

# CEH v13 AI

(Certified Ethical Hacker)

Certification Training



## Course Highlights



**40-Hour**  
Instructor-led  
Training



**EC-Council**  
Authorized  
Partner



Practical Training  
on Latest Tools



Highly Interactive  
and Dynamic  
Sessions



Hands-on Labs



**98%** Exam  
Pass Rate



Access to  
Recorded  
Sessions



Extended Post  
Training Support



Career Guidance  
and Mentorship

# Tools Covered

## 1. Footprinting Tools

- ✓ Maltego
- ✓ Foca
- ✓ Recon-ng
- ✓ Google Dorks
- ✓ Whois
- ✓ theHarvester
- ✓ Shodan
- ✓ Dnsrecon
- ✓ Grecon
- ✓ Photon
- ✓ Sherlock
- ✓ Spiderfoot
- ✓ holehe

## 2. Scanning Tools

- ✓ Nmap
- ✓ Rustscan
- ✓ sx-Tool
- ✓ Colasoft Packet Builder
- ✓ Nessus
- ✓ OpenVAS
- ✓ QualysGuard
- ✓ Nikto
- ✓ Angry IP Scanner
- ✓ Hping3

## 3. Enumeration Tools

- ✓ Netcat
- ✓ SNMPCheck
- ✓ SNMPEnum
- ✓ Enum4Linux
- ✓ NbtScan
- ✓ SuperEnum
- ✓ RPCScan
- ✓ Dnsrecon

## 4. Vulnerability Assessment Tools

- ✓ Nessus
- ✓ OpenVAS
- ✓ QualysGuard
- ✓ Nikto
- ✓ Burp Suite
- ✓ W3af

## 5. System Hacking Tools

- ✓ Metasploit Framework
- ✓ Msfvenom
- ✓ Cain & Cabel
- ✓ John the Ripper
- ✓ Hydra
- ✓ Medusa

- ✓ Hashcat
- ✓ RainbowCrack
- ✓ Havoc
- ✓ PowerSploit
- ✓ Reverse-shell-generator
- ✓ L0pthCrack
- ✓ Winrtgen
- ✓ pwdump7
- ✓ Tanium Endpoint Management

## 6. Sniffing Tools

- ✓ Wireshark
- ✓ Tcpdump
- ✓ Ettercap
- ✓ Dsniff
- ✓ MITM
- ✓ Cain & Abel
- ✓ Macchanger

## 7. Social Engineering Tools

- ✓ Social-Engineer Toolkit (SET)
- ✓ Dark-Phish
- ✓ Shellphish

## 8. Denial of Service Tools

- ✓ Slowloris
- ✓ LOIC
- ✓ HOIC

- ✓ UltraDDoS
- ✓ PyDDoS
- ✓ PyFlooder

## 9. Session Hijacking Tools

- ✓ CAIDO
- ✓ Hetty
- ✓ OWASP ZAP

## 10. Evading IDS, Firewall, and honeypots Tools

- ✓ Nmap
- ✓ Tcpreplay
- ✓ Snort
- ✓ Hping3
- ✓ Pfsense

## 11. Hacking Web Server Tools

- ✓ Ghost\_eye
- ✓ Impacket
- ✓ Ncat
- ✓ NMAP
- ✓ Httprecon
- ✓ ID Serve

## 12. Web Application Hacking Tools

- ✓ OWASP ZAP
- ✓ Burp Suite
- ✓ SQLmap
- ✓ Wapiti
- ✓ Nikto
- ✓ DirBuster
- ✓ Wpscan
- ✓ Skipfish
- ✓ PwnXSS
- ✓ Dirsearch
- ✓ ClickjackPOC

## 13. SQL Injection Tools

- ✓ DSSS
- ✓ ghauri
- ✓ SQLmap

## 14. Hacking Wireless Networks Tools

- ✓ Sparrow-wifi
- ✓ Airodump-ng
- ✓ Aircrack-ng

## 15. Hacking Mobile Platforms Tools

- ✓ AndroRAT
- ✓ PhoneSploit-Pro
- ✓ LOIC

## 16. IoT and OT Tools

- ✓ Bevywise IoT Simulator

## 17. AI Tools

- ✓ ShellGPT
- ✓ Tranis AI
- ✓ Malware.AI
- ✓ ChatGPT
- ✓ DeepfakeVFX
- ✓ SmartScanner
- ✓ OSS Insight
- ✓ DeepExploit
- ✓ Hoodem

## About Course

The **Certified Ethical Hacker (CEH v13)** training program is designed to equip professionals with the essential skills to become proficient in ethical hacking and cybersecurity. The **v13 version** introduces a robust integration of **AI-powered technologies** and advanced techniques to enhance the learning experience and effectiveness of ethical hacking strategies.

Through hands-on labs, real-world simulations, and cutting-edge AI-driven tools, participants will become proficient in ethical hacking techniques and critical cybersecurity practices for defending against traditional and modern AI-powered threats.

## Differences Between CEH v12 and CEH v13

	CEH v12	CEH v13
<b>Total Number of Modules</b>	20	20
<b>Total Number of Slides</b>	1676	1266
<b>Total Number of Labs</b>	220	91 Core Labs + 130 Self-study Labs*
<b>Attack Techniques</b>	519	550
<b>New Technology Added</b>	MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, Techniques for Establishing Persistence, Evading NAC and Endpoint Security, Fog Computing, Edge Computing, and Grid Computing	AI-Driven Ethical Hacking, Active Directory Attacks, Ransomware Attacks and Mitigation, AI and Machine Learning in Cybersecurity, IoT Security Challenges, Critical Infrastructure Vulnerabilities, Deepfake Threats

## Course Objectives

- ✔ Ethical hacking fundamentals, cyber kill chain concepts, an overview of information security and security measures with AI-enhanced threat detection and response.
- ✔ Concepts, methodologies, and tools of footprinting using AI for automated information gathering and reconnaissance.
- ✔ Concepts of vulnerability assessment, its categories and strategies, and AI-driven exposure to technologies used in the industry.
- ✔ Social engineering concepts and terminologies, including identity theft, impersonation, insider threats, social engineering techniques, and AI-based countermeasures.
- ✔ Operational Technology (OT) essentials, threats, attack methodologies, and AI-powered attack prevention.
- ✔ Recognizing vulnerabilities in IoT and ensuring the safety of IoT devices using AI-based security solutions.
- ✔ Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, cryptanalysis, and enhanced cryptographic defense.
- ✔ Cloud computing, threats and security, AI-driven container technology, and serverless computing security measures.

## Target Audience

- ✓ Security Analysts
- ✓ Ethical Hackers
- ✓ System Administrators
- ✓ Network Administrators
- ✓ Network and Security Engineers
- ✓ Cyber Security Managers
- ✓ Information Security Auditors
- ✓ Security Professionals

## Pre-Requisites

- ✓ Basic understanding of network essentials and core concepts, including server and network components.

## Exam Information

Certification Name	C EH v13 (MCQ Exam)	C EH v13 (Practical Exam)
Exam Format	Multiple Choice Questions	iLabs Cyber Range
Number of Questions	125 Questions	20 Questions
Exam Duration	240 Minutes	360 Minutes
Passing Score	60-80%	70%
Exam Delivery	VUE / ECCEXAM	-

# Course Content

## Module 1 Introduction to Ethical Hacking

### ✓ Information Security Overview

- ✓ Elements of Information Security
- ✓ Information Security Attacks
  - Motives (Goals)
  - Tactics, Techniques, and Procedures (TTPs)
  - Vulnerability
- ✓ Classification of Attacks
- ✓ Information Warfare

### ✓ Hacking Concepts

- ✓ What is Hacking?
- ✓ Who is a Hacker and their Motivations?

