Ethical Hacking Essentials

(Version 1)

Course Outline

Module 01: Information Security Fundamentals

- **Discuss Information Security Fundamentals**
  - What is Information Security?
  - Need for Security
  - Elements of Information Security
  - The Security, Functionality, and Usability Triangle
  - Security Challenges
  - Motives, Goals, and Objectives of Information Security Attacks
  - Classification of Attacks
  - Information Security Attack Vectors
- **Discuss Various Information Security Laws and Regulations**
  - 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: Ethical Hacking Fundamentals

- **Understand Cyber Kill Chain Methodology**
  - Cyber Kill Chain Methodology
  - Tactics, Techniques, and Procedures (TTPs)
  - Adversary Behavioral Identification
  - Indicators of Compromise (IoCs)
    - Categories of Indicators of Compromise
- **Discuss Hacking Concepts and Hacker Classes**
  - What is Hacking?
  - Who is a Hacker?
  - Hacker Classes/Threat Actors
    - Black Hats
    - White Hats
    - Gray Hats
    - Suicide Hackers
    - Script Kiddies
    - Cyber Terrorists
    - State-Sponsored Hackers
    - Hacktivist
    - Hacker Teams
    - Industrial Spies
    - Insider
    - Criminal Syndicates
    - Organized Hackers
- **Understand Different Phases of Hacking Cycle**
  - Hacking Phase: Reconnaissance
  - Hacking Phase: Scanning
  - Hacking Phase: Gaining Access
  - Hacking Phase: Maintaining Access
  - Hacking Phase: Clearing Tracks

- **Discuss Ethical Hacking Concepts, Scope, and Limitations**
  - What is Ethical Hacking?
  - Why Ethical Hacking is Necessary
  - Scope and Limitations of Ethical Hacking
  - Skills of an Ethical Hacker
- **Ethical Hacking Tools**
  - Reconnaissance Using Advanced Google Hacking Techniques
  - Reconnaissance Tools
  - Scanning Tools
  - Enumeration Tools

Lab Exercise

- Perform Passive Footprinting to Gather Information About a Target
  - Gather Information using Advanced Google Hacking Techniques
  - Extract a Company's Data using Web Data Extractor
  - Perform Whois Lookup using DomainTools
- Perform Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network
  - Perform Network Tracerouting in Windows and Linux Machines
  - Perform Host Discovery using Nmap
  - Perform Port and Service Discovery using MegaPing
  - Perform OS Discovery using Unicornscan
- Perform Enumeration on a System or Network to Extract Usernames, Machine Names, Network Resources, Shares, etc.
  - Perform NetBIOS Enumeration using Windows Command-Line Utilities
  - Perform NetBIOS Enumeration using NetBIOS Enumerator

Module 03: Information Security Threats and Vulnerability Assessment

- **Define Threat and Threat Sources**
  - What is a Threat?
  - Threats Sources
    - Natural
    - Unintentional

- Intentional
  - ➢ Internal
  - ➢ External

- **Define Malware and its Types**
  - Introduction to Malware
  - Different Ways for Malware to Enter a System
  - Common Techniques Attackers Use to Distribute Malware on the Web
  - Components of Malware
  - Types of Malware
    - Trojans
      - ✓ What is a Trojan?
      - ✓ Indications of Trojan Attack
      - ✓ How Hackers Use Trojans
      - ✓ Common Ports used by Trojans
      - ✓ Types of Trojans
      - ✓ Creating a Trojan
    - Virus
      - ✓ What is a Virus?
      - ✓ Purpose of Creating Viruses
      - ✓ Indications of Virus Attack
      - ✓ Stages of Virus Lifecycle
      - ✓ How does a Computer Get Infected by Viruses?
      - ✓ Types of Viruses
      - ✓ Creating a Virus
    - Ransomware
    - Computer Worms
      - ✓ How is a Worm Different from a Virus?
      - ✓ Worm Makers
    - Rootkits
    - Potentially Unwanted Application or Applications (PUAs)
      - ✓ Adware

- Spyware
- Keylogger
  - ✓ What a Keylogger can Do?
- Botnets
  - ✓ Why Attackers use Botnets?
- Fileless Malware
  - ✓ Reasons for Using Fileless Malware in Cyber Attacks
  - ✓ Fileless Propagation Techniques

o Malware Countermeasures

- Trojan Countermeasures
- Virus and Worm Countermeasures
- Rootkit Countermeasures
- Spyware Countermeasures
- PUAs/ Adware Countermeasures
- Keylogger Countermeasures
- Fileless Malware Countermeasures

