
- Cloud Attacks
  - Service Hijacking using Social Engineering
  - Service Hijacking using Network Sniffing
  - Side-Channel Attacks or Cross-guest VM Breaches
  - Wrapping Attack

- Man-in-the-Cloud (MITC) Attack
- Cloud Hopper Attack
- Cloud Cryptojacking
- Cloudborne Attack
- Instance Metadata Service (IMDS) Attack
- Cache Poisoned Denial of Service (CPDoS)/Content Delivery Network (CDN) Cache Poisoning Attack
- Cloud Snooper Attack
- Golden SAML Attack
- Other Cloud Attacks

- Cloud Malware

Cloud Hacking

- What is Cloud Hacking?
- Hacking Cloud
  - Container Vulnerability Scanning using Trivy
  - Kubernetes Vulnerability Scanning using Sysdig
  - Enumerating S3 Buckets
  - Identifying Open S3 Buckets using S3Scanner
  - Enumerating AWS Account IDs
  - Enumerating IAM Roles
  - Enumerating Bucket Permissions using S3Inspector
  - Enumerating Kubernetes etcd
  - Enumerating Azure Active Directory (AD) Accounts
  - Gathering Cloud Keys Through IMDS Attack
  - Exploiting Amazon Cloud Infrastructure using Nimbostratus
  - Exploiting Misconfigured AWS S3 Buckets
  - Compromising AWS IAM Credentials
  - Hijacking Misconfigured IAM Roles using Pacu
  - Cracking AWS Access Keys using DumpsterDiver
  - Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)
  - Serverless-Based Attacks on AWS Lambda
  - Exploiting Shadow Admins in AWS

- Exploiting Docker Remote API
- Hacking Container Volumes
- CloudGoat 2 – Vulnerable by Design AWS Deployment Tool
- Gaining Access by Exploiting SSRF Vulnerability
- AWS IAM Privilege Escalation Techniques
- Escalating Privileges of Google Storage Buckets using GCPBucketBrute
- Privilege Escalation Using Misconfigured User Accounts in Azure AD
- Creating Backdoor Accounts in AWS
- Backdooring Docker Images using dockerscan
- Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating CloudTrial Service

- AWS Hacking Tool: AWS pwn

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
- Security Assertion Markup Language (SAML)
- Cloud Network Security
  - Virtual Private Cloud (VPC)
  - Public and Private Subnets
  - Transit Gateways
  - VPC Endpoint
- Cloud Security Controls
  - Cloud Application Security
  - High Availability Across Zones
  - Cloud Integration and Auditing
  - Security Groups
  - Instance Awareness
- Kubernetes Vulnerabilities and Solutions

- Serverless Security Risks and Solutions
- Best Practices for Container Security
- Best Practices for Docker Security
- Best Practices for Kubernetes Security
- Best Practices for Serverless Security
- Zero Trust Networks
- Organization/Provider Cloud Security Compliance Checklist
- International Cloud Security Organizations
- Shadow Cloud Asset Discovery Tools
- Cloud Security Tools
- Container Security Tools
- Kubernetes Security Tools
- Serverless Application Security Solutions
- Cloud Access Security Broker (CASB)
  - CASB Solutions
    - Forcepoint CASB
- Next-Generation Secure Web Gateway (NG SWG)
  - NG SWG Solutions

Module 20: Cryptography

Cryptography Concepts

- Cryptography
- Government Access to Keys (GAK)

Encryption Algorithms

- Ciphers
- Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
- RC4, RC5, and RC6 Algorithms
- Twofish and Threefish
- Serpent and TEA
- CAST-128
- GOST Block Cipher and Camellia

- DSA and Related Signature Schemes
- Rivest Shamir Adleman (RSA)
- Diffie-Hellman
- YAK
- Message Digest (One-Way Hash) Functions
  - Message Digest Function: MD5 and MD6
  - Message Digest Function: Secure Hashing Algorithm (SHA)
  - RIPEMD – 160 and HMAC
- Other Encryption Techniques
  - Post-quantum Cryptography
  - Lightweight Cryptography
- Comparison of Cryptographic Algorithms
- Cipher Modes of Operation
  - Electronic Code Book (ECB) Mode
  - Cipher Block Chaining (CBC) Mode
  - Cipher Feedback (CFB) Mode
  - Counter Mode
- Modes of Authenticated Encryption
  - Authenticated Encryption with Message Authentication Code (MAC)
  - Authenticated Encryption with Associated Data (AEAD)
- Applications of Cryptography - Blockchain
  - Types of Blockchain

