# EC-Council Certified Ethical Hacker (CEH) v11.0

Length Days: 5
Length Hours: 40
Language: Bulgarian or English

# Course Outline

**(Version 11)**

## 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

### Cyber Kill Chain Concepts

- Cyber Kill Chain Methodology
- Tactics, Techniques, and Procedures (TTPs)
- Adversary Behavioral Identification
- Indicators of Compromise (IoCs)

### Hacking Concepts

- What is Hacking?
- Who is a Hacker?
- Hacker Classes
- Hacking Phase: Reconnaissance
- Hacking Phase: Scanning
- Hacking Phase: Gaining Access
- Hacking Phase: Maintaining Access
- Hacking Phase: Clearing Tracks

### Ethical Hacking Concepts

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

- Skills of an Ethical Hacker

**Information Security Controls**

- Information Assurance (IA)
- Defense-in-Depth
- What is Risk?
- Cyber Threat Intelligence
- Threat Modeling
- Incident Management
- Role of AI and ML in Cyber Security

**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)
- Cyber Law in Different Countries

## Module 02: Footprinting and Reconnaissance

**Footprinting Concepts**

- What is Footprinting?

**Footprinting through Search Engines**

- Footprinting through Search Engines
- Footprint Using Advanced Google Hacking Techniques
- Google Hacking Database
- VoIP and VPN Footprinting through Google Hacking Database
- Other Techniques for Footprinting through 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
- Gather Information from Financial Services
- 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

**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
- 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
- Extracting Website Links
- Gathering Wordlist from the Target Website
- Extracting Metadata of Public Documents
- Other Techniques for Website Footprinting

**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

**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: Hping2/Hping3
- Scanning Tools
- Scanning Tools for Mobile

**Host Discovery**

- Host Discovery Techniques

**Port and Service Discovery**

- Port Scanning Techniques
- Service Version Discovery
- Nmap Scan Time Reduction Techniques
- Port Scanning Countermeasures

**OS Discovery (Banner Grabbing/OS Fingerprinting)**

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

**Scanning Beyond IDS and Firewall**

- IDS/Firewall Evasion Techniques

**Draw Network Diagrams**

- Drawing Network Diagrams
- Network Discovery and Mapping Tools
- Network Discovery Tools for Mobile

## Module 04: Enumeration

**Enumeration Concepts**

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

**NetBIOS Enumeration**

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

**SNMP Enumeration**

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

**LDAP Enumeration**

- LDAP Enumeration
- LDAP Enumeration Tools

**NTP and NFS Enumeration**

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

**SMTP and DNS Enumeration**

- SMTP Enumeration
- SMTP Enumeration Tools
- DNS Enumeration Using Zone Transfer
- DNS Cache Snooping
- DNSSEC Zone Walking

**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

## Module 05: Vulnerability Analysis

**Vulnerability Assessment Concepts**

- Vulnerability Research
- Resources for Vulnerability Research
- What is Vulnerability Assessment?
- Vulnerability Scoring Systems and Databases
- Vulnerability-Management Life Cycle

**Vulnerability Classification and Assessment Types**

- Vulnerability Classification
- Types of Vulnerability Assessment

**Vulnerability Assessment Solutions and 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
- Analyzing Vulnerability Scanning Report

## Module 06: System Hacking

**System Hacking Concepts**

- CEH Hacking Methodology (CHM)
- System Hacking Goals

**Gaining Access**

- Cracking Passwords
- Vulnerability Exploitation

**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
- Other Privilege Escalation Techniques
- Privilege Escalation Tools
- How to Defend Against Privilege Escalation

**Maintaining Access**

- Executing Applications
- Hiding Files

**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
- 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

**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
- How to Infect Systems Using a Trojan

**Virus and Worm Concepts**

- Introduction to Viruses
- Stages of Virus Lifecycle
- Working of Viruses
- Types of Viruses
- How to Infect Systems Using a Virus: Creating a Virus
- How to Infect Systems Using a Virus: Propagating and Deploying a Virus
- Computer Worms