Lab Exercise

o Create a Trojan to Gain Access to the Target System

- Create a Trojan Server using Theef RAT Trojan
- Gain Control over a Victim Machine using the njRAT RAT Trojan

o Create a Virus to Infect the Target System

- Create a Virus using the JPS Virus Maker Tool and Infect the Target System

▪ **Define Vulnerabilities**

o What is Vulnerability?

o Vulnerability Classification

o Examples of Network Security Vulnerabilities

o Impact of Vulnerabilities

▪ **Define Vulnerability Assessment**

o Vulnerability Research

o Resources for Vulnerability Research

- What is Vulnerability Assessment?
- Information Obtained from the Vulnerability Scanning
- Vulnerability Scanning Approaches
- Vulnerability Scoring Systems and Databases
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerabilities and Exposures (CVE)
  - National Vulnerability Database (NVD)
  - Common Weakness Enumeration (CWE)
- Types of Vulnerability Assessment
- Vulnerability-Management Life Cycle
- Vulnerability Assessment Tools
- Vulnerability Exploitation

Lab Exercise

- Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network
  - Perform Vulnerability Analysis using OpenVAS

Module 04: Password Cracking Techniques and Countermeasures

- **Discuss Password Cracking Techniques**
  - Password Cracking
  - Password Complexity
  - Microsoft Authentication
  - Types of Password Attacks
    - Active Online Attacks
      - ✓ Dictionary Attack
      - ✓ Brute-Force Attack
      - ✓ Rule-based Attack
      - ✓ Password Guessing
      - ✓ Default Passwords
      - ✓ Trojans/Spyware/Keyloggers
      - ✓ Hash Injection/Pass-the-Hash (PtH) Attack

- ✓ LLMNR/NBT-NS Poisoning
- ✓ Pass the Ticket Attack

- Passive Online Attacks
  - ✓ Wire Sniffing
  - ✓ Man-in-the-Middle
  - ✓ Replay Attacks
- Offline Attacks
  - ✓ Rainbow Table Attack
- Non-Electronic Attacks

Lab Exercise

- Perform Active Online Attack to Crack the System's Password
  - Perform Active Online Attack to Crack the System's Password using Responder

- **Discuss Password Cracking Tools**
  - Password-Cracking Tools
    - L0phtCrack
    - ophcrack
    - RainbowCrack

Lab Exercise

- Audit System Passwords
  - Audit System Passwords using L0phtCrack
  - Audit System Passwords using John the Ripper

- **Discuss Password Cracking Countermeasures**
  - Password Cracking Countermeasures

Module 05: Social Engineering Techniques and Countermeasures

- **Discuss Social Engineering Concepts and its Phases**
  - What is Social Engineering?
  - Common Targets of Social Engineering
  - Impact of Social Engineering Attack on an Organization
  - Behaviors Vulnerable to Attacks
  - Factors that Make Companies Vulnerable to Attacks

- Why is Social Engineering Effective?
- Phases of a Social Engineering Attack

- **Discuss 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
      - ✓ Pop-Up Windows
      - ✓ Hoax Letters
      - ✓ Chain Letters
      - ✓ Instant Chat Messenger
      - ✓ Spam Email
      - ✓ Scareware
      - ✓ Phishing
        - ➢ Examples of Phishing Emails
        - ➢ Types of Phishing
        - ➢ Phishing Tools
    - Mobile-based Social Engineering
      - ✓ Publishing Malicious Apps
      - ✓ Repackaging Legitimate Apps
      - ✓ Fake Security Applications
      - ✓ SMiShing (SMS Phishing)

Lab Exercise

- Perform Social Engineering using Various Techniques to Sniff Users' Credentials

- Sniff Credentials using the Social-Engineer Toolkit (SET)