### ✓ Ethical Hacking Concepts

- ✓ What is Ethical Hacking?
- ✓ Why is Ethical Hacking Necessary?
- ✓ Scope and Limitations of Ethical Hacking
- ✓ Skills of an Ethical Hacker
- ✓ AI-Driven Ethical Hacking
- ✓ How AI-Driven Ethical Hacking Helps Ethical Hackers?
- ✓ Myth: AI will Replace Ethical Hackers
- ✓ ChatGPT-Powered AI Tool

## ✓ Hacking Methodologies and Frameworks

- ✓ CEH Ethical Hacking Framework
- ✓ Cyber Kill Chain Methodology
- ✓ Adversary Behavioral Identification
- ✓ Indicators of Compromise (IoCs)
- ✓ MITRE ATT&CK Framework
- ✓ Diamond Model of Intrusion Analysis

## ✓ 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

## ✓ Information Security Laws and Standards

- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ ISO/IEC Standards
- ✓ 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 2 Footprinting and Reconnaissance

### ✓ Footprinting Concepts

- ✓ Reconnaissance
  - Types of Footprinting/Reconnaissances
- ✓ Information Obtained in Footprinting
- ✓ Objectives of Footprinting
- ✓ Footprinting Threats
- ✓ Footprinting Methodology

### ✓ Footprinting through Search Engines

- ✓ Footprinting Using Advanced Google Hacking Techniques
  - What can a Hacker Do with Google Hacking?
  - Footprinting Using Advanced Google Hacking Techniques with AI
  - Google Hacking Database
- ✓ VPN Footprinting through Google Hacking Database with AI
  - VPN Footprinting through Google Hacking Database with AI
- ✓ Footprinting through SHODAN Search Engine
- ✓ Other Techniques for Footprinting through Search Engines

## ✓ **Footprinting through Internet Research Services**

- ✓ Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI
- ✓ Extracting Website Information from <https://archive.org>
- ✓ Footprinting through People Search Services
- ✓ Footprinting through Job Sites
- ✓ Dark Web Footprinting
  - Searching the Dark Web with Advanced Search Parameters
- ✓ Determining the Operating System
- ✓ Competitive Intelligence Gathering
  - When Did this Company Begin?
  - How Did it Develop?
  - What Are the Company's Plans?
  - What Expert Opinions Say About the Company?
- ✓ Other Techniques for Footprinting through Internet Research Services

## ✓ **Footprinting through Social Networking Sites**

- ✓ People Search on Social Networking Sites
- ✓ Gathering Information from LinkedIn
- ✓ Harvesting Email Lists with AI
- ✓ Analyzing Target Social Media Presence
  - Tools for Footprinting through Social Networking Sites
  - Footprinting through Social Networking Sites with AI

### ✓ **Whois Footprinting**

- ✓ Whois Lookup
- ✓ Finding IP Geolocation Information

### ✓ **DNS Footprinting**

- ✓ Extracting DNS Information
- ✓ DNS Lookup with AI
- ✓ Reverse DNS Lookup

### ✓ **Network and Email Footprinting**

- ✓ Locate the Network Range
- ✓ Traceroute with AI
  - Traceroute Analysis
  - Traceroute Tools
- ✓ Tracking Email Communications
  - Collecting Information from Email Header
  - Email Tracking Tools

### ✓ **Footprinting through Social Engineering**

- ✓ Collecting Information through Social Engineering on Social Networking Sites
- ✓ Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

### ✓ **Footprinting Tasks using Advanced Tools and AI**

- ✓ AI-Powered OSINT Tools
- ✓ Create and Run Custom Python Script to Automate Footprinting Tasks with AI

### ✓ **Footprinting Countermeasures**

**Module 3** Scanning Networks

- ✓ **Network Scanning Concepts**
  - ✓ Overview of Network Scanning
  - ✓ TCP Communication Flags
  - ✓ TCP/IP Communication
- ✓ **Scanning Tools**
- ✓ **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
    - Host Discovery with AI
    - Ping Sweep Tools

## ✔ Port and Service Discovery

- ✔ Port Scanning Techniques
- ✔ TCP Connect/Full-Open Scan
  - Stealth Scan (Half-Open Scan)
  - Inverse TCP Flag Scan
  - Xmas Scan
  - TCP Maimon Scan
  - ACK Flag Probe Scan
  - IDLE/IPID Header Scan
  - UDP Scan
  - SCTP INIT Scan
  - SCTP COOKIE ECHO Scan
  - SSDP and List Scan
  - IPv6 Scan
  - Port Scanning with AI
  - Service Version Discovery with AI
  - Nmap Scan Time Reduction Techniques

## ✔ OS Discovery (Banner Grabbing/OS Fingerprinting)

- ✔ OS Discovery/Banner Grabbing
- ✔ How to Identify Target System OS
  - OS Discovery using Nmap and Unicornscan
  - OS Discovery using Nmap Script Engine
  - OS Discovery using IPv6 Fingerprinting
  - OS Discovery with AI
- ✔ Create and Run Custom Script to Automate Network Scanning Tasks With AI

## ✓ Scanning Beyond IDS and Firewall

- ✓ 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
- ✓ Anonymizers
  - Censorship Circumvention Tools

## ✓ Network Scanning Countermeasures

- ✓ Ping Sweep Countermeasures
- ✓ Port Scanning Countermeasures
- ✓ Banner Grabbing Countermeasures
- ✓ IP Spoofing Detection Techniques
- ✓ IP Spoofing Countermeasures
- ✓ Scanning Detection and Prevention Tools

**Module 4 Enumeration****✓ Enumeration Concepts**

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

**✓ NetBIOS Enumeration**

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

**✓ SNMP Enumeration**

- ✓ Working of SNMP
- ✓ Management Information Base (MIB)
- ✓ Enumerating SNMP using SnmpWalk and Nmap
- ✓ Enumerating SNMP using Nmap
- ✓ SNMP Enumeration Tools
- ✓ SNMP Enumeration with SnmpWalk and Nmap using AI

**✓ LDAP Enumeration**

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

**✓ NTP and NFS Enumeration**

- ✓ NTP Enumeration
- ✓ NTP Enumeration Commands and Tools
- ✓ NFS Enumeration
- ✓ NFS Enumeration Tools

## ✔ SMTP and DNS Enumeration

- ✔ SMTP Enumeration
- ✔ SMTP Enumeration using Nmap
- ✔ SMTP Enumeration using Metasploit
- ✔ SMTP Enumeration Tools
- ✔ SMTP Enumeration using AI
- ✔ DNS Enumeration Using Zone Transfer
- ✔ DNS Cache Snooping
- ✔ DNSSEC Zone Walking
- ✔ DNS Enumeration Using OWASP Amass
- ✔ DNS and DNSSEC Enumeration Using Nmap
- ✔ DNS Enumeration with Nmap Using AI
- ✔ DNS Cache Snooping using AI

## ✔ Other Enumeration Techniques

- ✔ IPsec Enumeration with AI
- ✔ VoIP Enumeration
- ✔ RPC Enumeration
- ✔ Unix/Linux User Enumeration
- ✔ SMB Enumeration with AI
- ✔ Create and Run Custom Script to Automate Network Enumeration Tasks with AI

## ✔ Enumeration Countermeasures

## Module 5 Vulnerability Analysis

### ✓ Vulnerability Assessment Concepts

- ✓ 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
- ✓ Vulnerability Scoring Systems and Databases
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerabilities and Exposures (CVE)
  - National Vulnerability Database (NVD)
  - Common Weakness Enumeration (CWE)
- ✓ Vulnerability-Management Life Cycle
  - Pre-Assessment Phase
  - Vulnerability Assessment Phase
  - Post-Assessment Phase

- ✓ Vulnerability Research
  - Resources for Vulnerability Research
- ✓ Vulnerability Scanning and Analysis
  - Types of Vulnerability Scanning

## ✓ 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
  - Nessus Essentials
  - GFI LanGuard
  - OpenVAS
  - Nikto
  - Qualys Vulnerability Management
- ✓ AI-Powered Vulnerability Assessment Tools
- ✓ Vulnerability Assessment using AI
- ✓ Vulnerability Scan using Nmap with AI
- ✓ Vulnerability Assessment using Python Script with AI
- ✓ Vulnerability Scan using Skipfish with AI

## ✓ Vulnerability Assessment Reports

- ✓ Components of a Vulnerability Assessment Report

**Module 6** System Hacking **Gaining Access** Cracking Passwords

- Microsoft Authentication
- How Hash Passwords Are Stored in Windows SAM?
- Tools to Extract the Password Hashes
- NTLM Authentication Process
- Kerberos Authentication
- Password Cracking
- Types of Password Attacks
  - Non-Electronic Attacks
  - Types of Password Attacks
  - Active Online Attacks
  - Other Active Online Attacks
  - Passive Online Attacks
  - Offline Attacks
- Password Recovery Tools
- 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
- Detecting SMB Attacks Against Windows

**Module 6** System Hacking **Gaining Access**

- ✓ Cracking Passwords
  - Microsoft Authentication
  - How Hash Passwords Are Stored in Windows SAM?
  - Tools to Extract the Password Hashes
  - NTLM Authentication Process
  - Kerberos Authentication
  - Password Cracking
    - Non-Electronic Attacks
    - Types of Password Attacks
    - Active Online Attacks
    - Other Active Online Attacks
    - Passive Online Attacks
    - Offline Attacks
  - Password Recovery Tools
  - 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
  - Detecting SMB Attacks Against Windows

- ✓ Vulnerability Exploitation
  - Exploit Sites
  - Windows Exploit Suggester – Next Generation (WES-NG)
  - Metasploit Framework
  - Metasploit Modules
  - AI-Powered Vulnerability Exploitation Tools
  - Buffer Overflow
    - Types of Buffer Overflow
    - Simple Buffer Overflow in C
    - Windows Buffer Overflow Exploitation
  - Return-Oriented Programming (ROP) Attack
  - Bypassing ASLR and DEP Security Mechanisms
  - Heap Spraying
  - IT Spraying
  - Exploit Chaining
  - Domain Mapping and Exploitation with BloodHound
  - Post AD Enumeration using PowerView
  - Identifying Insecurities Using GhostPack Seatbelt
  - Buffer Overflow Detection Tools
  - Defending Against Buffer Overflow