**Fileless Malware Concepts**

- What is Fileless Malware?
- Taxomony 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
- 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
- Dynamic Malware Analysis
- Virus Detection Methods

- Trojan Analysis: Emotet
- Virus Analysis: SamSam Ransomware
- Fileless Malware Analysis: Astaroth Attack

**Countermeasures**

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

**Anti-Malware Software**

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

**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
- DNS Poisoning Tools
- How to Defend Against DNS Spoofing

**Sniffing Tools**

- Sniffing Tool: Wireshark
- Sniffing Tools
- Packet Sniffing Tools for Mobile Phones

**Countermeasures**

- How to Defend Against Sniffing

**Sniffing Detection Techniques**

- How to Detect Sniffing
- Sniffer Detection Techniques: Ping Method and DNS Method
- Sniffer Detection Techniques: 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
- Computer-based Social Engineering
- Mobile-based Social Engineering

**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

**Countermeasures**

- Social Engineering Countermeasures
- 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?

**DoS/DDoS Attack Techniques**

- Basic Categories of DoS/DDoS Attack Vectors
- Multi-Vector Attack
- Peer-to-Peer Attack
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial-of-Service (DRDoS) 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?

**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 GitHub

**DoS/DDoS Attack Tools**

- DoS/DDoS Attack Tools
- DoS and DDoS Attack Tools for Mobiles

**Countermeasures**

- Detection Techniques
- DoS/DDoS Countermeasure Strategies
- DDoS Attack Countermeasures
- Techniques to Defend against Botnets
- Additional DoS/DDoS Countermeasures
- DoS/DDoS Protection at ISP Level
- Enabling TCP Intercept on Cisco IOS Software

**DoS/DDoS Protection Tools**

- Advanced DDoS Protection Appliances
- DoS/DDoS Protection Tools
- DoS/DDoS 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
- Compromising Session IDs Using Man-in-the-Middle Attack
- Compromising Session IDs Using 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

**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

**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

- Approaches to Prevent MITM Attacks
- IPSec
- Session Hijacking Prevention Tools

## Module 12: Evading IDS, Firewalls, and Honeypots

**IDS, IPS, Firewall, and Honeypot Concepts**

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Firewall
- Honeypot

**IDS, IPS, Firewall, and Honeypot Solutions**

- Intrusion Detection Tools
- Intrusion Prevention Tools
- Firewalls
- Honeypot Tools

**Evading IDS**

- IDS Evasion Techniques

**Evading Firewalls**

- Firewall Evasion Techniques

**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**

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

**Web Server Attack Methodology**

- Information Gathering
- Web Server Footprinting/Banner Grabbing
- Website Mirroring
- Vulnerability Scanning
- Session Hijacking
- Web Server Password Hacking
- Using Application Server as a Proxy

**Web Server Attack Tools**

- Metasploit
- Web Server Attack Tools

**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

**Patch Management**

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

**Web Server Security Tools**

- Web Application Security Scanners
- Web Server Security Scanners
- Web Server Malware Infection Monitoring Tools
- Web Server Security Tools
- Web Server Pen Testing 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 – 2017
- Other Web Application Threats

**Web Application Hacking Methodology**

- Web Application Hacking Methodology
- Footprint Web Infrastructure
- Analyze Web Applications
- Bypass Client-side Controls
- Attack Authentication Mechanism
- Attack Authorization Schemes
- Attack Access Controls
- Attack Session Management Mechanism
- Perform Injection/Input Validation Attacks
- Attack Application Logic Flaws
- Attack Shared Environments
- Attack Database Connectivity
- Attack Web Application Client
- Attack Web Services

- Additional Web Application Hacking Tools

**Web API, Webhooks, and Web Shell**

- What is Web API?
- What are Webhooks?
- OWASP Top 10 API Security Risks
- API Vulnerabilities
- Web API Hacking Methodology
- Web Shells
- Gaining Backdoor Access via Web Shell
- How to Prevent Installation of a Web Shell
- Web Shell Detection Tools
- 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
- Source Code Review
- Encoding Schemes
- Whitelisting vs. Blacklisting Applications
- 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