- **Discuss Insider Threats and Identity Theft**
  - Insider Threats/Insider Attacks
    - Reasons for Insider Attacks
    - Types of Insider Threats
    - Why are Insider Attacks Effective?
  - Identity Theft
    - Types of Identity Theft
- **Discuss Various Social Engineering Countermeasures**
  - Social Engineering Countermeasures
  - Insider Threats Countermeasures
  - Identity Theft Countermeasures
  - How to Detect Phishing Emails?
  - Anti-Phishing Toolbar
  - Social Engineering Tools
    - Audit Organization's Security for Phishing Attacks using OhPhish

Lab Exercise

- Detect a Phishing Attack
  - Detect Phishing using Netcraft

Module 06: Network Level Attacks and Countermeasures

Sniffing

- **Understand Packet Sniffing Concepts**
  - Packet Sniffing
  - How a Sniffer Works
  - Types of Sniffing
    - Passive Sniffing
    - Active Sniffing
  - How an Attacker Hacks the Network Using Sniffers
  - Protocols Vulnerable to Sniffing
- **Discuss Sniffing Techniques**

- MAC Flooding
- DHCP Starvation Attack
- ARP Spoofing Attack
  - ARP Poisoning Tools
- MAC Spoofing/Duplicating
- DNS Poisoning
- Sniffing Tools
  - Wireshark

Lab Exercise

- Perform MAC Flooding to Compromise the Security of Network Switches
  - Perform MAC Flooding using macof
- Perform ARP Poisoning to Divert all Communication between Two Machines
  - Perform ARP Poisoning using arpspoof

- **Discuss Sniffing Countermeasures**
  - Sniffing Countermeasures
  - Sniffer Detection Techniques
    - Ping Method
    - DNS Method
    - ARP Method

Lab Exercise

- Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy
  - Detect ARP Poisoning in a Switch-Based Network

Denial-of-Service

- **Discuss Types of DoS and DDoS Attacks**
  - What is a DoS Attack?
  - What is a DDoS Attack?
  - DoS/DDoS Attack Techniques
    - UDP Flood Attack
    - ICMP Flood Attack
    - Ping of Death
    - Smurf Attacks

- SYN Flood Attack
- Fragmentation Attack
- Multi-Vector Attack
- Peer-to-Peer Attack
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial-of-Service (DRDoS) Attack

o DoS/DDoS Attack Tools

Lab Exercise

o Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevents Access to System Resources for Legitimate Users

- Perform a DoS Attack on a Target Host using hping3
- Perform a DDoS Attack using HOIC

▪ **Discuss DoS and DDoS Attack Countermeasures**

o Dos/DDoS Attack Countermeasures

o DoS/DDoS Protection Tools

Lab Exercise

o Detect and Protect Against DDoS Attack

- Detect and Protect against DDoS Attack using Anti DDoS Guardian

Session Hijacking

▪ **Discuss Types Session Hijacking Attacks**

o What is Session Hijacking?

o Why is Session Hijacking Successful?

o Session Hijacking Process

o Types of Session Hijacking

o Session Hijacking in OSI Model

o Spoofing vs. Hijacking

o Session Hijacking Tools

Lab Exercise

o Perform Session Hijacking to Seize Control of a Valid TCP Communication Session Between Two Computers

- Hijack a Session using Zed Attack Proxy (ZAP)

- **Discuss Session Hijacking Attack Countermeasures**
  - Session Hijacking Detection Methods
  - Session Hijacking Countermeasures
  - Session Hijacking Detection Tools

Lab Exercise

- Detect Session Hijacking Attempts using Manual Method
  - Detect Session Hijacking using Wireshark

Module 07: Web Application Attacks and Countermeasures

Web Server Attacks

- **Discuss Various Web Server Attacks**
  - Web Server Operations
  - Web Server Components
  - Web Server Security Issues
  - Impact of Web Server Attacks
  - 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
    - Server-Side Request Forgery (SSRF) Attack
  - Web Server Attack Tools

Lab Exercise

- Perform a Web Server Attack to Crack FTP Credentials
  - Crack FTP Credentials using a Dictionary Attack

- **Discuss Web Server Attack Countermeasures**
  - Web Server Attack Countermeasures
  - Web Server Security Tools

Web Application Attacks

- **Understand Web Application Architecture and Vulnerability Stack**
  - Introduction to Web Applications
    - How Web Application Work
  - Web Application Architecture
  - Web Services
    - Types of Web Services
  - Vulnerability Stack
- **Discuss Web Application Threats and Attacks**
  - OWASP Top 10 Application Security Risks – 2017
    - A1 - Injection Flaws
    - 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
    - A8 - Insecure Deserialization
    - A9 - Using Components with Known Vulnerabilities
    - A10 - Insufficient Logging and Monitoring
  - Web Application Attack Tools