## ✓ Escalating Privileges

- ✓ Privilege Escalation
- ✓ Privilege Escalation Using DLL Hijacking
- ✓ Privilege Escalation by Exploiting Vulnerabilities
- ✓ Privilege Escalation Using DLL Injection
- ✓ 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 by Bypassing User Account Control (UAC)
- ✓ Privilege Escalation by Abusing Boot or Logon Initialization Scripts
- ✓ Privilege Escalation by Modifying Domain Policy
- ✓ Privilege Escalation by Modifying Other Domain Controllers Group Policies
- ✓ Privilege Escalation by Abusing Active Directory Certificate Services (AD CS)
- ✓ Other Privilege Escalation Techniques
- ✓ Privilege Escalation Tools
- ✓ How to Defend Against Privilege Escalation
  - Tools for Defending Against DLL and Dylib Injection
  - Defending Against Spectre and Meltdown Vulnerabilities
  - Tools for Detecting Spectre and Meltdown Vulnerabilities

## ✓ Maintaining Access

### ✓ Executing Applications

#### → Remote Code Execution Techniques

#### → Keyloggers

- Types of Keyloggers
- Remote Keylogger Attacks Using Metasploit
- Hardware Keyloggers
- Keyloggers for Windows
- Keyloggers for macOS
- How to Defend Against Keyloggers

#### → Anti-Keyloggers

#### → Spyware

- Spyware Tools
- Types of Spyware
- How to Defend Against Spyware

#### → Anti-Spyware

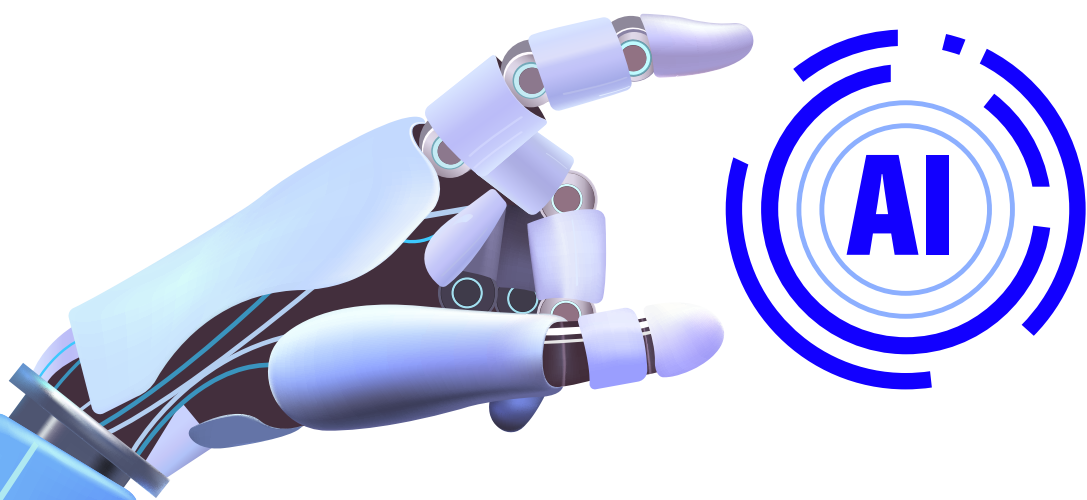
### ✓ Hiding Files

#### → Rootkits

- Types of Rootkits
- How a Rootkit Works
- Popular Rootkits
- Steps for Detecting Rootkits
- How to Defend against Rootkits
- Anti-Rootkits

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

- ✓ Establishing Persistence
  - Maintaining Persistence Using Windows Sticky Keys
  - Maintaining Persistence by Abusing Boot or Logon Autostart Executors
  - Domain Dominance Through Different Paths
    - Remote Code Execution
    - Abusing Data Protection API (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
- ✓ Disable File using Cipher.exe
- ✓ Disable Windows Functionality
- ✓ Deleting Windows Activity History
- ✓ Deleting Incognito History
- ✓ Hiding Artifacts in Windows, Linux, and macOS
- ✓ Anti-Forensics Techniques
- ✓ Track-Covering Tools
- ✓ Defending against Covering Tracks

**Module 7 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
  - Rootkit Trojans
  - Botnet Trojans
  - E-banking Trojans
    - Working of E-banking Trojans
    - E-banking Trojan: CHAVECLOAK

- 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
  - Deploying a Dropper or Downloader
  - Employing a Wrapper
  - Employing a Crypter
  - Propagating and Deploying a Trojan
  - Deploying a Trojan through Email Channels
  - Deploy a Trojan through Covert Channels
  - Deploying a Trojan through Proxy Servers
  - Deploying a Trojan through USB/Flash Drives
  - Techniques for Evading Antivirus Software
  - Exploit Kits

## ✓ Viruses and Worms

- ✓ 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
  - Encrypted 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 Viruses
  - E-mail Viruses
  - Armored Viruses
  - Add-on Viruses
  - Intrusive Viruses
  - Direct Action or Transient Viruses
  - Terminate and Stay Resident (TSR) Viruses

- ✓ How to Infect Systems Using a Virus
  - Propagating and Deploying a Virus
  - Virus Hoaxes
  - Fake AntiVirus
- ✓ Ransomware
  - How to Infect Systems Using a Ransomware: Creating Ransomware
- ✓ Computer Worms
  - How to Infect Systems Using a Worm
  - 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/In-Memory Exploits/ Script-based Injection/Exploiting System Admin Tools/Phishing/ Windows Registry/
- ✓ Fileless Malware Obfuscation Techniques to Bypass Antivirus

### ✓ **AI-based Malware Concepts**

- ✓ What is AI-based Malware?
  - Working of AI-based Malware
- ✓ Indicators of AI-based Malware
- ✓ Challenges of AI-based Malware
- ✓ Techniques Used in AI-based Malware Development
  - Generative Adversarial Networks (GANs)
  - Reinforcement Learning
  - Natural Language Processing (NLP)

- ✓ How to Infect Systems Using a Virus
  - Propagating and Deploying a Virus
  - Virus Hoaxes
  - Fake AntiVirus
- ✓ Ransomware
  - How to Infect Systems Using a Ransomware: Creating Ransomware
- ✓ Computer Worms
  - How to Infect Systems Using a Worm
  - 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/In-Memory Exploits/ Script-based Injection/Exploiting System Admin Tools/Phishing/ Windows Registry/
- ✓ Fileless Malware Obfuscation Techniques to Bypass Antivirus

### ✓ AI-based Malware Concepts

- ✓ What is AI-based Malware?
  - Working of AI-based Malware
- ✓ Indicators of AI-based Malware
- ✓ Challenges of AI-based Malware
- ✓ Techniques Used in AI-based Malware Development
  - Generative Adversarial Networks (GANs)
  - Reinforcement Learning
  - Natural Language Processing (NLP)

- ✓ Examples of AI-based Malware
  - AI-Generated Videos: Malware Spread Through YouTube

## ✓ Malware Analysis

- ✓ What is a Sheep Dip Computer?
- ✓ Antivirus Sensor Systems
- ✓ Malware Analysis Procedure
- ✓ Preparing Testbed
- ✓ Static Malware Analysis
  - File Fingerprinting
  - Local and Online Malware Scanning
  - Performing Strings Search
  - Identifying Packing/Obfuscation Methods
  - Finding the Portable Executables (PE) Information
  - Identifying File Dependencies
  - Malware Disassembly
  - Analyzing ELF Executable Files
  - Analyzing Mach Object (Mach-O) Executable Files
  - Analyzing Malicious MS Office Documents
  - Analyzing Suspicious PDF Document
  - Analyzing Suspicious Documents Using YARA
- ✓ 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
- Scheduled Tasks Monitoring
- Browser Activity Monitoring
  
- ✓ Virus Detection Methods
- ✓ Malware Code Emulation
- ✓ Malware Code Instrumentation
- ✓ Trojan Analysis: Coyote
  - Coyote Malware Attack Phases
- ✓ Virus Analysis: GhostLocker 2.0
  - GhostLocker 2.0 Malware Attack Phases
- ✓ Fileless Malware Analysis: PyLoose
  - PyLoose Malware Attack Phases
- ✓ AI-based Malware Analysis: FakeGPT
  - FakeGPT Malware Attack Phases

## ✓ Malware Countermeasures

- ✓ Trojan Countermeasures
- ✓ Backdoor Countermeasures
- ✓ Virus and Worm Countermeasures
- ✓ Fileless Malware Countermeasures
- ✓ AI-based Malware Countermeasures
- ✓ Adware Countermeasures
- ✓ APT Countermeasures

## ✓ Anti-Malware Software

- ✓ Anti-Trojan Software
- ✓ Antivirus Software
- ✓ Fileless Malware Detection Tools
- ✓ Fileless Malware Protection Tools
- ✓ AI-Powered Malware Detection and Analysis Tools
- ✓ Endpoint Detection and Response (EDR/XDR) Tools

**Module 8 Sniffing****✓ Sniffing Concepts**

- ✓ Network Sniffing
- ✓ How a Sniffer Works
- ✓ Types of Sniffing: Passive/Active Sniffing
- ✓ 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
- ✓ DHCP Attacks
  - How DHCP Works
  - DHCP Request/Reply Messages
  - IPv4 DHCP Packet Format
  - DHCP Starvation Attack
  - Rogue DHCP Server Attack
  - DHCP Attack Tools
  - How to Defend Against DHCP Starvation and Rogue Server Attacks

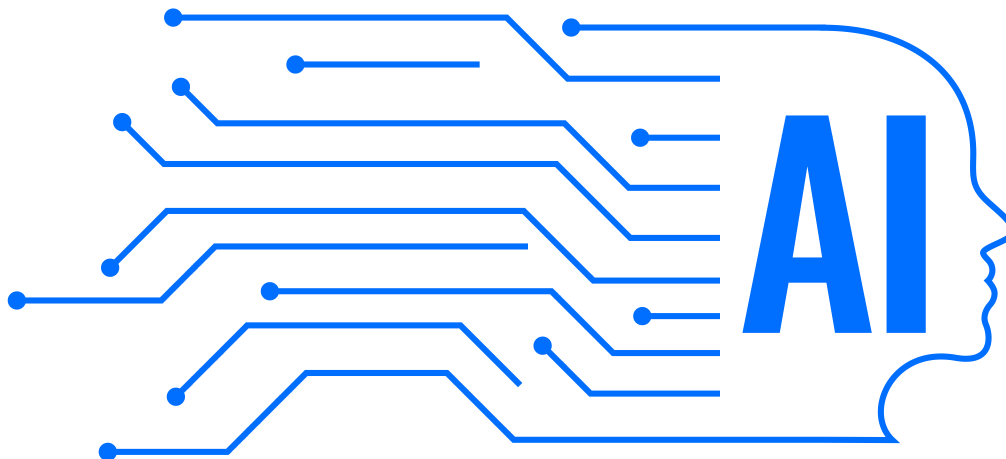
- ✓ ARP Poisoning
  - What Is Address Resolution Protocol (ARP)?
  - ARP Spoofing Attack
  - Threats of ARP Poisoning
  - ARP Spoofing/Poisoning Tools
  - How to Defend Against ARP Poisoning
  - Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
  - ARP Spoofing Detection Tools
- ✓ 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
- ✓ DNS Poisoning
  - DNS Poisoning Techniques
    - Intranet DNS Spoofing
    - Internet DNS Spoofing
    - Proxy Server DNS Poisoning
    - DNS Cache Poisoning
  - DNS Poisoning Tools
  - How to Defend Against DNS Spoofing

## ✓ Sniffing Tools

- ✓ Wireshark
  - Follow TCP Stream in Wireshark
  - Display Filters in Wireshark
  - Additional Wireshark Filters
- ✓ Sniffing Tools

## ✓ Sniffing Countermeasures

- ✓ How to Defend Against Sniffing
- ✓ How to Detect Sniffing
- ✓ Sniffer Detection Techniques
- ✓ Promiscuous Detection Tools



**Module 9** Social Engineering**✓ Social Engineering Concepts**

- ✓ 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
- ✓ Types of Social Engineering

**✓ Human-based Social Engineering Techniques**

- ✓ Impersonation
- ✓ Impersonation (Vishing)
- ✓ Eavesdropping
- ✓ Shoulder Surfing
- ✓ Dumpster Diving
- ✓ Reverse Social Engineering
- ✓ Piggybacking
- ✓ Tailgating
- ✓ Diversion Theft
- ✓ Honey Trap
- ✓ Baiting
- ✓ Quid Pro Quo
- ✓ Elicitation
- ✓ Bait and Switching

- ✓ **Computer-based Social Engineering Techniques**
  - ✓ Phishing (Types/Tools/Examples)
  - ✓ Crafting Phishing Emails with ChatGPT
  - ✓ Perform Impersonation using AI: Create Deepfake Videos
  - ✓ Perform Impersonation using AI: Voice Cloning
  - ✓ Impersonation on Facebook
  - ✓ Perform Impersonation on Social Networking Sites
  - ✓ Social Networking Threats to Corporate Networks
  - ✓ Identity Theft (Types/Techniques/Indicators of Identity Theft)
  
- ✓ **Mobile-based Social Engineering Techniques**
  - ✓ Publishing Malicious Apps
  - ✓ Repackaging Legitimate Apps
  - ✓ Fake Security Applications
  - ✓ QRJacking
  - ✓ SMiShing (SMS Phishing)
  
- ✓ **Social Engineering Countermeasures**
  - ✓ Social Engineering Countermeasures
  - ✓ How to Defend against Phishing Attacks?
  - ✓ Identity Theft Countermeasures
  - ✓ Voice Cloning Countermeasures
  - ✓ Deepfake Attack Countermeasures
  - ✓ How to Detect Phishing Emails?
  - ✓ Anti-Phishing Toolbar
  - ✓ Common Social Engineering Targets and Defense Strategies
  - ✓ Audit Organization's Security for Phishing Attacks using OhPhish

**Module 10 Denial-of-Service****DoS/DDoS Concepts**

- ✓ What is DoS/DDoS Attack?
- ✓ How do DDoS Attacks Work?

**Botnets**

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

**DDoS Case Study**

- ✓ DDoS Attack
- ✓ Hackers Advertise Links for Downloading Botnets
- ✓ Use of Mobile Devices as Botnets for Launching DDoS Attacks
- ✓ DDoS Case Study: HTTP/2 'Rapid Reset' Attack on Google Cloud

**DoS/DDoS Attack Techniques**

- ✓ Basic Categories of DoS/DDoS Attack Vectors
- ✓ DoS/DDoS Attack Techniques
  - UDP Flood Attack
  - ICMP Flood Attack
  - Ping of Death Attack
  - Smurf Attack
  - Pulse Wave DDoS Attack
  - Zero-Day DDoS Attack

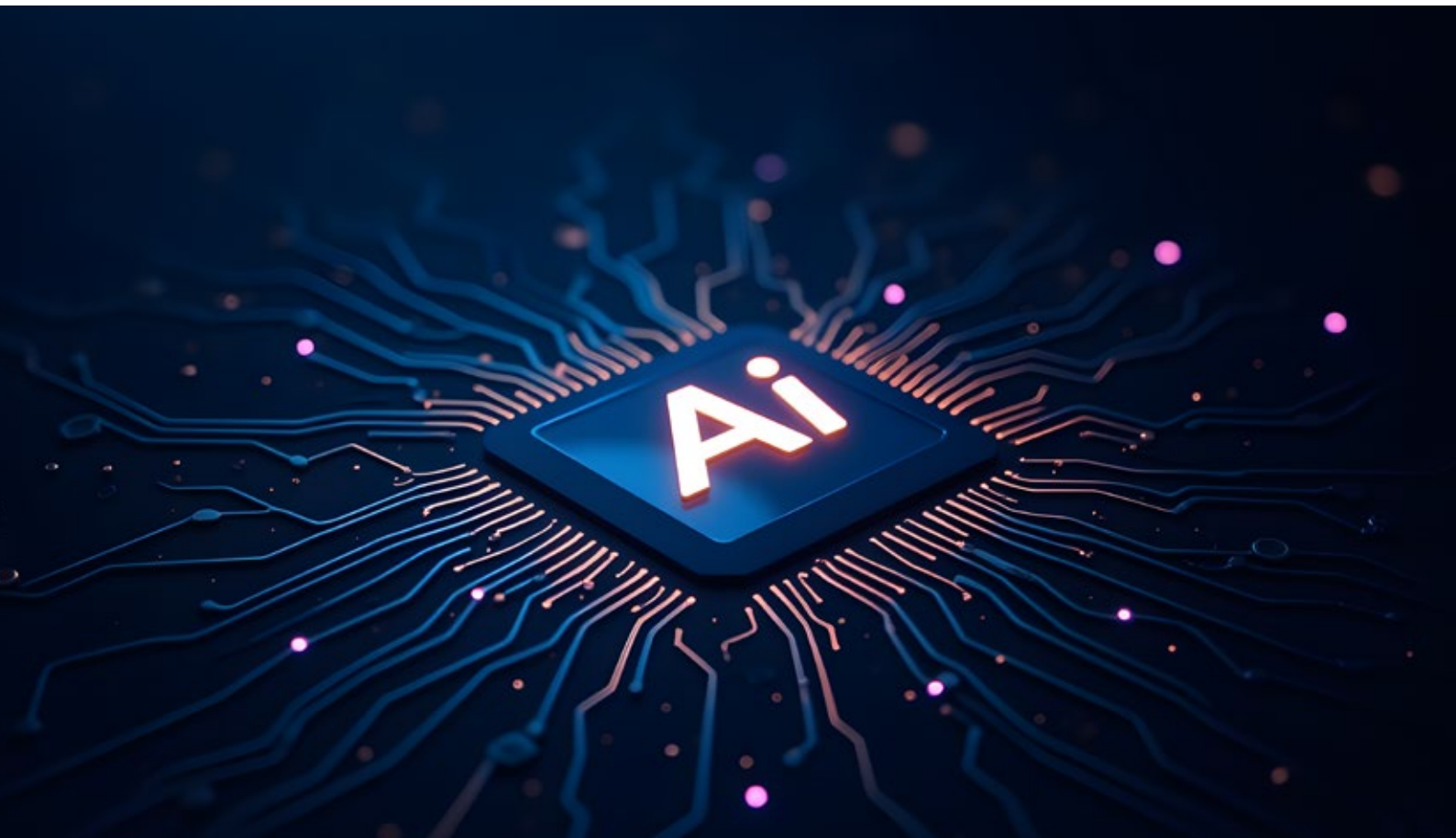
- NTP Amplification Attack
- SYN Flood Attack
- Fragmentation Attack
- Spoofed Session Flood Attack
- HTTP GET/POST Attack
- Slowloris Attack
- UDP Application Layer Flood Attack
- Multi-Vector Attack
- Peer-to-Peer Attack
- Permanent Denial-of-Service Attack
- TCP SACK Panic Attack
- Distributed Reflection Denial-of-Service (DRDoS) Attack
- DDoS Extortion/Ransom DDoS (RDoS) Attack

- ✓ DoS/DDoS Attack Toolkits in the Wild

### ✓ 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/Services



**Module 11** Session Hijacking**✓ Session Hijacking Concepts**

- ✓ What is Session Hijacking?
- ✓ 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**

- ✓ Compromising Session IDs Using Sniffing
- ✓ Compromising Session IDs by Predicting Session Token
  - How to Predict a Session Token
- ✓ Compromising Session IDs Using Man-in-the-Browser/Manipulator-in-the-Browser Attack
- ✓ Compromising Session IDs Using Man-in-the-Browser/Manipulator-in-the-Browser Attack
- ✓ Compromising Session IDs Using Client-side Attacks
  - Cross-site Script Attack
  - Cross-site Request Forgery Attack
- ✓ Compromising Session IDs Using Session Replay Attacks
- ✓ Compromising Session IDs Using Session Fixation
- ✓ Session Hijacking Using Proxy Servers/ CRIME Attack/ Forbidden Attack/ Session Donation Attack

## ✓ Network-Level Session Hijacking

- ✓ Three-way Handshake
- ✓ TCP/IP Hijacking
- ✓ IP Spoofing: Source Routed Packets
- ✓ RST Hijacking
- ✓ Blind Hijacking
- ✓ UDP Hijacking
- ✓ MITM Attack Using Forged ICMP and ARP Spoofing
- ✓ PetitPotam Hijacking

## ✓ Session Hijacking Tools

## ✓ 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 to Prevent Session Hijacking
- ✓ Approaches to Prevent MITM Attacks
- ✓ IPsec
- ✓ Session Hijacking Prevention Tools

**Module 12 Evading IDS, Firewalls, and Honeypots****✓ IDS, IPS, and Firewall Concepts**

- ✓ Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - How an IDS Detects an Intrusion?
  - General Indications of Intrusions
  - Types of Intrusion Detection System (IDS)
  - Types of IDS Alerts
  
- ✓ Firewall
  - Firewall Architecture
  - Demilitarized Zone (DMZ)
  - Types of Firewalls
    - Types of Firewalls Based on Configuration
    - Types of Firewalls Based on Working Mechanism
    - Packet Filtering Firewall
    - Circuit-Level Gateway Firewall
    - Application-Level Firewall
    - Stateful Multilayer Inspection Firewall
    - Application Proxy
    - Network Address Translation (NAT)
    - Virtual Private Network
    - Next-Generation Firewalls (NGFWs)
    - Firewall Limitations

## ✓ IDS, IPS, and Firewall Solutions

- ✓ Intrusion Detection using YARA Rules
- ✓ Intrusion Detection Tools
- ✓ Intrusion Prevention Tools
- ✓ Firewalls

## ✓ Evading IDS/Firewalls

- ✓ IDS/Firewall Evasion Techniques
  - IDS/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 an IDS/Firewall Using a Proxy Server
  - Bypassing an IDS/Firewall through the ICMP Tunneling Method
  - Bypassing an IDS/Firewall through the ACK Tunneling method
  - Bypassing an IDS/Firewall through the HTTP Tunneling Method
  - Bypassing Firewalls through the SSH Tunneling Method
  - Bypassing Firewalls through the DNS Tunneling Method
  - Bypassing an IDS/Firewall through External Systems
  - Bypassing an IDS/Firewall through MITM Attacks
  - Bypassing an IDS/Firewall through Content
  - Bypassing an IDS/WAF using an XSS Attack
  - Other Techniques for Bypassing WAF
  - Bypassing an IDS/Firewall through HTML Smuggling
  - Evading an IDS/Firewall through Windows BITS

- ✓ Other Techniques for IDS Evasion
  - Insertion Attack
  - Evasion
  - Denial-of-Service Attack (DoS)
  - Obfuscating
  - False Positive Generation
  - Session Splicing
  - Unicode Evasion Technique
  - Fragmentation Attack
  - Time-To-Live Attacks
  - Urgency Flag
  - Invalid RST Packets
  - Polymorphic Shellcode
  - ASCII Shellcode
  - Application-Layer Attacks
  - Desynchronization
  - Domain Generation Algorithms (DGA)
  - Encryption
  - Flooding

### ✓ Evading NAC and Endpoint Security

- ✓ NAC and Endpoint Security Evasion Techniques
- ✓ Bypassing NAC using VLAN Hopping/Pre-authenticated Device
- ✓ Bypassing Endpoint Security using Ghostwriting/Application
- ✓ Whitelisting
- ✓ Bypassing Endpoint Security by Dechaining Macros
- ✓ Bypassing Endpoint Security by Clearing Memory Hooks
- ✓ Bypassing Endpoint Security by Process Injection
- ✓ Bypassing the EDR using LoLBins

- ✓ Bypassing Endpoint Security by CPL (Control Panel) Side-Loading
- ✓ Bypassing Endpoint Security using ChatGPT
- ✓ Bypassing Antivirus using Metasploit Templates
- ✓ Bypassing Windows Antimalware Scan Interface (AMSI)
- ✓ Other Techniques for Bypassing Endpoint Security

### ✓ IDS/Firewall Evading Tools

- ✓ Packet Fragment Generator Tools

### ✓ Honeypot Concepts

- ✓ Types of Honeypots
- ✓ Honeypot Tools
- ✓ Detecting and Defeating Honeypots
- ✓ Honeypot Detection Tools

### ✓ IDS/Firewall Evasion Countermeasures

- ✓ How to Defend Against IDS Evasion
- ✓ How to Defend Against Firewall Evasion
- ✓ How to Defend Against Endpoint Security Evasion
- ✓ How to Defend Against NAC Evasion
- ✓ How to Defend Against Anti-virus Evasion

**Module 13 Hacking Web Servers****✓ Web Server Concepts**

- ✓ Web Server Operations
- ✓ Web Server Security Issues
- ✓ Why are Web Servers Compromised?
- ✓ Apache Web Server Architecture
  - Apache Vulnerabilities
- ✓ IIS Web Server Architecture
  - IIS Vulnerabilities
- ✓ NGINX Web Server Architecture
  - NGINX Vulnerabilities

**✓ 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
- ✓ FTP Brute Force with AI
- ✓ HTTP/2 Continuation Flood Attack
- ✓ Frontjacking Attack

- ✓ Other Web Server Attacks
  - Web Server Password Cracking
  - 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
  - Web Server Footprinting with AI
  - Web Server Footprinting using Netcat with AI
- ✓ IIS Information Gathering using Shodan
- ✓ Abusing Apache mod\_userdir to Enumerate User Accounts
- ✓ Enumerating Web Server Information Using Nmap
- ✓ Finding Default Credentials of Web Server
- ✓ Directory Brute Forcing with AI
- ✓ NGINX Vulnerability Scanning using NginxPwner
- ✓ Finding Exploitable Vulnerabilities with AI
- ✓ Session Hijacking
- ✓ Web Server Password Hacking
- ✓ Using Application Server as a Proxy
- ✓ Path Traversal via Misconfigured NGINX Alias
- ✓ 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 Application Security Scanners
- ✓ Web Server Security Scanners
- ✓ Web Server Malware Infection Monitoring Tools
- ✓ Web Server Security Tools
- ✓ Web Server Pentesting Tools

## ✓ Patch Management

- ✓ Patches and Hotfixes
- ✓ What is Patch Management?
- ✓ Installation of a Patch
- ✓ Patch Management Best Practices
- ✓ 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
  - A04 – Insecure Design
  - A05 – Security Misconfiguration
  - A06 – Vulnerable and Outdated Components/Using Components with Known Vulnerabilities
  - A07 – Identification and Authentication Failures/Broken Authentication
  - A08 – Software and Data Integrity Failures
  - A09 – Security Logging and Monitoring Failures/Insufficient Logging and Monitoring
  - A10 – Server-Side Request Forgery (SSRF)
- ✓ Web Application Attacks
  - Directory Traversal
  - Hidden Field Manipulation Attack
  - Pass-the-Cookie Attack
  - Same-Site Attack
  - SQL Injection Attacks

- Command Injection Attacks
- Command Injection Example
- File Injection Attack
- LDAP Injection Attacks
- Other Injection Attacks
- Cross-Site Scripting (XSS) Attacks
- Cross-Site Scripting Attack Scenario: Attack via Email
- XSS Attack in Blog Posting
- XSS Attack in Comment Field
- Techniques to Evade XSS Filters
- Web-based Timing Attacks
- XML External Entity (XXE) Attack
- Unvalidated Redirects and Forwards
- Magecart Attack
- Watering Hole Attack
- Cross-Site Request Forgery (CSRF) Attack
- Cookie/Session Poisoning
- Insecure Deserialization
- Web Service Attack
- Web Service Footprinting Attack
- Web Service XML Poisoning
- DNS Rebinding Attack
- Clickjacking Attack
- MarioNet Attack

## ✓ Web Application Hacking Methodology

- ✓ Footprint Web Infrastructure
  - Server Discovery
  - Server Discovery: Banner Grabbing

- Port and Service Discovery
- Detecting Web App Firewalls and Proxies on Target Site
- WAF Detection with AI
- Hidden Content Discovery
- Detect Load Balancers
  - Detecting Load Balancers using AI
- Detecting Web App Technologies
- WebSockets Enumeration
- ✓ Analyze Web Applications
  - Website Mirroring
  - Website Mirroring with AI
  - Website Mirroring using Htttrack with AI
  - Identify Entry Points for User Input
  - Identify Server-Side Technologies using AI
  - Identify Files and Directories with AI
  - Identify Web Application Vulnerabilities with AI
- ✓ Bypass Client-Side Controls
  - Attack Hidden Form Fields
  - Attack Browser Extensions
  - Attack Google Chrome Browser Extensions
  - Perform Source Code Review
- ✓ Attack Authentication Mechanism
  - Design Flaws in Authentication Mechanism
  - Implementation Flaws in Authentication Mechanism
  - Username Enumeration
  - Password Attacks: Password Functionality Exploits

- Password Attacks: Brute-forcing
- Password Attacks: Attack Password Reset Mechanism
- Authorization Attack: HTTP Request Tampering o Session Attacks:
- Session ID Prediction/Brute Forcing
- Cookie Exploitation: Cookie Poisoning
- Bypass Authentication: Bypass SAML-based SSO
- Bypass Authentication: Bypass Rate Limit
- Bypass Authentication: Bypass Multi-Factor Authentication
- ✓ Attack Authentication Schemes
  - Authorization Attack
  - HTTP Request Tampering
  - Cookie Parameter Tampering
- ✓ Attack Access Controls
  - Exploiting Insecure Access Controls
  - Access Controls Attack Methods
- ✓ Attack Session Management Mechanism
  - Session Management Attack
  - Attacking Session Token Generation Mechanism
  - Attacking Session Tokens Handling Mechanism: Session Token Sniffing
  - Manipulating WebSocket Traffic
- ✓ Perform Injection/Input Validation Attacks
  - Injection Attacks/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
- ✓ Create and Run Custom Scripts to Automate Web Application Hacking Tasks With AI

## **Web API and Webhooks**

- ✓ Web API
  - Web Service APIs
- ✓ Webhooks
- ✓ OWASP Top 10 API Security Risks
- ✓ Webhooks Security Risks
- ✓ API Vulnerabilities
- ✓ Web API Hacking Methodology
  - Identify the Target
  - Detect Security Standards
  - API Enumeration
  - Identify the Attack Surface

- Launch Attacks
- REST API Vulnerability Scanning
- Bypassing IDOR via Parameter Pollution
- ✓ Secure API Architecture
- ✓ 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
  - Web Application Fuzz Testing with AI
  - AI-Powered Fuzz Testing
- ✓ AI-Powered Static Application Security Testing (SAST)
- ✓ AI-Powered Dynamic Application Security Testing (DAST)
- ✓ Source Code Review
- ✓ Encoding Schemes
- ✓ Whitelisting vs. Blacklisting Applications
- ✓ Application Whitelisting and Blacklisting Tools
- ✓ Content Filtering Tools
- ✓ How to Defend Against Injection Attacks
- ✓ Web Application Attack Countermeasures
- ✓ How to Defend Against Web Application Attacks
- ✓ Best Practices for Securing WebSocket Connections
- ✓ RASP for Protecting Web Servers
- ✓ Web Application Security Testing Tools
- ✓ Web Application Firewalls

**Module 15 SQL Injections****✓ 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—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**

- ✓ In-Band SQL Injection
  - Error Based SQL Injection
  - Union SQL Injection
- ✓ Blind/Inferential SQL Injection
  - No Error Message Returned
  - Time-based SQL Injection
  - Boolean Exploitation
  - 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
  - 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 Error Based SQL Injection
  - Perform Error Based SQL Injection using Stored Procedure Injection
  - Perform Union SQL Injection
  - Bypass Website Logins Using SQL Injection
  - Perform Blind SQL Injection — Boolean 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
  - Exporting a Value with Regular Expression Attack
  - Perform Double Blind SQL Injection
  - Perform Blind SQL Injection Using Out-of-Band Exploitation
  - Technique
  - Exploiting Second-Order SQL Injection
  - Bypass Firewall to Perform SQL Injection
  - Bypassing WAF Using JSON-Based SQL Injection Attack
  - Perform SQL Injection to Insert a New User and Update Password

- ✓ Advanced SQL Injection
  - Database, Table, and Column Enumeration
  - Advanced Enumeration
  - 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
- ✓ SQL Injection Tools
- ✓ Discovering SQL Injection Vulnerabilities with AI
- ✓ Checking for Boolean based SQL Injection with AI
- ✓ Checking for Error based SQL Injection with AI
- ✓ Checking for Time-based SQL Injection with AI
- ✓ Checking for UNION based SQL Injection with AI

## ✓ Evasion Techniques

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

## ✓ SQL Injection Countermeasures

- ✓ How to Defend Against SQL Injection Attacks
- ✓ Defenses in the Application
- ✓ Detecting SQL Injection Attacks
- ✓ SQL Injection Detection Tools

**Module 16 Hacking Wireless Networks****Wireless Concepts**

- ✓ Wireless Terminology
- ✓ Wireless Networks
- ✓ Wireless Standards
- ✓ Service Set Identifier (SSID)
- ✓ Wi-Fi Authentication Process
- ✓ Types of Wireless Antennas

**Wireless Encryption**

- ✓ Wired Equivalent Privacy (WEP)
- ✓ Wi-Fi Protected Access (WPA)
- ✓ WPA2
- ✓ WPA3
- ✓ Comparison of WEP, WPA, WPA2, and WPA3
- ✓ Issues with WEP, WPA, WPA2, and WPA3

**Wireless Threats**

- ✓ Access control/ Integrity/ Confidentiality/
- ✓ Availability/Authentication/ Honeypot AP/ Wormhole/ Sinkhole/
- ✓ Inter-Chip Privilege Escalation/ Wireless Co-Existence Attack

**Wireless Hacking Methodology**

- ✓ Wi-Fi Discovery
  - Wireless Network Footprinting
  - Finding Wi-Fi Networks in Range to Attack
  - Wi-Fi Discovery Tools
  - Mobile-based Wi-Fi Discovery Tools
  - Finding WPS-Enabled APs

- ✓ Wireless Traffic Analysis
  - Choosing the Optimal Wi-Fi Card
  - Perform Spectrum Analysis
- ✓ Launch of Wireless Attacks
  - Airocrack-ng Suite
  - Detection of Hidden SSIDs
  - Denial-of-Service
  - Man-in-the-Middle Attack
  - MITM Attack Using Aircrack-ng
  - MAC Spoofing Attack
  - Wireless ARP Poisoning Attack
  - ARP Poisoning Attack Using Ettercap
  - Rogue APs
  - Creation of a Rogue AP Using MANA Toolkit
  - Evil Twin
  - Key Reinstallation Attack (KRACK)
  - Wi-Fi Jamming Signal Attack
  - Wi-Fi Jamming Devices
  - deAUTH Attack
  - Wi-Jacking Attack
  - RFID Cloning Attack
  - WPA/WPA2 Encryption Cracking
  - Cracking WPA/WPA2 Using Aircrack-ng
  - WPA Brute Forcing Using Fern WiFi Cracker
  - WPA3 Encryption Cracking
  - Cracking WPA3 Using Aircrack-ng and hashcat
  - Cracking WPA3 Using Reaver

- ✓ **Wireless Attack Countermeasures**
  - ✓ Defense Against WPA/WPA2/WPA3 Cracking
  - ✓ Defense Against KRACK Attacks
  - ✓ Defense Against aLTER Attacks
  - ✓ Detection and Blocking of Rogue APs
  - ✓ Defense Against Wireless Attacks
  - ✓ Wireless Intrusion Prevention Systems
  - ✓ WIPS Deployment
  - ✓ Wi-Fi Security Auditing Tools
  - ✓ Wi-Fi IPSs



**Module 17 Hacking Mobile Platforms****✓ Mobile Platform Attack Vectors**

- ✓ Vulnerable Areas in Mobile Business Environment
- ✓ OWASP Top 10 Mobile Risks - 2024
- ✓ 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)
- ✓ Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
- ✓ Agent Smith Attack
- ✓ Exploiting SS7 Vulnerability
- ✓ Simjacker: SIM Card Attack
- ✓ Call Spoofing
- ✓ OTP Hijacking/Two-Factor Authentication Hijacking
- ✓ OTP Hijacking Tools
- ✓ Camera/Microphone Capture Attacks
- ✓ Camera/Microphone Hijacking Tools

**✓ Hacking Android OS**

- ✓ Android OS
  - Android Device Administration API

- ✓ Android Rooting
  - Rooting Android Using KingoRoot
  - Android Rooting Tools
- ✓ Hacking Android Devices
  - Identifying Attack Surfaces Using drozer
  - Bypassing FRP on Android Phones Using 4ukey
  - Hacking with zANTI and Kali NetHunter
  - Launch DoS Attack using Low Orbit Ion Cannon (LOIC)
  - Hacking with Orbot Proxy
  - Exploiting Android Device through ADB Using PhoneSploit Pro
  - Launching Man-in-the-Disk Attack
  - Launching Spearphone Attack
  - Exploiting Android Devices Using Metasploit
  - Analyzing Android Devices
  - Other Techniques for Hacking Android Devices
  - Android Malware
- ✓ Android Hacking Tools
- ✓ Android-based Sniffers
- ✓ Securing Android Devices
- ✓ Android Security Tools
  - Android Device Tracking Tools
  - Android Vulnerability Scanners
  - Static Analysis of Android APK
  - Online Android Analyzers

## ✓ Hacking iOS

- ✓ Apple iOS
- ✓ Jailbreaking iOS-
  - Jailbreaking Tools and Techniques
  - Jailbreaking iOS Using Hexxa Plus
- ✓ Hacking iOS Devices
  - Hacking using Spyzie
  - iOS Trustjacking
  - Post-exploitation on iOS Devices Using SeaShell Framework
  - Analyzing and Manipulating iOS Applications
  - Analyzing iOS Devices
  - 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
- ✓ Bring Your Own Device (BYOD)
  - BYOD Risks
  - BYOD Policy Implementation
  - BYOD Security Guidelines

## ✓ Mobile Security Guidelines

- ✓ Mobile Security Guidelines
- ✓ OWASP Top 10 Mobile Risks and Solutions
- ✓ General Guidelines for Mobile Platform Security
- ✓ Mobile Device Security Guidelines for the Administrator
- ✓ SMS Phishing Countermeasures
- ✓ OTP Hijacking Countermeasures
- ✓ Critical Data Storage in Android and iOS: KeyStore and Keychain
- ✓ Recommendations
- ✓ Reverse Engineering Mobile Applications

## ✓ Mobile Security Tools

- ✓ Source Code Analysis Tools
- ✓ Reverse Engineering Tools
- ✓ App Repackaging Detectors
- ✓ Mobile Protection Tools
- ✓ Mobile Anti-Spyware
- ✓ Mobile Pen Testing Toolkits

**Module 18 IoT Hacking & OT Hacking****✓ IoT Hacking****✓ IoT Concepts and Attacks**

- ✓ 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 Security Problems
- ✓ OWASP Top 10 IoT Threats
- ✓ OWASP IoT Attack Surface Areas
- ✓ IoT Vulnerabilities
- ✓ IoT Threats
- ✓ Hacking IoT Devices: General Scenario
- ✓ 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
- ✓ IoT Attacks in Different Sectors
- ✓ IoT Malware
- ✓ Case Study: IZ1H9

## ✓ IoT Hacking Methodology

- ✓ What is IoT Device Hacking?
- ✓ IoT Hacking Methodology
  - Information Gathering
  - Information Gathering using Shodan
  - Information Gathering using MultiPing
  - Information Gathering using FCC ID Search
  - Information-Gathering Tools
  - Information Gathering through Sniffing
  - Sniffing using Cascoda Packet Sniffer
  - Sniffing Tools
  - Vulnerability Scanning
  - Vulnerability Scanning using IoTSeeker
  - Vulnerability Scanning using Genzai
  - Vulnerability Scanning using Nmap
  - Vulnerability-Scanning Tools
  - Analyzing Spectrum and IoT Traffic
  - Tools to Perform SDR-Based Attacks
- ✓ Launch Attacks
  - Rolling Code Attack using RFCrack
  - Hacking Zigbee Devices with Open Sniffer
  - 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
- Exploiting Cameras using CamOver
- ✓ Gain Remote Access
  - Gaining Remote Access using Telnet
  - Maintain Access
  - Maintain Access by Exploiting Firmware
  - Firmware Analysis and Reverse Engineering
- ✓ IoT Hacking Tools
- ✓ IoT Attack Countermeasures
  - How to Defend Against IoT Hacking
  - General Guidelines for IoT Device Manufacturers
  - OWASP Top 10 IoT Vulnerabilities Solutions
  - IoT Framework Security Considerations
  - IoT Hardware Security Best Practices
  - Secure Development Practices for IoT Applications
  - IoT Device Management
  - IoT Security Tools

## ✓ OT Hacking

- ✓ OT Concepts and Attacks
  - What is OT?
  - Essential Terminology
  - Introduction to ICS (Industrial Control Systems)
  - Components of an ICS
  - IT/OT Convergence (IIOT)
  - The Purdue Model

- OT Technologies and Protocols
- Challenges of OT
- OT Vulnerabilities
- MITRE ATT&CK for ICS
- OT Threats
- HMI-Based Attacks
- Side-Channel Attacks
- Hacking Programmable Logic Controller (PLC)
- Evil PLC Attack
- Hacking Industrial Systems through RF Remote Controllers
- OT Supply Chain Attacks
- OT Malware
- OT Malware Analysis: COSMICENERGY
- ✓ OT Hacking Methodology
  - What is OT Hacking?
  - OT Hacking Methodology
  - Information Gathering
    - Identifying ICS/SCADA Systems using Shodan
    - Gathering Default Passwords using CIRT.net
    - Information-Gathering Tools
    - Scanning ICS/SCADA Systems using Nmap
    - Sniffing using NetworkMiner
    - Analyzing Modbus/TCP Traffic using Wireshark
    - Discovering ICS/SCADA Network Protocols using Malcolm
    - Vulnerability Scanning
    - Vulnerability Scanning using Nessus
    - Vulnerability Scanning using Skybox
    - Sniffing and Vulnerability-Scanning Tools
    - Fuzzing ICS Protocols

- Launch Attacks
  - Hacking ICS Hardware
  - Hacking Modbus Slaves using Metasploit
  - Hacking PLC using modbus-cli
- Gain and Maintain Remote Access
  - Gaining Remote Access using DNP3
- 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
  - OT Security Solutions
  - OT Security Tools

**Module 19 Cloud Computing****✓ Cloud Computing Concepts**

- ✓ Introduction to Cloud Computing
- ✓ Types of Cloud Computing Services
- ✓ Shared Responsibilities in Cloud
- ✓ Cloud Deployment Models
- ✓ NIST Cloud Deployment Reference Architecture
- ✓ Cloud Storage Architecture
- ✓ 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?
- ✓ 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 Kubernetes Risks
- ✓ OWASP Top 10 Serverless Security Risks
- ✓ Cloud Computing Threats
  - Data Security
  - Cloud Service Misuse
  - Interface and API Security
  - Operational Security
  - Infrastructure and System Configuration
  - Network Security
  - Governance and Legal Risks
  - Development and Resource Management
- ✓ 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
- Living Off the Cloud Attack (LotC)
- Other Cloud Attacks

✓ Cloud Malware

### ✓ Cloud Hacking

- ✓ Cloud Hacking
- ✓ Cloud Hacking Methodology
  - Identifying Target Cloud Environment
  - Discovering Open Ports and Services Using Masscan
  - Vulnerability Scanning Using Prowler
  - Identifying Misconfigurations in Cloud Resources Using CloudSploit
  - Cleanup and Maintaining Stealth

### ✓ AWS Hacking

- ✓ Enumerating S3 Buckets
  - Enumerating S3 Buckets Using SScanner
  - Enumerating S3 Bucket Permissions Using BucketLoot
  - Enumerating S3 Buckets Using CloudBrute
- ✓ Enumerating EC2 Instances
- ✓ Enumerating AWS RDS Instances
- ✓ Enumerating AWS Account IDs
- ✓ Enumerating IAM Roles
- ✓ Enumerating Weak IAM Policies Using Cloudsplaining
- ✓ Enumerating AWS Cognito

- ✓ Enumerating DNS Records of AWS Accounts Using Ghostbuster
- ✓ Enumerating Serverless Resources in AWS
- ✓ Discovering Attack Paths Using Cartography
- ✓ Discovering Attack Paths Using CloudFox
- ✓ Identify Security Groups Exposed to the Internet
- ✓ AWS Threat Emulation using Stratus Red Team
- ✓ Gathering Cloud Keys Through IMDS Attack
- ✓ Exploiting Misconfigured AWS S3 Buckets
- ✓ Compromising AWS IAM Credentials
- ✓ Hijacking Misconfigured IAM Roles using Pacu
- ✓ Scanning AWS Access Keys using DumpsterDiver
- ✓ Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)
- ✓ Exploiting Shadow Admins in AWS
- ✓ Gaining Access by Exploiting SSRF Vulnerabilities
- ✓ Attacks on AWS Lambda
- ✓ AWS IAM Privilege Escalation Techniques
- ✓ Creating Backdoor Accounts in AWS
- ✓ Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating the CloudTrail Service
- ✓ Establishing Persistence on EC2 Instances
- ✓ Lateral Movement: Moving Between AWS Accounts and Regions
- ✓ AWSGoat: A Damn Vulnerable AWS Infrastructure

### ✓ Microsoft Azure Hacking

- ✓ Azure Reconnaissance Using AADInternals
- ✓ Identifying Azure Services and Resources
- ✓ Enumerating Azure Active Directory (AD) Accounts
- ✓ Identifying Attack Surface using Stormspotter

- ✓ Collecting Data from AzureAD and AzureRM using AzureHound
- ✓ Accessing Publicly Exposed Blob Storage using Gobblin
- ✓ Identifying Open Network Security Groups (NSGs) in Azure
- ✓ Exploiting Managed Identities and Azure Functions
- ✓ Privilege Escalation Using Misconfigured User Accounts in Azure AD
- ✓ Creating Persistent Backdoors in Azure AD Using Service Principals
- ✓ Exploiting VNet Peering Connections
- ✓ AzureGoat – Vulnerable by Design Azure Infrastructure

### ✓ Google Cloud Hacking

- ✓ Enumerating GCP Resources using Google Cloud CLI
  - Enumerating GCP Organizations, Projects, and Cloud Storage Buckets
  - Enumerating Google Cloud Service Accounts
  - Enumerating Google Cloud Resources
  - Enumerating Google Cloud IAM Roles and Policies
  - Enumerating Google Cloud Services using gcp\_service\_enum
  - Enumerating GCP Resources using GCP Scanner
  - Enumerating Google Cloud Storage Buckets using gcloud\_enum
- ✓ Enumerating Privilege Escalation Vulnerabilities using GCP Privilege Escalation Scanner
- ✓ Escalating Privileges of Google Storage Buckets using GCPBucketBrute
- ✓ Maintaining Access: Creating Backdoors with IAM Roles in GCP
- ✓ GCPGoat: Vulnerable by Design GCP Infrastructure

## ✓ Container Hacking

- ✓ Information Gathering using kubectl
- ✓ Enumerating Registries
- ✓ Container/Kubernetes Vulnerability Scanning
- ✓ Exploiting Docker Remote API
- ✓ Hacking Container Volumes
- ✓ LXD/LXC Container Group Privilege Escalation
- ✓ Post Enumeration on Kubernetes etcd

## ✓ 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
- ✓ Assessing Cloud Security using Scout Suite
- ✓ Best Practices for Securing the Cloud
- ✓ Best Practices for Securing AWS Cloud
- ✓ Best Practices for Securing Microsoft Azure
- ✓ Best Practices for Securing Google Cloud Platform
- ✓ NIST Recommendations for Cloud Security
- ✓ Security Assertion Markup Language (SAML)
- ✓ Cloud Network Security
- ✓ Cloud Security Controls
- ✓ 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
- ✓ Next-Generation Secure Web Gateway (NG SWG)



**Module 20** **Cryptography****✓ Cryptography Concepts and Encryption Algorithms**

- ✓ Cryptography
- ✓ Government Access to Keys (GAK)
- ✓ Ciphers
- ✓ Symmetric Encryption Algorithms
- ✓ Data Encryption Standard (DES)
- ✓ Triple Data Encryption Standard (DES)
- ✓ Advanced Encryption Standard (AES)
- ✓ RC4, RC5, and RC6 Algorithms
- ✓ Blowfish
- ✓ Twofish
- ✓ Threefish
- ✓ Serpent
- ✓ TEA
- ✓ CAST-128
- ✓ GOST Block Cipher
- ✓ Camellia
- ✓ Asymmetric Encryption Algorithms
- ✓ DSA and Related Signature Schemes
- ✓ Rivest Shamir Adleman (RSA)
- ✓ Diffie-Hellman
- ✓ Elliptic Curve Cryptography (ECC)
- ✓ YAK
- ✓ Message Digest (One-way Hash) Functions
- ✓ Message Digest Function: MD5 and MD6
- ✓ Message Digest Function: Secure Hashing Algorithm (SHA)

- ✓ RIPEMD-160
- ✓ HMAC
- ✓ CHAP
- ✓ EAP
- ✓ GOST – Hash Function
- ✓ Message Digest Functions Calculators
- ✓ Multi-layer Hashing Calculators
- ✓ Hardware-Based Encryption
- ✓ Quantum Cryptography
- ✓ Other Encryption Techniques
- ✓ Cipher Modes of Operation
- ✓ Modes of Authenticated Encryption
- ✓ Cryptography Tools

### ✓ Applications of Cryptography

- ✓ Public Key Infrastructure (PKI)
- ✓ Certification Authorities
- ✓ Signed Certificate (CA) vs. Self-Signed Certificate
- ✓ Digital Signature
- ✓ Secure Sockets Layer (SSL)
- ✓ Transport Layer Security (TLS)
- ✓ Cryptography Toolkits
- ✓ Pretty Good Privacy (PGP)
- ✓ GNU Privacy Guard (GPG)
- ✓ Web of Trust (WOT)
- ✓ Encrypting Email Messages in Outlook
- ✓ Signing/Encrypting Email Messages on Mac
- ✓ Encrypting/Decrypting Email Messages Using OpenPGP
- ✓ Email Encryption Tools

- ✓ Disk Encryption
- ✓ Disk Encryption Tools for Linux/macOS
- ✓ Blockchain

## ✓ Cryptanalysis

- ✓ Cryptanalysis Methods
- ✓ Cryptography Attacks
- ✓ Code-Breaking Methodologies
- ✓ Brute-Force Attack
- ✓ Birthday Attack
- ✓ Birthday Paradox: Probability
- ✓ Brute Forcing VeryCrypt Encryption
- ✓ Meet-in-the-Middle Attack on Digital Signature Schemes
- ✓ Side-Channel Attack
- ✓ Hash Collision Attack
- ✓ DUHK Attack
- ✓ DROWN Attack
- ✓ Rainbow Table Attack
- ✓ Related-Key Attack
- ✓ Padding Oracle Attack
- ✓ Attacks on Blockchain
- ✓ Quantum Computing Risks
- ✓ Quantum Computing Attacks
- ✓ Cryptanalysis Tools
- ✓ Online MD5 Decryption Tools

## ✓ Cryptography Attack Countermeasures

- ✓ How to Defend Against Cryptographic Attacks
- ✓ Key Stretching



[www.infosectrain.com](http://www.infosectrain.com) | [sales@infosectrain.com](mailto:sales@infosectrain.com)