Cryptography Tools

- MD5 and MD6 Hash Calculators
- Hash Calculators for Mobile
- 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 Toolkits
- Pretty Good Privacy (PGP)
- GNU Privacy Guard (CPG)
- Web of Trust (WOT)
- Encrypting Email Messages in Outlook
  - S/MIME Encryption
  - Microsoft 365 Message Encryption
- Signing/Encrypting Email Messages on Mac
- Encrypting/Decrypting Email Messages Using OpenPGP
- Email Encryption Tools

Disk Encryption

- Disk Encryption
- Disk Encryption Tools: VeraCrypt and Symantec Drive Encryption
- Disk Encryption Tools
- Disk Encryption Tools for Linux
- Disk Encryption Tools for macOS

Cryptanalysis

- Cryptanalysis Methods
  - Quantum 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
- Related-Key Attack
- Padding Oracle Attack
- DROWN Attack

- Cryptanalysis Tools
- Online MD5 Decryption Tools

Cryptography Attack Countermeasures

- How to Defend Against Cryptographic Attacks
- Key Stretching

Appendix A: Ethical Hacking Essential Concepts - I

Operating System Concepts

- Windows Operating System
  - Windows Architecture
  - Windows Commands
- Unix Operating System
  - UNIX Directory Structure
  - UNIX Commands
- Linux Operating System
  - Linux Features
- macOS Operating System
  - macOS Layered Architecture

File Systems

- Understanding File Systems
  - Types of File Systems
  - Windows File Systems
    - File Allocation Table (FAT)
    - FAT32
    - New Technology File System (NTFS)
    - NTFS Architecture

- NTFS System Files
- Encrypting File Systems (EFS)
- Components of EFS
- Sparse Files

o Linux File Systems

- Linux File System Architecture
- Filesystem Hierarchy Standard (FHS)
- Extended File System (EXT)
- Second Extended File System (EXT2)
- Third Extended File System (EXT3)
- Fourth Extended File System (EXT4)

o macOS File Systems

Computer Network Fundamentals

- Computer Networks
  - Open System Interconnection (OSI) Model
  - TCP/IP Model
  - Comparing OSI and TCP/IP
  - Types of Networks
  - Wireless Standards
  - Wireless Technologies
  - Network Topologies
  - 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
- Common Fiber Technologies
  - Types of Cables
    - Fiber Optic Cable, Coaxial Cable, CAT 3, CAT 4, CAT 5, CAT 5e, CAT 6, 10/100/1000BaseT (UTP Ethernet)
- TCP/IP Protocol Suite

- Application Layer Protocols
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)
    - ✓ DNS Packet Format
    - ✓ DNS Hierarchy
  - DNSSEC
    - ✓ How DNSSEC Works
    - ✓ Managing DNSSEC for Domain Name
    - ✓ What is a DS Record?
    - ✓ How does DNSSEC Protect Internet Users?
    - ✓ Operation of DNSSEC
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP
  - Hyper Text Transfer Protocol Secure (HTTPS)
  - File Transfer Protocol (FTP)
    - ✓ How FTP Works?
  - Secure File Transfer Protocol (SFTP)
  - Trivial File Transfer Protocol (TFTP)
  - Simple Mail Transfer Protocol (SMTP)
  - S/MIME
    - ✓ How it Works?
  - Pretty Good Privacy (PGP)
  - Difference between PGP and S/MIME
  - Telnet
  - SSH
  - SOAP (Simple Object Access Protocol)
  - Simple Network Management Protocol (SNMP)
  - NTP (Network Time Protocol)
  - RPC (Remote Procedure Call)
  - Server Message Block (SMB) Protocol
  - Session Initiation Protocol (SIP)

- RADIUS
- TACACS+
- Routing Information Protocol (RIP)

o Transport Layer Protocols

- Transmission Control Protocol (TCP)
  - ✓ TCP Header Format
  - ✓ TCP Services
- User Datagram Protocol (UDP)
  - ✓ UDP Operation
- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

o Internet Layer Protocols

- Internet Protocol (IP)
  - ✓ IP Header: Protocol Field
- What is Internet Protocol v6 (IPv6)?
  - ✓ IPv6 Header
  - ✓ IPv4 and IPv6 Transition Mechanisms
  - ✓ IPv4 vs. IPv6
  - ✓ Internet Protocol Security (IPsec)
- Internet Control Message Protocol (ICMP)
  - ✓ Error Reporting and Correction
  - ✓ ICMP Message Delivery
  - ✓ Format of an ICMP Message
- Address Resolution Protocol (ARP)
  - ✓ ARP Packet Format
  - ✓ ARP Packet Encapsulation
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- HSRP (Hot Standby Router Protocol)
- Virtual Router Redundancy Protocol (VRRP)