Lab Exercise

- Perform a Web Application Attack to Compromise the Security of Web Applications to Steal Sensitive Information
  - Perform Parameter Tampering using Burp Suite

- **Discuss Web Application Attack Countermeasures**
  - Web Application Attack Countermeasures
  - Web Application Security Testing Tools

SQL Injection Attacks

- **Discuss Types of SQL Injection Attacks**
  - What is SQL Injection?
  - Why Bother about SQL Injection?
  - SQL Injection and Server-side Technologies
  - 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
      - Blind SQL Injection: Heavy Query
    - Out-of-Band SQL injection
  - SQL Injection Tools

Lab Exercise

- Perform SQL Injection Attacks on a Target Web Application to Manipulate the Backend Database
  - Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

- **Discuss SQL Injection Attack Countermeasures**
  - SQL Injection Attack Countermeasures
  - SQL Injection Detection Tools

Lab Exercise

- Detect SQL Injection Vulnerabilities using SQL Injection Detection Tools
  - Detect SQL Injection Vulnerabilities using DSSS

Module 08: Wireless Attacks and Countermeasures

- **Understand Wireless Terminology**
  - Wireless Terminology

- Wireless Networks
  - Types of Wireless Networks
- Wireless Standards

- **Discuss Different Types of 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
- **Describe Wireless Network-specific Attack Techniques**
  - Rogue AP Attack
  - Client Mis-association
  - Misconfigured AP Attack
  - Unauthorized Association
  - Ad-Hoc Connection Attack
  - Honeypot AP Attack
  - AP MAC Spoofing
  - Key Reinstallation Attack (KRACK)
  - Jamming Signal Attack
  - Wi-Fi Jamming Devices
  - Cracking WEP Using Aircrack-ng
  - Cracking WPA-PSK Using Aircrack-ng
  - Wireless Attack Tools
    - Aircrack-ng Suite
    - AirMagnet WiFi Analyzer PRO

Lab Exercise

- Perform Wi-Fi Packet Analysis
  - Wi-Fi Packet Analysis using Wireshark
- Perform Wireless Attacks to Crack Wireless Encryption
  - Crack a WEP Network using Aircrack-ng

- Crack a WPA2 Network using Aircrack-ng

- **Understand Bluetooth Attacks**
  - Bluetooth Stack
  - Bluetooth Modes
  - Bluetooth Hacking
  - Bluetooth Threats
  - Bluetooth Attack Tools
- **Discuss Wireless Attack Countermeasures**
  - Wireless Attack Countermeasures
  - Bluetooth Attack Countermeasures
  - Wireless Security Tools

Module 09: Mobile Attacks and Countermeasures

- **Understand Mobile Attack Anatomy**
  - 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
- **Discuss Mobile Platform Attack Vectors and Vulnerabilities**
  - Mobile Attack Vectors
  - Mobile Platform Vulnerabilities and Risks
  - Security Issues Arising from App Stores
  - App Sandboxing Issues
  - Mobile Spam
  - SMS Phishing Attack (SMiShing) (Targeted Attack Scan)
    - Why is SMS Phishing Effective?
    - SMS Phishing Attack Examples
  - Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
  - Agent Smith Attack
  - Exploiting SS7 Vulnerability
  - Simjacker: SIM Card Attack

- Hacking an Android Device Using Metasploit
- Android Hacking Tools
- iOS Hacking Tools

Lab Exercise

- Hack an Android Device by Creating Binary Payloads
  - Hack an Android Device by Creating Binary Payloads using Parrot Security

- **Understand Mobile Device Management (MDM) Concept**
  - Mobile Device Management (MDM)
  - Bring Your Own Device (BYOD)
    - BYOD Risks
- **Discuss Mobile Attack Countermeasures**
  - OWASP Top 10 Mobile Controls
  - General Guidelines for Mobile Platform Security
  - Mobile Security Tools

Lab Exercise

- Secure Android Devices using Various Android Security Tools
  - Secure Android Devices from Malicious Apps using Malwarebytes Security