**SQL Injection Methodology**

- Information Gathering and SQL Injection Vulnerability Detection
- Launch SQL Injection Attacks
- Advanced SQL Injection

**SQL Injection Tools**

- SQL Injection Tools
- SQL Injection Tools for Mobile Devices

**Evasion Techniques**

- Evading IDS
- Types of Signature Evasion Techniques

**Countermeasures**

- How to Defend Against SQL Injection Attacks
- 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 Modes
- Wi-Fi Authentication Process Using a Centralized Authentication Server
- Types of Wireless Antennas

**Wireless Encryption**

- Types of Wireless Encryption
- Comparison of WEP, WPA, WPA2, and WPA3
- Issues in WEP, WPA, and WPA2

**Wireless Threats**

- Wireless Threats

**Wireless Hacking Methodology**

- Wireless Hacking Methodology
- Wi-Fi Discovery
- GPS Mapping
- Wireless Traffic Analysis
- Launch of Wireless Attacks
- Wi-Fi Encryption Cracking

**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
- Bluetooth Hacking Tools

**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)
- Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
- Agent Smith Attack
- Exploiting SS7 Vulnerability
- Simjacker: SIM Card Attack

**Hacking Android OS**

- Android OS
- Android Rooting
- Hacking Android Devices
- Android Hacking Tools
- Securing Android Devices
- Android Security Tools

**Hacking iOS**

- Apple iOS
- Jailbreaking iOS
- Hacking iOS Devices
- Securing iOS Devices
- iOS Device Security Tools
- iOS Device Tracking Tools

**Mobile Device Management**

- Mobile Device Management (MDM)
- Mobile Device Management Solutions: IBM MaaS360
- Bring Your Own Device (BYOD)

**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
- Reverse Engineering Mobile Applications
- Mobile Security Tools

## 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
- IoT Attacks in Different Sectors
- Case Study: Dyn Attack

**IoT Hacking Methodology**

- What is IoT Device Hacking?
- IoT Hacking Methodology

**IoT Hacking Tools**

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

**Countermeasures**

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

**OT Attacks**

- OT Vulnerabilities
- OT Threats
- OT Attacks
- OT Malware Analysis: LockerGoga Ransomware

**OT Hacking Methodology**

- What is OT Hacking?
- OT Hacking Methodology

**OT Hacking Tools**

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

**Countermeasures**

- How to Defend Against OT Hacking
- OT Vulnerabilities and Solutions
- How to Secure an IT/OT Environment
- 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
- Separation of Responsibilities in Cloud
- Cloud Deployment Models
- NIST Cloud Deployment Reference Architecture
- Cloud Storage Architecture
- Role of AI in Cloud Computing
- Virtual Reality and Augmented Reality on Cloud
- Cloud Service Providers

**Container Technology**

- What is a Container?
- Containers Vs. Virtual Machines
- What is Docker?
- Container Orchestration
- What is Kubernetes?
- 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

**Cloud Hacking**

- What is Cloud Hacking?
- Hacking Cloud
- 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
- 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
- Cloud Security Tools
- Container Security Tools
- Kubernetes Security Tools
- Serverless Application Security 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
- Other Encryption Techniques
- Comparison of Cryptographic Algorithms

**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)

**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)
- Email Encryption Tools

**Disk Encryption**

- Disk Encryption
- Disk Encryption Tools: VeraCrypt and Symantec Drive Encryption
- Disk Encryption Tools

**Cryptanalysis**

- Cryptanalysis Methods
- Code Breaking Methodologies

- Cryptography Attacks
- Cryptanalysis Tools
- Online MD5 Decryption Tools

**Countermeasures**

- How to Defend Against Cryptographic Attacks
- Key Stretching