        - BGP (Border Gateway Protocol)
    - Link Layer Protocols
        - Fiber Distributed Data Interface (FDDI)
        - Token Ring
        - CDP (Cisco Discovery Protocol)
        - VLAN Trunking Protocol (VTP)
        - STP (Spanning Tree Protocol)
        - Point-to-point Protocol (PPP)
- IP Addressing and Port Numbers
    - Internet Assigned Numbers Authority (IANA)
    - IP Addressing
    - Classful IP Addressing
    - Address Classes
    - Subnet Masking
    - Subnetting
    - Supernetting
    - IPv6 Addressing
    - Difference between IPv4 and IPv6
    - Port Numbers
- Network Terminology
    - Routing
    - Network Address Translation (NAT)
    - Port Address Translation (PAT)
    - VLAN
    - Shared Media Network
    - Switched Media Network

Basic Network Troubleshooting

- Unreachable Networks
- Destination Unreachable Message
- ICMP Echo (Request) and Echo Reply
- Time Exceeded Message

- IP Parameter Problem
- ICMP Control Messages
- ICMP Redirects
- Troubleshooting
  - Steps for Network Troubleshooting
    - Troubleshooting IP Problems
    - Troubleshooting Local Connectivity Issues
    - Troubleshooting Physical Connectivity Issues
    - Troubleshooting Routing Problems
    - Troubleshooting Upper-layer Faults
    - Troubleshooting Wireless Network Connection Issues
  - Network Troubleshooting Tools
    - Ping
    - Traceroute and Tracert
    - Ipconfig and Ifconfig
    - NSlookup
    - Netstat
    - PuTTY and Tera Term
    - Subnet and IP Calculators
    - Speedtest.net
    - Pathping and mtr
    - Route

Virtualization

- Introduction to Virtualization
- Characteristics of Virtualization
- Benefits of Virtualization
- Common Virtualization Vendors
- Virtualization Security and Concerns
- Virtual Firewall
- Virtual Operating Systems
- Virtual Databases

Network File System (NFS)

- Network File System (NFS)
- NFS Host and File Level Security

Web Markup and Programming Languages

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

Application Development Frameworks and Their Vulnerabilities

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

Web Subcomponents

- Web Subcomponents
- Thick and Thin Clients
- Applet
- Servlet
- ActiveX
- Flash Application

Database Connectivity

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

Appendix B: Ethical Hacking Essential Concepts - II

Information Security Controls

- Information Security Management Program
- Enterprise Information Security Architecture (EISA)
- Administrative Security Controls
  - Regulatory Frameworks Compliance
  - Information Security Policies
    - Types of Security Policies
    - Examples of Security Policies
    - Privacy Policies at Workplace
    - Steps to Create and Implement Security Policies
    - HR or Legal Implications of Security Policy Enforcement
  - Security Awareness and Training
    - Security Policy
    - Physical Security
    - Social Engineering
    - Data Classification
  - Separation of Duties (SoD) and Principle of Least Privileges (POLP)
- Physical Security Controls
  - Physical Security
  - Types of Physical Security Controls
  - Physical Security Controls

- Technical Security Controls
  - Access Control
  - Types of Access Control
  - Identity and Access Management (IAM)
  - User Identification, Authentication, Authorization, and Accounting
  - Types of Authentication
    - Password Authentication
    - Two-factor Authentication
    - Biometrics
    - Smart Card Authentication
    - Single Sign-on (SSO)
  - Types of Authorization
  - Accounting

Network Segmentation

- Network Segmentation
- Network Security Zoning
- Network Segmentation Example: Demilitarized Zone (DMZ)
- Secure Network Administration Principles
  - Network Virtualization (NV)
  - Virtual Networks
  - VLANs

Network Security Solutions

- Security Incident and Event Management (SIEM)
  - SIEM Architecture
- User Behavior Analytics (UBA)
- Unified Threat Management (UTM)
- Load Balancer
- Network Access Control (NAC)
- Virtual Private Network (VPN)
  - How VPN Works
  - VPN Components

- VPN Concentrators
- Functions of a VPN Concentrator

- Secure Router Configuration
  - Router Security Measures
  - Design, Implement, and Enforce Router Security Policy

Data Leakage

- Data Leakage
- Data Leakage Threats
- What is Data Loss Prevention (DLP)?

Data Backup

- Data Backup
- RAID (Redundant Array Of Independent Disks) Technology
  - Advantages and Disadvantages of RAID Systems
  - RAID Level 0: Disk Striping
  - RAID Level 1: Disk Mirroring
  - RAID Level 3: Disk Striping with Parity
  - RAID Level 5: Block Interleaved Distributed Parity
  - RAID Level 10: Blocks Striped and Mirrored
  - RAID Level 50: Mirroring and Striping Across Multiple RAID Levels
- Selecting an Appropriate Backup Method
- Choosing the Backup Location
- Data Recovery

Risk Management Concepts

- Risk Management
- Risk Management Framework
  - Enterprise Risk Management Framework (ERM)
    - Goals of the ERM Framework
  - NIST Risk Management Framework
  - COSO ERM Framework
  - COBIT Framework
- Enterprise Network Risk Management Policy

- Risk Mitigation
- Control the Risks
- Risk Calculation Formulas
- Quantitative Risk vs. Qualitative Risk

Business Continuity and Disaster Recovery

- Business Continuity (BC)
- Disaster Recovery (DR)
- Business Impact Analysis (BIA)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)

Cyber Threat Intelligence

- Threat Intelligence Frameworks
  - Collective Intelligence Framework (CIF)
- Threat Intelligence Data Collection
- Threat Intelligence Sources
  - Open-Source Intelligence (OSINT)
  - Human Intelligence (HUMINT)
  - Signals Intelligence (SIGINT)
  - Technical Intelligence (TECHINT)
  - Geo-spatial Intelligence (GEOINT)
  - Imagery Intelligence (IMINT)
  - Measurement and Signature Intelligence (MASINT)
  - Covert Human Intelligence Sources (CHIS)
  - Financial Intelligence (FININT)
  - Social Media Intelligence (SOCMINT)
  - Cyber Counterintelligence (CCI)
  - Indicators of Compromise (IoCs)
  - Industry Association and Vertical Communities
  - Commercial Sources

- Government and Law Enforcement Sources
- Threat Intelligence Collection Management
  - Understanding Data Reliability
  - Produce Actionable Threat Intelligence
- Collecting IoCs
- Create an Accessible Threat Knowledge Base
- Organize and Store Cyber Threat Information in Knowledge Base
- Threat Intelligence Reports
  - Generating Concise Reports
- Threat Intelligence Dissemination

Threat Modeling

- Threat Modeling Methodologies
  - STRIDE
  - PASTA
  - TRIKE
  - VAST
  - DREAD
  - OCTAVE
- Threat Profiling and Attribution

Penetration Testing Concepts

- Penetration Testing
- Why do Penetration Testing?
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
- Blue and Red Teaming
- Types of Penetration Testing
- Phases of Penetration Testing
- Security Testing Methodology
- Risks Associated with Penetration Testing
  - Types of Risks Arising During Penetration Testing
- Pre-engagement Activities
- List the Goals of Penetration Testing

- Rules of Engagement (ROE)

Security Operations

- Security Operations
  - Security Operations Center (SOC)
  - SOC Operations
    - Log Collection
    - Log Retention and Archival
    - Log Analysis
    - Monitoring of Security Environments for Security Events
    - Event Correlation
    - Incident Management
    - Threat Identification
    - Threat Reaction
    - Reporting
  - SOC Workflow

Forensic Investigation

- Computer Forensics
- Phases Involved in the Computer Forensics Investigation Process
  - Pre-investigation Phase
  - Investigation Phase
  - Post-investigation Phase

Software Development Security

- Integrating Security in the Software Development Life Cycle (SDLC)
  - Functional vs. Security Activities in the SDLC
  - Advantages of Integrating Security in the SDLC
- Security Requirements
  - Gathering Security Requirements
  - Why We Need Different Approaches for Security Requirement Gathering
  - Key Benefits of Addressing Security at the Requirement Phase
- Secure Application Design and Architecture
  - Goals of the Secure Design Process

- Secure Design Principles
  - Design Secure Application Architecture

Security Governance Principles

- Corporate Governance Activities
- Information Security Governance Activities
  - Program Management
  - Security Engineering
  - Security Operations
- Corporate Governance & Security Responsibilities

Asset Management and Security

- Asset Management
  - Asset Ownership
  - Asset Classification
  - Asset Inventory
  - Asset Value
  - Protection Strategy and Governance
    - Corporate Governance
    - Security Governance