Module 10: IoT and OT Attacks and Countermeasures

IoT Attacks

- **Understand IoT Concepts**
  - What is the IoT?
  - How the IoT Works
  - IoT Architecture
  - IoT Application Areas and Devices
- **Discuss IoT Threats and Attacks**
  - Challenges of IoT
  - IoT Security Problems
  - OWASP Top 10 IoT Threats
  - 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
  - Fault Injection Attacks
- Capturing and Analyzing IoT Traffic using Wireshark
- IoT Attack Tools

Lab Exercise

- Perform Footprinting using Various Footprinting Techniques
  - Gather Information using Online Footprinting Tools
- Capture and Analyze IoT Device Traffic
  - Capture and Analyze IoT Traffic using Wireshark

- **Discuss IoT Attack Countermeasures**
  - IoT Attack Countermeasures
  - IoT Security Tools

OT Attacks

- **Understand OT Concepts**
  - What is OT?
  - Essential Terminology
  - IT/OT Convergence (IIOT)
  - The Purdue Model
- **Discuss OT Threats and Attacks**
  - Challenges of OT
  - OT Threats
  - OT Attacks
    - HMI-based Attacks
    - Side-Channel Attacks

- Hacking Programmable Logic Controller (PLC)
- Hacking Industrial Systems through RF Remote Controllers
  - ✓ Replay Attack
  - ✓ Command Injection
  - ✓ Re-pairing with Malicious RF controller
  - ✓ Malicious Reprogramming Attack

- OT Attack Tools

- **Discuss OT Attack Countermeasures**
  - OT Attack Countermeasures
  - OT Security Tools

Module 11: Cloud Computing Threats and Countermeasures

- **Understand Cloud Computing Concepts**
  - Introduction to Cloud Computing
  - Types of Cloud Computing Services
  - Separation of Responsibilities in Cloud
  - Cloud Deployment Models
    - Public Cloud
    - Private Cloud
    - Community Cloud
    - Hybrid Cloud
    - Multi Cloud
  - NIST Cloud Deployment Reference Architecture
  - Cloud Storage Architecture
  - Cloud Service Providers
- **Understand Container Technology**
  - What is a Container?
  - Containers Vs. Virtual Machines
  - What is Docker?
  - Microservices Vs. Docker
  - Docker Networking

- Container Orchestration
- What is Kubernetes?
  - Kubernetes Cluster Architecture
- Kubernetes Vs. Docker
- Container Security Challenges
- Container Management Platforms
- Kubernetes Platforms

- **Discuss Cloud Computing Threats**
  - OWASP Top 10 Cloud Security Risks
  - Cloud Computing Threats
  - Cloud Attacks
    - Side-Channel Attacks or Cross-guest VM Breaches
    - Wrapping Attack
    - Man-in-the-Cloud (MITC) Attack
    - Cloud Hopper Attack
    - Cloud Cryptojacking
    - Cloudborne Attack
    - Enumerating S3 Buckets using lazys3
  - Cloud Attack Tools

Lab Exercise

- Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools
  - Enumerate S3 Buckets using lazys3
- Exploit S3 Buckets
  - Exploit Open S3 Buckets using AWS CLI

- **Discuss Cloud Attack Countermeasures**
  - Cloud Attack Countermeasures
  - Cloud Security Tools

Module 12: Penetration Testing Fundamentals

- **Understand Fundamentals of Penetration Testing and its Benefits**
  - What is Penetration Testing?

- Benefits of Conducting a Penetration Test
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
- Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented

- **Discuss Strategies and Phases of Penetration Testing**
  - Strategies of Penetration Testing
    - Black-box
    - White-box
    - Gray-box
  - Penetration Testing Process
  - Phases of Penetration Testing
  - Penetration Testing Methodologies
- **Guidelines and Recommendations for Penetration Testing**
  - Characteristics of a Good Penetration Test
  - When should Pen Testing be Performed?
  - Ethics of a Penetration Tester
  - Evolving as a Penetration Tester
  - Qualification, Experience, Certifications, and Skills Required for a Pen Tester
    - Communication Skills of a Penetration Tester
    - Profile of a Good Penetration Tester
    - Responsibilities of a Penetration Tester
  - Risks Associated with Penetration Testing
    - Types of Risks Arising from Penetration Testing
    - Addressing Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions