Version Change Document

EC-Council
Official Curricula

EC-Council C|EH v13

Certified Ethical Hacker

Ethical Hacking and Countermeasures

Version Comparison

	CEHv12	CEHv13
Total Number of Modules	**20**	**20**
Total Number of Slides	**1676**	**1266**
Total Number of Labs	**220**	**91 Core Labs + 130 Self-study Labs***
Attack Techniques	**519**	**550**
New Technology Added	**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**
OS Used for Labs	**Windows 11, Windows Server 2022, Windows Server 2019, Parrot Security, Android, Ubuntu Linux**	**Windows 11, Windows Server 2022, Windows Server 2019, Parrot Security, Android, Ubuntu Linux**
Exam	**125 Questions (MCQ)**	**125 Questions (MCQ)**
Exam Duration	**4 Hours**	**4 Hours**
Exam Delivery	**VUE / ECCEXAM**	**VUE / ECCEXAM**
NICE Compliance	**Final NICE 2.0 Framework**	**Final NICE 2.0 Framework**

* Self-study labs will be available separately as the **CEH Self Study Upgrade Lab Pack**.

CEHv13 Change Summary

1. The Module 01: Introduction to Ethical Hacking module includes AI-driven ethical hacking in CEHv13
2. The Module 2: Footprinting and Reconnaissance to Module 7: Malware Threats, Module 9: Social Engineering, and Module 13: Hacking Web Servers to Module 15: SQL Injection cover various techniques to automate hacking using AI in CEHv13
3. The Module 06: System Hacking includes exploitation of AD environments in CEHv13.
4. The Module 07: Malware Threats includes malware analysis for the latest malware in CEHv13
5. The Module 07: Malware Threats includes AI-based malware concepts in CEHv13
6. The Module 09: Social Engineering includes deepfake attacks in CEHv13
7. The Module 13: Hacking Web Servers includes Apache, IIS, and NGINX architecture, vulnerabilities, and hacking in CEHv13
8. The Module 17: Hacking Mobile Platforms includes analyzing Android and iOS devices in CEHv13.
9. The Module 19: Cloud Computing includes AWS, Azure, Google Cloud, and container hacking sections in CEHv13
10. The Module 20: Cryptography includes attacks and risks on Blockchain and quantum computing in CEHv13
11. Update information as per the latest developments with a proper flow
12. Latest OS covered and a patched testing environment
13. All the tool screenshots are replaced with the latest version
14. All the tool listing slides are updated with the latest tools
15. All the countermeasure slides are updated

Module Comparison

CEHv12	CEHv13
Module 01: Introduction to Ethical Hacking	Module 01: Introduction to Ethical Hacking
Module 02: Footprinting and Reconnaissance	Module 02: Footprinting and Reconnaissance
Module 03: Scanning Networks	Module 03: Scanning Networks
Module 04: Enumeration	Module 04: Enumeration
Module 05: Vulnerability Analysis	Module 05: Vulnerability Analysis
Module 06: System Hacking	Module 06: System Hacking
Module 07: Malware Threats	Module 07: Malware Threats
Module 08: Sniffing	Module 08: Sniffing
Module 09: Social Engineering	Module 09: Social Engineering
Module 10: Denial-of-Service	Module 10: Denial-of-Service
Module 11: Session Hijacking	Module 11: Session Hijacking
Module 12: Evading IDS, Firewalls, and Honeypots	Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: Hacking Web Servers	Module 13: Hacking Web Servers
Module 14: Hacking Web Applications	Module 14: Hacking Web Applications
Module 15: SQL Injection	Module 15: SQL Injection
Module 16: Hacking Wireless Networks	Module 16: Hacking Wireless Networks
Module 17: Hacking Mobile Platforms	Module 17: Hacking Mobile Platforms
Module 18: IoT and OT Hacking	Module 18: IoT and OT Hacking
Module 19: Cloud Computing	Module 19: Cloud Computing
Module 20: Cryptography	Module 20: Cryptography

Courseware Content Comparison

The notations used:

1. **Red** points are new slides in CEHv13
2. **Blue** points are substantially modified in CEHv13
3. ~~**Striked**~~ points are removed from CEHv12

CEHv12	CEHv13
Module 01: Introduction to Ethical Hacking	**Module 01: Introduction to Ethical Hacking**
Information Security Overview	**Information Security Overview**
▪ Elements of Information Security	▪ Elements of Information Security
▪ Motives, Goals, and Objectives of Information Security Attacks	▪ Information Security Attacks: Motives, Goals, and Objectives
▪ Classification of Attacks	○ Motives (Goals)
▪ Information Warfare	○ Tactics, Techniques, and Procedures (TTPs)
Hacking Methodologies and Frameworks	○ Vulnerability
▪ CEH Hacking Methodology (CHM)	▪ Classification of Attacks
▪ Cyber Kill Chain Methodology	▪ Information Warfare
▪ Tactics, Techniques, and Procedures (TTPs)	**Hacking Concepts**
▪ Adversary Behavioral Identification	▪ What is Hacking?
▪ Indicators of Compromise (IoCs)	▪ Who is a Hacker?
○ Categories of Indicators of Compromise	▪ Hacker and their Motivations
▪ MITRE ATT&CK Framework	**Ethical Hacking Concepts**
▪ Diamond Model of Intrusion Analysis	▪ What is Ethical Hacking?
Hacking Concepts	▪ Why Ethical Hacking is Necessary
▪ What is Hacking?	▪ Scope and Limitations of Ethical Hacking
▪ Who is a Hacker?	▪ Skills of an Ethical Hacker
▪ Hacker Classes	▪ AI-Driven Ethical Hacking
Ethical Hacking Concepts	▪ How AI-Driven Ethical Hacking Helps Ethical Hacker?
▪ What is Ethical Hacking?	▪ Myth: AI will Replace Ethical Hackers
▪ Why Ethical Hacking is Necessary	▪ ChatGPT-Powered AI Tools for Ethical Hackers
▪ Scope and Limitations of Ethical Hacking	**Hacking Methodologies and Frameworks**
▪ Skills of an Ethical Hacker	▪ CEH Ethical Hacking Framework
Information Security Controls	▪ Cyber Kill Chain Methodology
▪ Information Assurance (IA)	○ Tactics, Techniques, and Procedures (TTPs)
▪ Continual/Adaptive Security Strategy	▪ Adversary Behavioral Identification
▪ Defense-in-Depth	▪ Indicators of Compromise (IoCs)

▪ What is Risk?	○ Categories of Indicators of Compromise
▪ Risk Management	▪ MITRE ATT&CK Framework
▪ Cyber Threat Intelligence	▪ Diamond Model of Intrusion Analysis
○ Threat Intelligence Lifecycle	**Information Security Controls**
▪ Threat Modeling	▪ Information Assurance (IA)
▪ Incident Management	▪ Continual/Adaptive Security Strategy
○ Incident Handling and Response	▪ Defense-in-Depth
▪ Role of AI and ML in Cyber Security	▪ What is Risk?
○ How Do AI and ML Prevent Cyber Attacks?	▪ Risk Management
Information Security Laws and Standards	▪ Cyber Threat Intelligence
▪ Payment Card Industry Data Security Standard (PCI DSS)	▪ Threat Intelligence Lifecycle
▪ ~~ISO/IEC 27001:2013~~	▪ Threat Modeling
▪ Health Insurance Portability and Accountability Act (HIPAA)	▪ Incident Management
▪ Sarbanes Oxley Act (SOX)	▪ Incident Handling and Response
▪ The Digital Millennium Copyright Act (DMCA)	▪ Role of AI and ML in Cyber Security
▪ The Federal Information Security Management Act (FISMA)	○ How Do AI and ML Prevent Cyber Attacks?
▪ General Data Protection Regulation (GDPR)	**Information Security Laws and Standards**
▪ Data Protection Act 2018 (DPA)	▪ Payment Card Industry Data Security Standard (PCI DSS)
▪ Cyber Law in Different Countries	▪ 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 02: Footprinting and Reconnaissance	**Module 02: Footprinting and Reconnaissance**
Footprinting Concepts	**Footprinting Concepts**
▪ What is Footprinting?	▪ Reconnaissance
▪ Information Obtained in Footprinting	○ Types of Footprinting/Reconnaissance
▪ Footprinting Methodology	▪ Information Obtained in Footprinting
Footprinting through Search Engines	▪ Objectives of Footprinting

▪ Footprinting through Search Engines	▪ Footprinting Threats
▪ Footprint Using Advanced Google Hacking Techniques	▪ Footprinting Methodology
▪ Google Hacking Database	**Footprinting through Search Engines**
▪ VPN Footprinting through Google Hacking Database	▪ Footprinting Using Advanced Google Hacking Techniques
▪ Other Techniques for Footprinting through Search Engines	○ What can a Hacker Do with Google Hacking?
○ Google Advanced Search	○ Footprinting Using Advanced Google Hacking Techniques with AI
○ Advanced Image Search	○ Google Hacking Database
○ Reverse Image Search	▪ VPN Footprinting through Google Hacking Database
○ Video Search Engines	○ VPN Footprinting through Google Hacking Database with AI
○ Meta Search Engines	▪ Footprinting through SHODAN Search Engine
○ FTP Search Engines	▪ Other Techniques for Footprinting through Search Engines
○ IoT Search Engines	**Footprinting through Internet Research Services**
Footprinting through Web Services	▪ Finding a Company's Top-Level Domains (TLDs) and Sub-domains
▪ Finding a Company's Top-Level Domains (TLDs) and Sub-domains	○ Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI
▪ Finding the Geographical Location of the Target	▪ Extracting Website Information from https://archive.org
▪ People Search on Social Networking Sites and People Search Services	▪ Footprinting through People Search Services
▪ Gathering Information from LinkedIn	▪ Footprinting through Job Sites
▪ Harvesting Email Lists	▪ Dark Web Footprinting
▪ Footprinting through Job Sites	○ Searching the Dark Web with Advanced Search Parameters
▪ Deep and Dark Web Footprinting	▪ Determining the Operating System
▪ Determining the Operating System	▪ Competitive Intelligence Gathering
▪ VoIP and VPN Footprinting through SHODAN	○ Competitive Intelligence - When Did this Company Begin? How Did it Develop?
▪ Competitive Intelligence Gathering	○ Competitive Intelligence - What Are the Company's Plans?
▪ Other Techniques for Footprinting through Web Services	○ Competitive Intelligence - What Expert Opinions Say About the Company?
○ Finding the Geographical Location of the Target	▪ Other Techniques for Footprinting through Internet Research Services
○ Gathering Information from Financial Services	**Footprinting through Social Networking Sites**

○ Gathering Information from Business Profile Sites	▪ People Search on Social Networking Sites
○ Monitoring Targets Using Alerts	▪ Gathering Information from LinkedIn
○ Tracking the Online Reputation of the Target	▪ Harvesting Email Lists
○ Gathering Information from Groups, Forums, and Blogs	○ Harvesting Email Lists with AI
○ Gathering Information from NNTP Usenet Newsgroups	▪ Analyzing Target Social Media Presence
○ Gathering Information from Public Source-Code Repositories	○ Tools for Footprinting through Social Networking Sites
Footprinting through Social Networking Sites	○ Footprinting through Social Networking Sites with AI
▪ Collecting Information through Social Engineering on Social Networking Sites	**Whois Footprinting**
▪ General Resources for Locating Information from Social Media Sites	▪ Whois Lookup
▪ Conducting Location Search on Social Media Sites	▪ Finding IP Geolocation Information
▪ Constructing and Analyzing Social Network Graphs	**DNS Footprinting**
▪ Tools for Footprinting through Social Networking Sites	▪ Extracting DNS Information
Website Footprinting	▪ DNS Lookup with AI
▪ Website Footprinting	▪ Reverse DNS Lookup
▪ Website Footprinting using Web Spiders	**Network and Email Footprinting**
▪ Mirroring Entire Website	▪ Locate the Network Range
▪ Extracting Website Information from https://archive.org	▪ Traceroute
▪ Other Techniques for Website Footprinting	○ Traceroute with AI
○ Extracting Website Links	○ Traceroute Analysis
○ Gathering the Wordlist from the Target Website	○ Traceroute Tools
○ Extracting Metadata of Public Documents	▪ Tracking Email Communications
○ Monitoring Web Pages for Updates and Changes	○ Collecting Information from Email Header
○ Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website	○ Email Tracking Tools
○ Searching for Web Pages Posting Patterns and Revision Numbers	**Footprinting through Social Engineering**
○ Monitoring Website Traffic of the Target Company	▪ Collecting Information through Social Engineering on Social Networking Sites
Email Footprinting	▪ Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

▪ Tracking Email Communications	**Footprinting Tasks using Advanced Tools and AI**
▪ Email Tracking Tools	▪ AI-Powered OSINT Tools
Whois Footprinting	▪ Create and Run Custom Python Script to Automate Footprinting Tasks with AI
▪ Whois Lookup	**Footprinting Countermeasures**
▪ Finding IP Geolocation Information	
DNS Footprinting	
▪ Extracting DNS Information	
▪ Reverse DNS Lookup	
Network Footprinting	
▪ Locate the Network Range	
▪ Traceroute	
▪ Traceroute Analysis	
▪ Traceroute Tools	
Footprinting through Social Engineering	
▪ Footprinting through Social Engineering	
▪ Collect Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation	
Footprinting Tools	
▪ Footprinting Tools: Maltego and Recon-ng	
▪ Footprinting Tools: FOCA and OSRFramework	
▪ Footprinting Tools: OSINT Framework	
▪ Footprinting Tools: Recon-Dog and BillCipher	
▪ Footprinting Tools: Spyse	
Footprinting Countermeasures	
▪ Footprinting Countermeasures	
Module 03: Scanning Networks	**Module 03: Scanning Networks**
Network Scanning Concepts	**Network Scanning Concepts**
▪ Overview of Network Scanning	▪ Overview of Network Scanning
▪ TCP Communication Flags	▪ TCP Communication Flags
▪ TCP/IP Communication	▪ TCP/IP Communication
Scanning Tools	**Scanning Tools**
▪ Scanning Tools: Nmap	**Host Discovery**
▪ Scanning Tools: Hping3	▪ Host Discovery Techniques
○ Hping Commands	○ ARP Ping Scan
▪ Scanning Tools	○ UDP Ping Scan
~~▪ Scanning Tools for Mobile~~	○ ICMP ECHO Ping Scan

Host Discovery	○ ICMP ECHO Ping Sweep
▪ Host Discovery Techniques	○ ICMP Timestamp Ping Scan
○ ARP Ping Scan	○ ICMP Address Mask Ping Scan
○ UDP Ping Scan	○ TCP SYN Ping Scan
○ ICMP ECHO Ping Scan	○ TCP ACK Ping Scan
○ ICMP ECHO Ping Sweep	○ IP Protocol Ping Scan
○ ICMP Timestamp Ping Scan	○ Host Discovery with AI
○ ICMP Address Mask Ping Scan	○ Ping Sweep Tools
○ TCP SYN Ping Scan	**Port and Service Discovery**
○ TCP ACK Ping Scan	▪ Port Scanning Techniques
○ IP Protocol Ping Scan	▪ TCP Connect/Full-Open Scan
○ Ping Sweep Tools	○ Stealth Scan (Half-Open Scan)
Port and Service Discovery	○ Inverse TCP Flag Scan
▪ Port Scanning Techniques	○ Xmas Scan
○ TCP Scanning	○ TCP Maimon Scan
• TCP Connect/Full Open Scan	○ ACK Flag Probe Scan
• Stealth Scan (Half-open Scan)	○ IDLE/IPID Header Scan
• Inverse TCP Flag Scan	○ UDP Scan
✓ Xmas Scan	○ SCTP INIT Scan
✓ FIN Scan	○ SCTP COOKIE ECHO Scan
✓ NULL Scan	○ SSDP and List Scan
✓ TCP Maimon Scan	○ IPv6 Scan
• ACK Flag Probe Scan	○ Port Scanning with AI
✓ TTL-Based Scan	○ Service Version Discovery
✓ Window-Based Scan	○ Service Version Discovery with AI
• IDLE/IPID Header Scan	○ Nmap Scan Time Reduction Techniques
○ UDP Scan	**OS Discovery (Banner Grabbing/OS Fingerprinting)**
○ SCTP INIT Scan	▪ OS Discovery/Banner Grabbing
○ SCTP COOKIE ECHO Scan	▪ How to Identify Target System OS
○ SSDP and List Scan	○ OS Discovery using Nmap and Unicornscan
○ IPv6 Scan	○ OS Discovery using Nmap Script Engine
▪ Service Version Discovery	○ OS Discovery using IPv6 Fingerprinting
▪ Nmap Scan Time Reduction Techniques	○ OS Discovery with AI
OS Discovery (Banner Grabbing/OS Fingerprinting)	▪ Create and Run Custom Script to Automate Network Scanning Tasks With AI
▪ OS Discovery/Banner Grabbing	**Scanning Beyond IDS and Firewall**
▪ How to Identify Target System OS	▪ Packet Fragmentation
○ OS Discovery using Wireshark	▪ Source Routing

○ OS Discovery using Nmap and Unicornscan	Source Port Manipulation
○ OS Discovery using Nmap Script Engine	▪ IP Address Decoy
○ OS Discovery using IPv6 Fingerprinting	▪ IP Address Spoofing
Scanning Beyond IDS and Firewall	▪ MAC Address Spoofing
▪ IDS/Firewall Evasion Techniques	▪ Creating Custom Packets
○ Packet Fragmentation	▪ Randomizing Host Order and Sending Bad Checksums
○ Source Routing	▪ Proxy Servers
○ Source Port Manipulation	○ Proxy Chaining
○ IP Address Decoy	○ Proxy Tools
○ IP Address Spoofing	▪ Anonymizers
○ MAC Address Spoofing	○ Censorship Circumvention Tools
○ Creating Custom Packets	**Network Scanning Countermeasures**
○ Randomizing Host Order and Sending Bad Checksums	▪ Ping Sweep Countermeasures
○ Proxy Servers	▪ Port Scanning Countermeasures
• Proxy Chaining	▪ Banner Grabbing Countermeasures
• Proxy Tools	▪ IP Spoofing Detection Techniques
~~• Proxy Tools for Mobile~~	▪ IP Spoofing Countermeasures
○ Anonymizers	▪ Scanning Detection and Prevention Tools
• Censorship Circumvention Tools: Alkasir and Tails	
Network Scanning Countermeasures	
▪ Ping Sweep Countermeasures	
▪ Port Scanning Countermeasures	
▪ Banner Grabbing Countermeasures	
▪ IP Spoofing Detection Techniques	
○ Direct TTL Probes	
○ IP Identification Number	
○ TCP Flow Control Method	
▪ IP Spoofing Countermeasures	
▪ Scanning Detection and Prevention Tools	
Module 04: Enumeration	**Module 04: Enumeration**
Enumeration Concepts	**Enumeration Concepts**
▪ What is Enumeration?	▪ What is Enumeration?
▪ Techniques for Enumeration	▪ Techniques for Enumeration
▪ Services and Ports to Enumerate	▪ Services and Ports to Enumerate
NetBIOS Enumeration	**NetBIOS Enumeration**

▪ NetBIOS Enumeration	▪ NetBIOS Enumeration Tools
▪ NetBIOS Enumeration Tools	▪ Enumerating User Accounts
▪ Enumerating User Accounts	▪ Enumerating Shared Resources Using Net View
▪ Enumerating Shared Resources Using Net View	▪ NetBIOS Enumeration using AI
SNMP Enumeration	**SNMP Enumeration**
▪ SNMP (Simple Network Management Protocol) Enumeration	▪ Working of SNMP
▪ Working of SNMP	▪ Management Information Base (MIB)
▪ Management Information Base (MIB)	▪ Enumerating SNMP using SnmpWalk
▪ Enumerating SNMP using SnmpWalk	▪ Enumerating SNMP using Nmap
▪ Enumerating SNMP using Nmap	▪ SNMP Enumeration Tools
▪ SNMP Enumeration Tools	▪ SNMP Enumeration with SnmpWalk and Nmap using AI
LDAP Enumeration	**LDAP Enumeration**
▪ LDAP Enumeration	▪ Manual and Automated LDAP Enumeration
▪ Manual and Automated LDAP Enumeration	▪ LDAP Enumeration Tools
▪ LDAP Enumeration Tools	**NTP and NFS Enumeration**
NTP and NFS Enumeration	▪ NTP Enumeration
▪ NTP Enumeration	▪ NTP Enumeration Commands
▪ NTP Enumeration Commands	▪ NTP Enumeration Tools
▪ NTP Enumeration Tools	▪ NFS Enumeration
▪ NFS Enumeration	▪ NFS Enumeration Tools
▪ NFS Enumeration Tools	**SMTP and DNS Enumeration**
SMTP and DNS Enumeration	▪ SMTP Enumeration
▪ SMTP Enumeration	▪ SMTP Enumeration using Nmap
▪ SMTP Enumeration using Nmap	▪ SMTP Enumeration using Metasploit
▪ SMTP Enumeration using Metasploit	▪ SMTP Enumeration Tools
▪ SMTP Enumeration Tools	▪ SMTP Enumeration using AI
▪ DNS Enumeration Using Zone Transfer	▪ DNS Enumeration Using Zone Transfer
▪ DNS Cache Snooping	▪ DNS Cache Snooping
▪ DNSSEC Zone Walking	▪ DNSSEC Zone Walking
▪ DNS and DNSSEC Enumeration using Nmap	▪ DNS Enumeration Using OWASP Amass
Other Enumeration Techniques	▪ DNS and DNSSEC Enumeration Using Nmap
▪ IPsec Enumeration	▪ DNS Enumeration with Nmap Using AI
▪ VoIP Enumeration	▪ DNS Cache Snooping using AI
▪ RPC Enumeration	**Other Enumeration Techniques**
▪ Unix/Linux User Enumeration	▪ IPsec Enumeration
▪ ~~Telnet~~ and SMB Enumeration	▪ IPsec Enumeration with AI
~~▪ FTP and TFTP Enumeration~~	▪ VoIP Enumeration

~~▪ IPv6 Enumeration~~	▪ RPC Enumeration
~~▪ BGP Enumeration~~	▪ Unix/Linux User Enumeration
Enumeration Countermeasures	▪ SMB Enumeration
▪ Enumeration Countermeasures	▪ SMB Enumeration with AI
▪ DNS Enumeration Countermeasures	▪ Create and Run Custom Script to Automate Network Enumeration Tasks with AI
	Enumeration Countermeasures
Module 05: Vulnerability Analysis	**Module 05: Vulnerability Analysis**
Vulnerability Assessment Concepts	**Vulnerability Assessment Concepts**
▪ What is Vulnerability?	▪ Vulnerability Classification
~~o Examples of Vulnerabilities~~	o Misconfigurations/Weak Configurations
▪ Vulnerability Research	o Application Flaws
▪ Resources for Vulnerability Research	o Poor Patch Management
▪ What is Vulnerability Assessment?	o Design Flaws
▪ Vulnerability Scoring Systems and Databases	o Third-Party Risks
▪ Vulnerability-Management Life Cycle	o Default Installations/Default Configurations
o Pre-Assessment Phase	o Operating System Flaws
o Vulnerability Assessment Phase	o Default Passwords
o Post Assessment Phase	o Zero-Day Vulnerabilities
Vulnerability Classification and Assessment Types	o Legacy Platform Vulnerabilities
▪ Vulnerability Classification	o System Sprawl/Undocumented Assets
o Misconfigurations/Weak Configurations	o Improper Certificate and Key Management
o Application Flaws	▪ Vulnerability Scoring Systems and Databases
o Poor Patch Management	o Common Vulnerability Scoring System (CVSS)
o Design Flaws	o Common Vulnerabilities and Exposures (CVE)
o Third-Party Risks	o National Vulnerability Database (NVD)
o Default Installations/Default Configurations	o Common Weakness Enumeration (CWE)
o Operating System Flaws	▪ Vulnerability-Management Life Cycle
o Default Passwords	o Pre-Assessment Phase
o Zero-Day Vulnerabilities	o Vulnerability Assessment Phase
o Legacy Platform Vulnerabilities	o Post Assessment Phase
o System Sprawl/Undocumented Assets	▪ Vulnerability Research
o Improper Certificate and Key Management	o Resources for Vulnerability Research
▪ Types of Vulnerability Assessment	▪ Vulnerability Scanning and Analysis
Vulnerability Assessment Tools	o Types of Vulnerability Scanning
▪ Comparing Approaches to Vulnerability Assessment	**Vulnerability Assessment Tools**
▪ Characteristics of a Good Vulnerability Assessment	▪ Comparing Approaches to Vulnerability

Solution	Assessment
▪ Working of Vulnerability Scanning Solutions	▪ Characteristics of a Good Vulnerability Assessment Solution
▪ Types of Vulnerability Assessment Tools	▪ Working of Vulnerability Scanning Solutions
▪ Choosing a Vulnerability Assessment Tool	▪ Types of Vulnerability Assessment Tools
▪ Criteria for Choosing a Vulnerability Assessment Tool	▪ Choosing a Vulnerability Assessment Tool
▪ Best Practices for Selecting Vulnerability Assessment Tools	▪ Criteria for Choosing a Vulnerability Assessment Tool
▪ Vulnerability Assessment Tools: Qualys Vulnerability Management	▪ Best Practices for Selecting Vulnerability Assessment Tools
▪ Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard	▪ Vulnerability Assessment Tools
▪ Vulnerability Assessment Tools: OpenVAS and Nikto	○ Nessus Essentials
▪ Other Vulnerability Assessment Tools	○ GFI LanGuard
~~▪ Vulnerability Assessment Tools for Mobile~~	○ OpenVAS
Vulnerability Assessment Reports	○ Nikto
▪ Vulnerability Assessment Reports	○ Qualys Vulnerability Management
▪ Components of a Vulnerability Assessment Report	▪ 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 06: System Hacking	**Module 06: System Hacking**
Gaining Access	**Gaining Access**
▪ Cracking Passwords	▪ Cracking Passwords
○ Microsoft Authentication	○ Microsoft Authentication
○ How Hash Passwords Are Stored in Windows SAM?	○ How Hash Passwords Are Stored in Windows SAM?
○ NTLM Authentication Process	○ Tools to Extract the Password Hashes
○ Kerberos Authentication	○ NTLM Authentication Process
○ Password Cracking	○ Kerberos Authentication
○ Types of Password Attacks	○ Password Cracking
• Non-Electronic Attacks	○ Types of Password Attacks
• Active Online Attacks	• Non-Electronic Attacks

✓ Dictionary, Brute-Force, and Rule-based Attack	• Active Online Attacks
✓ Password Spraying Attack and Mask Attack	✓ Other Active Online Attacks
✓ Password Guessing	• Passive Online Attacks
✓ Default Passwords	• Offline Attacks
✓ Trojans/Spyware/Keyloggers	○ Password Recovery Tools
✓ Hash Injection/Pass-the-Hash (PtH) Attack	○ Password-Cracking Tools
✓ LLMNR/NBT-NS Poisoning	○ Password Salting
✓ Internal Monologue Attack	○ How to Defend against Password Cracking
✓ Cracking Kerberos Password	○ How to Defend against LLMNR/NBT-NS Poisoning
✓ Pass the Ticket Attack	○ Tools to Detect LLMNR/NBT-NS Poisoning
✓ Other Active Online Attacks	○ Detecting SMB Attacks against Windows
➢ GPU-based Attack	▪ Vulnerability Exploitation
• Passive Online Attacks	○ Exploit Sites
✓ Wire Sniffing	○ Windows Exploit Suggester - Next Generation (WES-NG)
✓ Man-in-the-Middle/Manipulator-in-the-Middle and Replay Attacks	○ Metasploit Framework
• Offline Attacks	○ Metasploit Modules
✓ Rainbow Table Attack	○ AI-Powered Vulnerability Exploitation Tools
✓ Distributed Network Attack	○ Buffer Overflow
○ Password Recovery Tools	• Types of Buffer Overflow
○ Tools to Extract the Password Hashes	• Simple Buffer Overflow in C
~~○ Password Cracking using Domain Password Audit Tool (DPAT)~~	• Windows Buffer Overflow Exploitation
○ Password-Cracking Tools: L0phtCrack	○ Return-Oriented Programming (ROP) Attack
○ Password-Cracking Tools: ophcrack	○ Bypassing ASLR and DEP Security Mechanisms
○ Password-Cracking Tools	○ Heap Spraying
○ Password Salting	○ JIT Spraying
○ How to Defend against Password Cracking	○ Exploit Chaining
○ How to Defend against LLMNR/NBT-NS Poisoning	○ Domain Mapping and Exploitation with Bloodhound
○ Tools to Detect LLMNR/NBT-NS Poisoning	○ Post AD Enumeration using PowerView
▪ Vulnerability Exploitation	○ Identifying Insecurities Using GhostPack Seatbelt
○ Exploit Sites	○ Buffer Overflow Detection Tools
○ Buffer Overflow	○ Defending against Buffer Overflows

• Types of Buffer Overflow: Stack-Based Buffer Overflow	**Escalating Privileges**
• Types of Buffer Overflow: Heap-Based Buffer Overflow	▪ Privilege Escalation
• Simple Buffer Overflow in C	▪ Privilege Escalation Using DLL Hijacking
• Windows Buffer Overflow Exploitation	▪ Privilege Escalation by Exploiting Vulnerabilities
○ Return-Oriented Programming (ROP) Attack	▪ Privilege Escalation Using Dylib Hijacking
○ Exploit Chaining	▪ Privilege Escalation Using Spectre and Meltdown Vulnerabilities
○ Active Directory Enumeration Using PowerView	▪ Privilege Escalation Using Named Pipe Impersonation
○ Domain Mapping and Exploitation with Bloodhound	▪ Privilege Escalation by Exploiting Misconfigured Services
○ Identifying Insecurities Using GhostPack Seatbelt	▪ Pivoting and Relaying to Hack External Machines
○ Buffer Overflow Detection Tools	▪ Privilege Escalation Using Misconfigured NFS
○ Defending against Buffer Overflows	▪ Privilege Escalation by Bypassing User Account Control (UAC)
Escalating Privileges	▪ Privilege Escalation by Abusing Boot or Logon Initialization Scripts
▪ Privilege Escalation	▪ Privilege Escalation by Modifying Domain Policy
▪ Privilege Escalation Using DLL Hijacking	▪ Retrieving Password Hashes of Other Domain Controllers Using DCSync Attack
▪ Privilege Escalation by Exploiting Vulnerabilities	▪ Privilege Escalation by Abusing Active Directory Certificate Services (ADCS)
▪ Privilege Escalation Using Dylib Hijacking	▪ Other Privilege Escalation Techniques
▪ Privilege Escalation Using Spectre and Meltdown Vulnerabilities	▪ Privilege Escalation Tools
▪ Privilege Escalation Using Named Pipe Impersonation	▪ How to Defend against Privilege Escalation
▪ Privilege Escalation by Exploiting Misconfigured Services	○ Tools for Defending against DLL and Dylib Hijacking
▪ Pivoting and Relaying to Hack External Machines	○ Defending against Spectre and Meltdown Vulnerabilities
▪ Privilege Escalation Using Misconfigured NFS	○ Tools for Detecting Spectre and Meltdown Vulnerabilities
▪ Privilege Escalation Using Windows Sticky Keys	**Maintaining Access**
▪ Privilege Escalation by Bypassing User Account Control (UAC)	▪ Executing Applications
▪ Privilege Escalation by Abusing Boot or Logon Initialization Scripts	○ Remote Code Execution Techniques
▪ Privilege Escalation by Modifying Domain Policy	• Tools for Executing Applications
▪ Retrieving Password Hashes of Other Domain	○ Keylogger

Controllers Using DCSync Attack	
▪ Other Privilege Escalation Techniques	• Types of Keystroke Loggers
○ Parent PID Spoofing	• Remote Keylogger Attack Using Metasploit
○ Abusing Accessibility Features	• Hardware Keyloggers
○ SID-History Injection	• Keyloggers for Windows
○ COM Hijacking	• Keyloggers for macOS
○ Scheduled Tasks in Linux	○ Spyware
▪ Privilege Escalation Tools	• Spyware Tools
○ FullPowers	• Types of Spyware
○ PEASS-ng	○ How to Defend against Keyloggers
▪ How to Defend Against Privilege Escalation	○ Anti-Keyloggers
○ Tools for Defending against DLL and Dylib Hijacking	○ How to Defend against Spyware
○ Defending against Spectre and Meltdown Vulnerabilities	○ Anti-Spyware
○ Tools for Detecting Spectre and Meltdown Vulnerabilities	▪ Hiding Files
Maintaining Access	○ Rootkits
▪ Executing Applications	• Types of Rootkits
○ Remote Code Execution Techniques	• How a Rootkit Works
• Tools for Executing Applications	• Popular Rootkits
○ Keylogger	• Detecting Rootkits
• Types of Keystroke Loggers	• Steps for Detecting Rootkits
• Remote Keylogger Attack Using Metasploit	• How to Defend against Rootkits
• Hardware Keyloggers	• Anti-Rootkits
• Keyloggers for Windows	○ NTFS Data Stream
• Keyloggers for macOS	• How to Create NTFS Streams
○ Spyware	• NTFS Stream Manipulation
• Spyware Tools: Spytech SpyAgent and Power Spy	• How to Defend against NTFS Streams
• Spyware Tools	• NTFS Stream Detectors
○ How to Defend Against Keyloggers	○ What is Steganography?
• Anti-Keyloggers	• Classification of Steganography
○ How to Defend Against Spyware	• Types of Steganography based on Cover Medium
• Anti-Spyware	• Whitespace Steganography
▪ Hiding Files	• Image Steganography
○ Rootkits	• Document Steganography
• Types of Rootkits	• Video Steganography

• How a Rootkit Works	• Audio Steganography
• Popular Rootkits	• Folder Steganography
✓ Purple Fox Rootkit	• Spam/Email Steganography
✓ MoonBounce	• Other Types of Steganography
✓ Dubbed Demodex Rootkit	• Steganalysis
• Detecting Rootkits	• Steganalysis Methods/Attacks on Steganography
• Steps for Detecting Rootkits	○ Detecting Steganography (Text, Image, Audio, and Video Files)
• How to Defend against Rootkits	○ Steganography Detection Tools
• Anti-Rootkits	▪ Establishing Persistence
○ NTFS Data Stream	○ Maintaining Persistence Using Windows Sticky Keys
• How to Create NTFS Streams	○ Maintaining Persistence by Abusing Boot or Logon Autostart Executions
• NTFS Stream Manipulation	○ Domain Dominance Through Different Paths
• How to Defend against NTFS Streams	• Remote Code Execution
• NTFS Stream Detectors	• Abusing Data Protection API (DPAPI)
○ What is Steganography?	• Malicious Replication
• Classification of Steganography	• Skeleton Key Attack
• Types of Steganography based on Cover Medium	• Golden Ticket Attack
✓ Whitespace Steganography	• Silver Ticket Attack
✓ Image Steganography	○ Maintain Domain Persistence Through AdminSDHolder
➢ Image Steganography Tools	○ Maintaining Persistence Through WMI Event Subscription
✓ Document Steganography	○ Overpass-the-Hash Attack
✓ Video Steganography	○ Linux Post-Exploitation
✓ Audio Steganography	○ Windows Post-Exploitation
✓ Folder Steganography	○ How to Defend against Persistence Attacks
✓ Spam/Email Steganography	**Clearing Logs**
✓ Other Types of Steganography	▪ Covering Tracks
~~• Steganography Tools for Mobile Phones~~	▪ Disabling Auditing: Auditpol
• Steganalysis	▪ Clearing Logs
• Steganalysis Methods/Attacks on Steganography	▪ Manually Clearing Event Logs
• Detecting Steganography (Text, Image, Audio, and Video Files)	▪ Ways to Clear Online Tracks
• Steganography Detection Tools	▪ Covering BASH Shell Tracks

▪ Establishing Persistence	▪ Covering Tracks on a Network
○ Maintaining Persistence by Abusing Boot or Logon Autostart Executions	▪ Covering Tracks on an OS
○ Domain Dominance through Different Paths	▪ Delete Files using Cipher.exe
• Remote Code Execution	▪ Disable Windows Functionality
• Abusing DPAPI	▪ Deleting Windows Activity History
• Malicious Replication	▪ Deleting Incognito History
• Skeleton Key Attack	▪ Hiding Artifacts in Windows, Linux, and macOS
• Golden Ticket Attack	▪ Anti-forensics Techniques
• Silver Ticket Attack	▪ Track-Covering Tools
○ Maintain Domain Persistence Through AdminSDHolder	▪ Defending against Covering Tracks
○ Maintaining Persistence Through WMI Event Subscription	
○ Overpass-the-Hash Attack	
○ Linux Post Exploitation	
○ Windows Post Exploitation	
○ How to Defend against Persistence Attacks	
Clearing Logs	
▪ Covering Tracks	
▪ Disabling Auditing: Auditpol	
▪ Clearing Logs	
▪ Manually Clearing Event Logs	
▪ Ways to Clear Online Tracks	
▪ Covering BASH Shell Tracks	
▪ Covering Tracks on a Network	
▪ Covering Tracks on an OS	
▪ Delete Files using Cipher.exe	
▪ Disable Windows Functionality	
▪ Hiding Artifacts in Windows, Linux, and macOS	
▪ Track-Covering Tools	
▪ Defending against Covering Tracks	
Module 07: Malware Threats	**Module 07: Malware Threats**
Malware Concepts	**Malware Concepts**
▪ Introduction to Malware	▪ Introduction to Malware
▪ Different Ways for Malware to Enter a System	○ Different Ways for Malware to Enter a System
▪ Common Techniques Attackers Use to Distribute Malware on the Web	○ Common Techniques Attackers Use to Distribute Malware on the Web

○ RTF Injection	▪ Components of Malware
▪ Components of Malware	▪ Potentially Unwanted Application or Applications (PUAs)
▪ Potentially Unwanted Application or Applications (PUAs)	○ Adware
○ Adware	**APT Concepts**
APT Concepts	▪ What are Advanced Persistent Threats?
▪ What are Advanced Persistent Threats?	○ Characteristics of Advanced Persistent Threats
▪ Characteristics of Advanced Persistent Threats	○ Advanced Persistent Threat Lifecycle
▪ Advanced Persistent Threat Lifecycle	**Trojan Concepts**
Trojan Concepts	▪ What is a Trojan?
▪ What is a Trojan?	▪ How Hackers Use Trojans
▪ How Hackers Use Trojans	▪ Common Ports used by Trojans
▪ Common Ports used by Trojans	▪ Types of Trojans
▪ Types of Trojans	○ Remote Access Trojans
○ Remote Access Trojans	○ Backdoor Trojans
○ Backdoor Trojans	○ Botnet Trojans
○ Botnet Trojans	○ Rootkit Trojans
○ Rootkit Trojans	○ E-banking Trojans
○ E-banking Trojans	• Working of E-banking Trojans
• Working of E-banking Trojans	• E-banking Trojan: CHAVECLOAK
• E-banking Trojan: Dreambot	○ Point-of-Sale Trojans
○ Point-of-Sale Trojans	○ Defacement Trojans
○ Defacement Trojans	○ Service Protocol Trojans
○ Service Protocol Trojans	○ Mobile Trojans
○ Mobile Trojans	○ IoT Trojans
○ IoT Trojans	○ Security Software Disabler Trojans
○ Security Software Disabler Trojans	○ Destructive Trojans
○ Destructive Trojans	○ DDoS Trojans
○ DDoS Trojans	○ Command Shell Trojans
○ Command Shell Trojans	▪ How to Infect Systems Using a Trojan
▪ How to Infect Systems Using a Trojan	○ Creating a Trojan
○ Creating a Trojan	○ Employing a Dropper or Downloader
○ Employing a Dropper or Downloader	○ Employing a Wrapper
○ Employing a Wrapper	○ Employing a Crypter
○ Employing a Crypter	○ Propagating and Deploying a Trojan
○ Propagating and Deploying a Trojan	○ Deploy a Trojan through Emails
○ Exploit Kits	○ Deploy a Trojan through Covert Channels
Virus and Worm Concepts	○ Deploy a Trojan through Proxy Servers

▪ Introduction to Viruses	○ Deploy a Trojan through USB/Flash Drives
▪ Stages of Virus Lifecycle	○ Techniques for Evading Antivirus Software
▪ Working of Viruses	○ Exploit Kits
○ How does a Computer Get Infected by Viruses?	**Virus and Worm Concepts**
▪ Types of Viruses	▪ Introduction to Viruses
○ System or Boot Sector Viruses	○ Stages of Virus Lifecycle
○ File Viruses	○ Working of Viruses
○ Multipartite Viruses	▪ How does a Computer Get Infected by Viruses?
○ Macro Viruses	▪ Types of Viruses
○ Cluster Viruses	○ System or Boot Sector Viruses
○ Stealth Viruses/Tunneling Viruses	○ File Viruses
○ Encryption Viruses	○ Multipartite Viruses
○ Sparse Infector Viruses	○ Macro Viruses
○ Polymorphic Viruses	○ Cluster Viruses
○ Metamorphic Viruses	○ Stealth Viruses/Tunneling Viruses
○ Overwriting File or Cavity Viruses	○ Encryption Viruses
○ Companion/Camouflage Viruses	○ Sparse Infector Viruses
○ Shell Viruses	○ Polymorphic Viruses
○ File Extension Viruses	○ Metamorphic Viruses
○ FAT Viruses	○ Overwriting File or Cavity Viruses
○ Logic Bomb Viruses	○ Companion/Camouflage Viruses
○ Web Scripting Virus	○ Shell Viruses
○ E-mail Viruses	○ File Extension Viruses
○ Armored Viruses	○ FAT Viruses
○ Add-on Viruses	○ Logic Bomb Viruses
○ Intrusive Viruses	○ Web Scripting Viruses
○ Direct Action or Transient Viruses	○ E-mail Viruses
○ Terminate and Stay Resident (TSR) Viruses	○ Armored Viruses
○ Ransomware	○ Add-on Viruses
• BlackCat	○ Intrusive Viruses
• BlackMatter	○ Direct Action or Transient Viruses
▪ How to Infect Systems Using a Virus: Creating a Virus	○ Terminate and Stay Resident (TSR) Viruses
▪ How to Infect Systems Using a Virus: Propagating and Deploying a Virus	▪ How to Infect Systems Using a Virus
▪ Computer Worms	○ Propagating and Deploying a Virus
○ Worm Makers	○ Virus Hoaxes
Fileless Malware Concepts	○ Fake AntiVirus
▪ What is Fileless Malware?	▪ Ransomware

▪ Taxonomy of Fileless Malware Threats	○ How to Infect Systems Using a Ransomware: Creating Ransomware
▪ How does Fileless Malware Work?	▪ Computer Worms
▪ Launching Fileless Malware through Document Exploits and In-Memory Exploits	○ How to Infect Systems Using a Worm
▪ Launching Fileless Malware through Script-based Injection	○ Worm Makers
▪ Launching Fileless Malware by Exploiting System Admin Tools	**Fileless Malware Concepts**
▪ Launching Fileless Malware through Phishing	▪ What is Fileless Malware?
▪ Maintaining Persistence with Fileless Techniques	○ Taxonomy of Fileless Malware Threats
▪ Fileless Malware	▪ How does Fileless Malware Work?
○ LemonDuck	▪ Launching Fileless Malware through Document Exploits
▪ Fileless Malware Obfuscation Techniques to Bypass Antivirus	▪ Launching Fileless Malware through In-Memory Exploits
Malware Analysis	▪ Launching Fileless Malware through Script-based Injection
▪ What is Sheep Dip Computer?	▪ Launching Fileless Malware by Exploiting System Admin Tools
▪ Antivirus Sensor Systems	▪ Launching Fileless Malware through Phishing
▪ Introduction to Malware Analysis	▪ Launching Fileless Malware through Windows Registry
▪ Malware Analysis Procedure: Preparing Testbed	▪ Maintaining Persistence with Fileless Techniques
▪ Static Malware Analysis	▪ Fileless Malware
○ File Fingerprinting	▪ Fileless Malware Obfuscation Techniques to Bypass Antivirus
○ Local and Online Malware Scanning	**AI-based Malware Concepts**
○ Performing Strings Search	▪ What is AI-based Malware?
○ Identifying Packing/Obfuscation Methods	○ Working of AI-based Malware
• Identifying Packing/Obfuscation Method of ELF Malware	▪ Indicators of AI-based Malware
• Detect It Easy (DIE)	▪ Challenges of AI-based Malware
○ Finding the Portable Executables (PE) Information	▪ Techniques Used in AI-based Malware Development
○ Identifying File Dependencies	○ Generative Adversarial Networks (GANs)
○ Malware Disassembly	○ Reinforcement Learning
• Ghidra	○ Natural Language Processing (NLP)
• x64dbg	▪ Examples of AI-based Malware
○ Analyzing ELF Executable Files	○ AI-Generated Videos: Malware Spread Through YouTube
○ Analyzing Mach Object (Mach-O) Executable	**Malware Analysis**

Files	
○ Analyzing Malicious MS Office Documents	▪ What is Sheep Dip Computer?
• Finding Suspicious Components	▪ Antivirus Sensor Systems
• Finding Macro Streams	▪ Introduction to Malware Analysis
• Dumping Macro Streams	▪ Malware Analysis Procedure
• Identifying Suspicious VBA Keywords	▪ Preparing Testbed
▪ Dynamic Malware Analysis	▪ Static Malware Analysis
○ Port Monitoring	○ File Fingerprinting
○ Process Monitoring	○ Local and Online Malware Scanning
○ Registry Monitoring	○ Performing Strings Search
○ Windows Services Monitoring	○ Identifying Packing/Obfuscation Methods
○ Startup Programs Monitoring	○ Finding the Portable Executables (PE) Information
○ Event Logs Monitoring/Analysis	○ Identifying File Dependencies
○ Installation Monitoring	○ Malware Disassembly
○ Files and Folders Monitoring	○ Analyzing ELF Executable Files
○ Device Drivers Monitoring	○ Analyzing Mach Object (Mach-O) Executable Files
○ Network Traffic Monitoring/Analysis	○ Analyzing Malicious MS Office Documents
○ DNS Monitoring/Resolution	○ Analyzing Suspicious PDF Document
○ API Calls Monitoring	○ Analyzing Suspicious Documents Using YARA
○ System Calls Monitoring	▪ Dynamic Malware Analysis
▪ Virus Detection Methods	○ Port Monitoring
▪ Trojan Analysis: ~~ElectroRAT~~	○ Process Monitoring
~~○ ElectroRAT Malware Attack Phases~~	○ Registry Monitoring
~~• Initial propagation and Infection~~	○ Windows Services Monitoring
~~• Deploying Malware~~	○ Startup Programs Monitoring
~~• Exploitation~~	○ Event Logs Monitoring/Analysis
~~• Maintaining Persistence~~	○ Installation Monitoring
▪ Virus Analysis: ~~REvil Ransomware~~	○ Files and Folders Monitoring
~~○ REvil Ransomware Attack Stages~~	○ Device Drivers Monitoring
~~• Initial Access~~	○ Network Traffic Monitoring/Analysis
~~• Download and Execution~~	○ DNS Monitoring/Resolution
~~• Exploitation~~	○ API Calls Monitoring
~~• Lateral Movement / Defense Evasion and Discovery~~	○ System Calls Monitoring
~~• Credential Access and Exfiltration / Command and Control~~	○ Scheduled Tasks Monitoring
▪ Fileless Malware Analysis: ~~SockDetour~~	○ Browser Activity Monitoring

~~○ SockDetour Fileless Malware Attack Stages~~	▪ Virus Detection Methods
~~● Pre-exploitation~~	▪ Malware Code Emulation
~~● Initial infection~~	▪ Malware Code Instrumentation
~~● Exploitation~~	▪ Trojan Analysis: Coyote
~~● Post-exploitation~~	○ Coyote Malware Attack Phases
~~● Client Authentication and C2 Communication After Exploitation~~	▪ Virus Analysis: GhostLocker 2.0
~~● Plugin Loading Feature~~	○ GhostLocker 2.0 Malware Attack Phases
Malware Countermeasures	▪ Fileless Malware Analysis: PyLoose
▪ Trojan Countermeasures	○ PyLoose Malware Attack Phases
▪ Backdoor Countermeasures	▪ AI-based Malware Analysis: FakeGPT
▪ Virus and Worm Countermeasures	○ FakeGPT Malware Attack Phases
▪ Fileless Malware Countermeasures	**Malware Countermeasures**
Anti-Malware Software	▪ Trojan Countermeasures
▪ Anti-Trojan Software	▪ Backdoor Countermeasures
▪ Antivirus Software	▪ Virus and Worm Countermeasures
▪ Fileless Malware Detection Tools	▪ Fileless Malware Countermeasures
▪ Fileless Malware Protection Tools	▪ 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 08: Sniffing	**Module 08: Sniffing**
Sniffing Concepts	**Sniffing Concepts**
▪ Network Sniffing	▪ Network Sniffing
▪ Types of Sniffing	▪ How a Sniffer Works
▪ How an Attacker Hacks the Network Using Sniffers	▪ Types of Sniffing
▪ Protocols Vulnerable to Sniffing	○ Passive Sniffing
▪ Sniffing in the Data Link Layer of the OSI Model	○ Active Sniffing
▪ Hardware Protocol Analyzers	▪ How an Attacker Hacks the Network Using Sniffers
▪ SPAN Port	▪ Protocols Vulnerable to Sniffing
▪ Wiretapping	▪ Sniffing in the Data Link Layer of the OSI Model

▪ Lawful Interception	▪ Hardware Protocol Analyzers
Sniffing Technique: MAC Attacks	▪ SPAN Port
▪ MAC Address/CAM Table	▪ Wiretapping
▪ How CAM Works	▪ Lawful Interception
▪ What Happens When a CAM Table Is Full?	**Sniffing Technique: MAC Attacks**
▪ MAC Flooding	▪ MAC Address
▪ Switch Port Stealing	▪ CAM Table
▪ How to Defend against MAC Attacks	▪ How CAM Works
Sniffing Technique: DHCP Attacks	▪ What Happens when a CAM Table is Full?
▪ How DHCP Works	▪ MAC Flooding
▪ DHCP Request/Reply Messages	▪ Switch Port Stealing
▪ DHCP Starvation Attack	▪ How to Defend against MAC Attacks
▪ Rogue DHCP Server Attack	**Sniffing Technique: DHCP Attacks**
▪ How to Defend Against DHCP Starvation and Rogue Server Attacks	▪ How DHCP Works
○ MAC Limiting Configuration on Juniper Switches	▪ DHCP Request/Reply Messages
○ Configuring DHCP Filtering on a Switch	▪ IPv4 DHCP Packet Format
Sniffing Technique: ARP Poisoning	▪ DHCP Starvation Attack
▪ What Is Address Resolution Protocol (ARP)?	▪ Rogue DHCP Server Attack
▪ ARP Spoofing Attack	▪ DHCP Attack Tools
▪ Threats of ARP Poisoning	▪ How to Defend Against DHCP Starvation and Rogue Server Attacks
▪ ARP Poisoning Tools	**Sniffing Technique: ARP Poisoning**
○ Habu	▪ What Is Address Resolution Protocol (ARP)?
▪ How to Defend Against ARP Poisoning	▪ ARP Spoofing Attack
▪ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches	▪ Threats of ARP Poisoning
▪ ARP Spoofing Detection Tools	▪ ARP Spoofing/Poisoning Tools
Sniffing Technique: Spoofing Attacks	▪ How to Defend Against ARP Poisoning
▪ MAC Spoofing/Duplicating	▪ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
▪ MAC Spoofing Technique: Windows	▪ ARP Spoofing Detection Tools
▪ MAC Spoofing Tools	**Sniffing Technique: Spoofing Attacks**
▪ IRDP Spoofing	▪ MAC Spoofing/Duplicating
▪ VLAN Hopping	▪ MAC Spoofing Technique: Windows
▪ STP Attack	▪ MAC Spoofing Tools
▪ How to Defend Against MAC Spoofing	▪ IRDP Spoofing
▪ How to Defend Against VLAN Hopping	▪ VLAN Hopping
▪ How to Defend Against STP Attacks	▪ STP Attack

Sniffing Technique: DNS Poisoning	▪ How to Defend Against MAC Spoofing
▪ DNS Poisoning Techniques	▪ How to Defend Against VLAN Hopping
○ Intranet DNS Spoofing	▪ How to Defend Against STP Attacks
○ Internet DNS Spoofing	**Sniffing Technique: DNS Poisoning**
○ Proxy Server DNS Poisoning	▪ DNS Poisoning Techniques
○ DNS Cache Poisoning	○ Intranet DNS Spoofing
• SAD DNS Attack	○ Internet DNS Spoofing
▪ DNS Poisoning Tools	○ Proxy Server DNS Poisoning
▪ How to Defend Against DNS Spoofing	○ DNS Cache Poisoning
Sniffing Tools	▪ DNS Poisoning Tools
▪ Sniffing Tool: Wireshark	▪ How to Defend Against DNS Spoofing
○ Follow TCP Stream in Wireshark	**Sniffing Tools**
○ Display Filters in Wireshark	▪ Wireshark
○ Additional Wireshark Filters	○ Follow TCP Stream in Wireshark
▪ Sniffing Tools	○ Display Filters in Wireshark
○ RITA (Real Intelligence Threat Analytics)	○ Additional Wireshark Filters
~~▪ Packet Sniffing Tools for Mobile Phones~~	▪ Sniffing Tools
Sniffing Countermeasures	**Sniffing Countermeasures**
▪ How to Defend Against Sniffing	▪ How to Defend Against Sniffing
▪ How to Detect Sniffing	▪ How to Detect Sniffing
▪ Sniffer Detection Techniques	▪ Sniffer Detection Techniques
○ Ping Method	▪ Promiscuous Detection Tools
○ DNS Method	
○ ARP Method	
▪ Promiscuous Detection Tools	
Module 09: Social Engineering	**Module 09: Social Engineering**
Social Engineering Concepts	**Social Engineering Concepts**
▪ What is Social Engineering?	▪ What is Social Engineering?
▪ Phases of a Social Engineering Attack	○ Common Targets of Social Engineering
Social Engineering Techniques	○ Impact of Social Engineering Attack on an Organization
▪ Types of Social Engineering	○ Behaviors Vulnerable to Attacks
▪ Human-based Social Engineering	○ Factors that Make Companies Vulnerable to Attacks
○ Impersonation	○ Why is Social Engineering Effective?
○ Impersonation (Vishing)	▪ Phases of a Social Engineering Attack
○ Eavesdropping	▪ Types of Social Engineering
○ Shoulder Surfing	**Human-based Social Engineering Techniques**

○ Dumpster Diving	▪ Impersonation
○ Reverse Social Engineering	▪ Impersonation (Vishing)
○ Piggybacking	▪ Eavesdropping
○ Tailgating	▪ Shoulder Surfing
○ Diversion Theft	▪ Dumpster Diving
○ Honey Trap	▪ Reverse Social Engineering
○ Baiting	▪ Piggybacking
○ Quid Pro Quo	▪ Tailgating
○ Elicitation	▪ Diversion Theft
▪ Computer-based Social Engineering	▪ Honey Trap
○ Phishing	▪ Baiting
• Examples of Phishing Emails	▪ Quid Pro Quo
• Types of Phishing	▪ Elicitation
✓ Spear Phishing	▪ Bait and Switching
✓ Whaling	**Computer-based Social Engineering Techniques**
✓ Pharming	▪ Phishing
✓ Spimming	○ Examples of Phishing Emails
✓ Angler Phishing	○ Types of Phishing
✓ Catfishing Attack	○ Phishing Tools
✓ Deepfake Attacks	▪ Crafting Phishing Emails with ChatGPT
○ Phishing Tools	▪ Other Techniques for Computer-based Social Engineering
▪ Mobile-based Social Engineering	▪ Perform Impersonation using AI: Create Deepfake Videos
○ Publishing Malicious Apps	▪ Perform Impersonation using AI: Voice Cloning
○ Repackaging Legitimate Apps	▪ Perform Impersonation on Social Networking Sites
○ Fake Security Applications	▪ Impersonation on Facebook
○ SMiShing (SMS Phishing)	▪ Social Networking Threats to Corporate Networks
Insider Threats	▪ Identity Theft
▪ Insider Threats/Insider Attacks	○ Types of Identity Theft
▪ Types of Insider Threats	○ Common Techniques Attackers Use to Obtain Personal Information for Identity Theft
○ Accidental Insider	○ Indications of Identity Theft
▪ Behavioral Indications of an Insider Threat	**Mobile-based Social Engineering Techniques**
Impersonation on Social Networking Sites	▪ Publishing Malicious Apps
▪ Social Engineering through Impersonation on Social Networking Sites	▪ Repackaging Legitimate Apps
▪ Impersonation on Facebook	▪ Fake Security Applications
▪ Social Networking Threats to Corporate Networks	▪ SMiShing (SMS Phishing)

Identity Theft	▪ QRLJacking
▪ Identity Theft	**Social Engineering Countermeasures**
Social Engineering Countermeasures	▪ Social Engineering Countermeasures
▪ Social Engineering Countermeasures	▪ How to Defend against Phishing Attacks?
▪ How to Defend against Phishing Attacks?	▪ Identity Theft Countermeasures
▪ Detecting Insider Threats	▪ Voice Cloning Countermeasures
▪ Insider Threats Countermeasures	▪ Deepfake Attack Countermeasures
▪ Identity Theft Countermeasures	▪ How to Detect Phishing Emails?
▪ How to Detect Phishing Emails?	▪ Anti-Phishing Toolbar
▪ Anti-Phishing Toolbar	▪ Common Social Engineering Targets and Defense Strategies
▪ Common Social Engineering Targets and Defense Strategies	▪ Audit Organization's Security for Phishing Attacks using OhPhish
▪ Social Engineering Tools	
▪ Audit Organization's Security for Phishing Attacks using OhPhish	
Module 10: Denial-of-Service	**Module 10: Denial-of-Service**
DoS/DDoS Concepts	**DoS/DDoS Concepts**
▪ What is a DoS Attack?	▪ What is a DoS Attack?
▪ What is a DDoS Attack?	▪ What is a DDoS Attack?
Botnets	○ How do DDoS Attacks Work?
▪ Organized Cyber Crime: Organizational Chart	**Botnets**
▪ Botnets	▪ Organized Cyber Crime: Organizational Chart
▪ A Typical Botnet Setup	▪ Botnets
▪ Botnet Ecosystem	▪ A Typical Botnet Setup
▪ Scanning Methods for Finding Vulnerable Machines	▪ Botnet Ecosystem
▪ How Does Malicious Code Propagate?	▪ Scanning Methods for Finding Vulnerable Machines
DoS/DDoS Attack Techniques	▪ How Does Malicious Code Propagate?
▪ Basic Categories of DoS/DDoS Attack Vectors	**DDoS Case Study**
○ Volumetric Attacks	▪ DDoS Attack
• UDP Flood Attack	▪ Hackers Advertise Links for Downloading Botnets
• ICMP Flood Attack	▪ Use of Mobile Devices as Botnets for Launching DDoS Attacks
• Ping of Death and Smurf Attacks	▪ DDoS Case Study: HTTP/2 'Rapid Reset' Attack on Google Cloud
• Pulse Wave and Zero-Day DDoS Attacks	**DoS/DDoS Attack Techniques**
○ Protocol Attacks	▪ Basic Categories of DoS/DDoS Attack Vectors

• SYN Flood Attack	▪ DoS/DDoS Attack Techniques
• Fragmentation Attack	○ UDP Flood Attack
• Spoofed Session Flood Attack	○ ICMP Flood Attack
○ Application Layer Attacks	○ Ping of Death Attack
• HTTP GET/POST and Slowloris Attacks	○ Smurf Attack
• UDP Application Layer Flood Attack	○ Pulse Wave DDoS Attack
▪ Multi-Vector Attack	○ Zero-Day DDoS Attack
▪ Peer-to-Peer Attack	○ NTP Amplification Attack
▪ Permanent Denial-of-Service Attack	○ SYN Flood Attack
▪ TCP SACK Panic	○ Fragmentation Attack
▪ Distributed Reflection Denial-of-Service (DRDoS) Attack	○ Spoofed Session Flood Attack
▪ DDoS Extortion/Ransom DDoS (RDDoS) Attack	○ HTTP GET/POST Attack
▪ DoS/DDoS Attack Tools	○ Slowloris Attack
~~▪ DoS and DDoS Attack Tools for Mobiles~~	○ UDP Application Layer Flood Attack
DDoS Case Study	○ Multi-Vector Attack
▪ DDoS Attack	○ Peer-to-Peer Attack
▪ Hackers Advertise Links for Downloading Botnets	○ Permanent Denial-of-Service Attack
▪ Use of Mobile Devices as Botnets for Launching DDoS Attacks	○ TCP SACK Panic Attack
▪ DDoS Case Study: ~~DDoS Attack on Microsoft Azure~~	○ Distributed Reflection Denial-of-Service (DRDoS) Attack
DoS/DDoS Attack Countermeasures	○ DDoS Extortion/Ransom DDoS (RDDoS) Attack
▪ Detection Techniques	▪ DoS/DDoS Attack Toolkits in the Wild
▪ DoS/DDoS Countermeasure Strategies	**DoS/DDoS Attack Countermeasures**
▪ DDoS Attack Countermeasures	▪ Detection Techniques
○ Protect Secondary Victims	▪ DoS/DDoS Countermeasure Strategies
○ Detect and Neutralize Handlers	▪ DDoS Attack Countermeasures
○ Prevent Potential Attacks	○ Protect Secondary Victims
○ Deflect Attacks	○ Detect and Neutralize Handlers
○ Mitigate Attacks	○ Prevent Potential Attacks
○ Post-Attack Forensics	○ Deflect Attacks
▪ Techniques to Defend against Botnets	○ Mitigate Attacks
▪ Additional DoS/DDoS Countermeasures	○ Post-Attack Forensics
▪ DoS/DDoS Protection at ISP Level	▪ Techniques to Defend against Botnets
▪ Enabling TCP Intercept on Cisco IOS Software	▪ Additional DoS/DDoS Countermeasures
▪ Advanced DDoS Protection Appliances	▪ DoS/DDoS Protection at ISP Level
▪ DoS/DDoS Protection Tools	▪ Enabling TCP Intercept on Cisco IOS Software
▪ DoS/DDoS Protection Services	▪ Advanced DDoS Protection Appliances

	▪ DoS/DDoS Protection Tools
	▪ DoS/DDoS Protection Services
Module 11: Session Hijacking	**Module 11: Session Hijacking**
Session Hijacking Concepts	**Session Hijacking Concepts**
▪ What is Session Hijacking?	▪ What is Session Hijacking?
▪ Why is Session Hijacking Successful?	▪ Why is Session Hijacking Successful?
▪ Session Hijacking Process	▪ Session Hijacking Process
▪ Packet Analysis of a Local Session Hijack	▪ Packet Analysis of a Local Session Hijack
▪ Types of Session Hijacking	▪ Types of Session Hijacking
▪ Session Hijacking in OSI Model	▪ Session Hijacking in OSI Model
▪ Spoofing vs. Hijacking	▪ Spoofing vs. Hijacking
Application-Level Session Hijacking	**Application-Level Session Hijacking**
▪ Application-Level Session Hijacking	▪ Compromising Session IDs Using Sniffing
▪ Compromising Session IDs using Sniffing and by Predicting Session Token	▪ Compromising Session IDs by Predicting Session Token
○ How to Predict a Session Token	○ How to Predict a Session Token
▪ Compromising Session IDs Using Man-in-the-Middle/Manipulator-in-the-Middle Attack	▪ Compromising Session IDs Using Man-in-the-Middle/Manipulator-in-the-Middle Attack
▪ 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
○ Steps to Perform Man-in-the-Browser Attack	▪ Compromising Session IDs Using Client-side Attacks
▪ 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 Script Attack	▪ Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery 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 Replay Attacks	▪ Compromising Session IDs Using Session Fixation
▪ Compromising Session IDs Using Session Fixation	▪ Session Hijacking Using Proxy Servers
▪ Session Hijacking Using Proxy Servers	▪ Session Hijacking Using CRIME Attack
▪ Session Hijacking Using CRIME Attack	▪ Session Hijacking Using Forbidden Attack
▪ Session Hijacking Using Forbidden Attack	▪ Session Hijacking Using Session Donation Attack
▪ Session Hijacking Using Session Donation Attack	**Network-Level Session Hijacking**
▪ PetitPotam Hijacking	▪ Three-way Handshake
Network-Level Session Hijacking	▪ TCP/IP Hijacking
▪ Network Level Session Hijacking	▪ IP Spoofing: Source Routed Packets
▪ TCP/IP Hijacking	▪ RST Hijacking

▪ IP Spoofing: Source Routed Packets	▪ Blind Hijacking
▪ RST Hijacking	▪ UDP Hijacking
▪ Blind and UDP Hijacking	▪ MITM Attack Using Forged ICMP and ARP Spoofing
▪ MiTM Attack Using Forged ICMP and ARP Spoofing	▪ PetitPotam Hijacking
Session Hijacking Tools	**Session Hijacking Tools**
▪ Session Hijacking Tools	**Session Hijacking Countermeasures**
○ Hetty	▪ Session Hijacking Detection Methods
~~▪ Session Hijacking Tools for Mobile Phones~~	▪ Protecting against Session Hijacking
Session Hijacking Countermeasures	▪ Web Development Guidelines to Prevent Session Hijacking
▪ Session Hijacking Detection Methods	▪ Web User Guidelines to Prevent Session Hijacking
▪ Protecting against Session Hijacking	▪ Session Hijacking Detection Tools
▪ Web Development Guidelines to Prevent Session Hijacking	▪ Approaches to Prevent Session Hijacking
▪ Web User Guidelines to Prevent Session Hijacking	▪ Approaches to Prevent MITM Attacks
▪ Session Hijacking Detection Tools	▪ IPsec
~~▪ Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions~~	▪ Session Hijacking Prevention Tools
▪ Approaches to Prevent Session Hijacking	
○ HTTP Referrer Header	
▪ Approaches to Prevent MITM Attacks	
○ DNS over HTTPS	
○ Password Manager	
○ Zero-trust Principles	
▪ IPsec	
○ IPsec Authentication and Confidentiality	
▪ Session Hijacking Prevention Tools	
Module 12: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
IDS, IPS, Firewall, and Honeypot Concepts	**IDS, IPS, and Firewall Concepts**
▪ Intrusion Detection System (IDS)	▪ Intrusion Detection System (IDS)
○ How an IDS Detects an Intrusion?	○ Intrusion Prevention System (IPS)
○ General Indications of Intrusions	○ How an IDS Detects an Intrusion?
○ Types of Intrusion Detection Systems	○ General Indications of Intrusions
○ Types of IDS Alerts	○ Types of Intrusion Detection Systems
▪ Intrusion Prevention System (IPS)	○ Types of IDS Alerts
▪ Firewall	▪ Firewall

○ Firewall Architecture	○ Firewall Architecture
○ Demilitarized Zone (DMZ)	○ Demilitarized Zone (DMZ)
○ Types of Firewalls	○ Types of Firewalls
○ Firewall Technologies	• Types of Firewalls Based on Configuration
• Packet Filtering Firewall	• Types of Firewalls Based on Working Mechanism
• Circuit-Level Gateway Firewall	○ Packet Filtering Firewall
• Application-Level Firewall	○ Circuit-Level Gateway Firewall
• Stateful Multilayer Inspection Firewall	○ Application-Level Firewall
• Application Proxy	○ Stateful Multilayer Inspection Firewall
• Network Address Translation (NAT)	○ Application Proxy
• Virtual Private Network	○ Network Address Translation (NAT)
○ Firewall Limitations	○ Virtual Private Network
▪ Honeypot	○ Next-Generation Firewalls (NGFWs)
○ Types of Honeypots	○ Firewall Limitations
IDS, IPS, Firewall, and Honeypot Solutions	**IDS, IPS, and Firewall Solutions**
▪ Intrusion Detection using YARA Rules	▪ Intrusion Detection using YARA Rules
▪ Intrusion Detection Tools	▪ Intrusion Detection Tools
○ Snort	▪ Intrusion Prevention Tools
• Snort Rules	▪ Firewalls
• Snort Rules: Rule Actions and IP Protocols	**Evading IDS/Firewalls**
• Snort Rules: The Direction Operator and IP Addresses	▪ IDS/Firewall Evasion Techniques
• Snort Rules: Port Numbers	○ IDS/Firewall Identification
• Intrusion Detection Tools	○ IP Address Spoofing
○ Intrusion Detection Tools for Mobile Devices	○ Source Routing
▪ Intrusion Prevention Tools	○ Tiny Fragments
▪ Firewalls	○ Bypass Blocked Sites Using an IP Address in Place of a URL
○ Firewalls for Mobile Devices	○ Bypass Blocked Sites Using Anonymous Website Surfing Sites
▪ Honeypot Tools	○ Bypass an IDS/Firewall Using a Proxy Server
Evading IDS	○ Bypassing an IDS/Firewall through the ICMP Tunneling Method
▪ IDS Evasion Techniques	○ Bypassing an IDS/Firewall through the ACK Tunneling method
○ Insertion Attack	○ Bypassing an IDS/Firewall through the HTTP Tunneling Method
○ Evasion	○ Bypassing Firewalls through the SSH Tunneling Method

○ Denial-of-Service Attack (DoS)	○ Bypassing Firewalls through the DNS Tunneling Method
○ Obfuscating	○ Bypassing an IDS/Firewall through External Systems
○ False Positive Generation	○ Bypassing an IDS/Firewall through MITM Attacks
○ Session Splicing	○ Bypassing an IDS/Firewall through Content
○ Unicode Evasion Technique	○ Bypassing an IDS/WAF using an XSS Attack
○ Fragmentation Attack	○ Other Techniques for Bypassing WAF
○ Overlapping Fragments	○ Bypassing an IDS/Firewall through HTML Smuggling
○ Time-To-Live Attacks	○ Evading an IDS/Firewall through Windows BITS
○ Invalid RST Packets	▪ Other Techniques for IDS Evasion
○ Urgency Flag	○ Insertion Attack
○ Polymorphic Shellcode	○ Evasion
○ ASCII Shellcode	○ Denial-of-Service Attack (DoS)
○ Application-Layer Attacks	○ Obfuscating
○ Desynchronization	○ False Positive Generation
○ Other Types of Evasion	○ Session Splicing
Evading Firewalls	○ Unicode Evasion Technique
▪ Firewall Evasion Techniques	○ Fragmentation Attack
○ Firewall Identification	○ Time-To-Live Attacks
○ IP Address Spoofing	○ Urgency Flag
○ Source Routing	○ Invalid RST Packets
○ Tiny Fragments	○ Polymorphic Shellcode
○ Bypass Blocked Sites Using an IP Address in Place of a URL	○ ASCII Shellcode
○ Bypass Blocked Sites Using Anonymous Website Surfing Sites	○ Application-Layer Attacks
○ Bypass a Firewall Using a Proxy Server	○ Desynchronization
○ Bypassing Firewalls through the ICMP Tunneling Method	○ Domain Generation Algorithms (DGA)
○ Bypassing Firewalls through the ACK Tunneling Method	○ Encryption
○ Bypassing Firewalls through the HTTP Tunneling Method	○ Flooding
• Why do I Need HTTP Tunneling?	**Evading NAC and Endpoint Security**
• HTTP Tunneling Tools	▪ NAC and Endpoint Security Evasion Techniques
○ Bypassing Firewalls through the SSH Tunneling Method	▪ Bypassing NAC using VLAN Hopping
• SSH Tunneling Tools: Bitvise and Secure	▪ Bypassing NAC using Pre-authenticated Device

Pipes	
○ Bypassing Firewalls through the DNS Tunneling Method	▪ Bypassing Endpoint Security using Ghostwriting
○ Bypassing Firewalls through External Systems	▪ Bypassing Endpoint Security using Application Whitelisting
○ Bypassing Firewalls through MITM Attacks	▪ Bypassing Endpoint Security by Dechaining Macros
○ Bypassing Firewalls through Content	▪ Bypassing Endpoint Security by Clearing Memory Hooks
○ Bypassing the WAF using an XSS Attack	▪ Bypassing Endpoint Security by Process Injection
○ Other Techniques for Bypassing WAF	▪ Bypassing the EDR using LoLBins
• Using HTTP Header Spoofing	▪ Bypassing Endpoint Security by CPL (Control Panel) Side-Loading
• Using Blacklist Detection	▪ Bypassing Endpoint Security using ChatGPT
• Using Fuzzing/Bruteforcing	▪ Bypassing Antivirus using Metasploit Templates
• Abusing SSL/TLS ciphers	▪ Bypassing Windows Antimalware Scan Interface (AMSI)
○ Bypassing Firewalls through HTML Smuggling	▪ Other Techniques for Bypassing Endpoint Security
○ Bypassing Firewalls through Windows BITS	**IDS/Firewall Evading Tools**
Evading NAC and Endpoint Security	▪ Packet Fragment Generator Tools
▪ Bypassing NAC using VLAN Hopping	**Honeypot Concepts**
▪ Bypassing NAC using Pre-authenticated Device	▪ Honeypot
▪ Bypassing Endpoint Security using Ghostwriting	○ Types of Honeypots
▪ Bypassing Endpoint Security using Application Whitelisting	○ Honeypot Tools
▪ Bypassing Endpoint Security using XLM Weaponization	▪ Detecting Honeypots
▪ Bypassing Endpoint Security by Dechaining Macros	▪ Detecting and Defeating Honeypots
▪ Bypassing Endpoint Security by Clearing Memory Hooks	▪ Honeypot Detection Tools
▪ Bypassing Antivirus using Metasploit Templates	**IDS/Firewall Evasion Countermeasures**
▪ Bypassing Symantec Endpoint Protection	▪ How to Defend Against IDS Evasion
▪ Other Techniques for Bypassing Endpoint Security	▪ How to Defend Against Firewall Evasion
○ Hosting Phishing Sites	▪ How to Defend Against Endpoint Security Evasion
○ Passing Encoded Commands	▪ How to Defend Against NAC Evasion
○ Fast Flux DNS Method	▪ How to Defend Against Anti-virus Evasion
○ Timing-based Evasion	
○ Signed Binary Proxy Execution	
IDS/Firewall Evading Tools	
▪ IDS/Firewall Evading Tools	

▪ Packet Fragment Generator Tools	
Detecting Honeypots	
▪ Detecting Honeypots	
○ Detecting and Defeating Honeypots	
▪ Honeypot Detection Tools: Send-Safe Honeypot Hunter	
IDS/Firewall Evasion Countermeasures	
▪ How to Defend Against IDS Evasion	
▪ How to Defend Against Firewall Evasion	
Module 13: Hacking Web Servers	**Module 13: Hacking Web Servers**
Web Server Concepts	**Web Server Concepts**
▪ Web Server Operations	▪ Web Server Operations
▪ Web Server Security Issues	▪ Web Server Security Issues
▪ Why are Web Servers Compromised?	▪ Why are Web Servers Compromised?
Web Server Attacks	▪ Apache Web Server Architecture
▪ DNS Server Hijacking	○ Apache Vulnerabilities
▪ DNS Amplification Attack	▪ IIS Web Server Architecture
▪ Directory Traversal Attacks	○ IIS Vulnerabilities
▪ Website Defacement	▪ NGINX Web Server Architecture
▪ Web Server Misconfiguration	○ NGINX Vulnerabilities
▪ HTTP Response-Splitting Attack	**Web Server Attacks**
▪ Web Cache Poisoning Attack	▪ DNS Server Hijacking
▪ SSH Brute Force Attack	▪ DNS Amplification Attack
○ Web Server Password Cracking	▪ Directory Traversal Attacks
▪ Other Web Server Attacks	▪ Website Defacement
○ DoS/DDoS Attacks	▪ Web Server Misconfiguration
○ Man-in-the-Middle Attack	▪ HTTP Response-Splitting Attack
○ Phishing Attacks	▪ Web Cache Poisoning Attack
○ Web Application Attacks	▪ SSH Brute Force Attack
Web Server Attack Methodology	▪ FTP Brute Force with AI
▪ Information Gathering	▪ HTTP/2 Continuation Flood Attack
○ Information Gathering from Robots.txt File	▪ Frontjacking Attack
▪ Web Server Footprinting/Banner Grabbing	▪ Other Web Server Attacks
○ Web Server Footprinting Tools	○ Web Server Password Cracking
○ Enumerating Web Server Information Using Nmap	○ DoS/DDoS Attacks
▪ Website Mirroring	○ Man-in-the-Middle Attack
○ Finding Default Credentials of Web Server	○ Phishing Attacks

○ Finding Default Content of Web Server	○ Web Application Attacks
○ Finding Directory Listings of Web Server	**Web Server Attack Methodology**
• Dirhunt	▪ Information Gathering
▪ Vulnerability Scanning	○ Information Gathering from Robots.txt File
○ Finding Exploitable Vulnerabilities	▪ Web Server Footprinting/Banner Grabbing
▪ Session Hijacking	○ Web Server Footprinting Tools
▪ Web Server Password Hacking	○ Web Server Footprinting with AI
▪ Using Application Server as a Proxy	○ Web Server Footprinting using Netcat with AI
▪ Web Server Attack Tools	▪ IIS Information Gathering using Shodan
○ Metasploit	▪ Abusing Apache mod_userdir to Enumerate User Accounts
• Metasploit Exploit Module	▪ Enumerating Web Server Information Using Nmap
• Metasploit Payload and Auxiliary Modules	▪ Finding Default Credentials of Web Server
• Metasploit NOPS Module	▪ Finding Default Content of Web Server
○ Web Server Attack Tools	▪ Directory Brute Forcing
Web Server Attack Countermeasures	○ Directory Brute Forcing with AI
▪ Place Web Servers in Separate Secure Server Security Segment on Network	▪ Vulnerability Scanning
▪ Countermeasures	○ NGINX Vulnerability Scanning using Nginxpwner
○ Patches and Updates	▪ Finding Exploitable Vulnerabilities
○ Protocols and Accounts	○ Finding Exploitable Vulnerabilities with AI
○ Files and Directories	▪ Session Hijacking
▪ Detecting Web Server Hacking Attempts	▪ Web Server Password Hacking
▪ How to Defend Against Web Server Attacks	▪ Using Application Server as a Proxy
▪ How to Defend against HTTP Response-Splitting and Web Cache Poisoning	▪ Path Traversal via Misconfigured NGINX Alias
▪ How to Defend against DNS Hijacking	▪ Web Server Attack Tools
▪ Web Server Security Tools	**Web Server Attack Countermeasures**
○ Web Application Security Scanners	▪ Place Web Servers in Separate Secure Server Security Segment on Network
○ Web Server Security Scanners	▪ Countermeasures: Patches and Updates
○ Web Server Malware Infection Monitoring Tools	▪ Countermeasures: Protocols and Accounts
○ Web Server Security Tools	▪ Countermeasures: Files and Directories
○ Web Server Pen Testing Tools	▪ Detecting Web Server Hacking Attempts
Patch Management	▪ How to Defend against Web Server Attacks
▪ Patches and Hotfixes	▪ How to Defend against HTTP Response-Splitting and Web Cache Poisoning

▪ What is Patch Management?	▪ How to Defend against DNS Hijacking
▪ Installation of a Patch	▪ Web Application Security Scanners
▪ Patch Management Tools	▪ Web Server Security Scanners
	▪ Web Server Malware Infection Monitoring Tools
	▪ Web Server Security Tools
	▪ Web Server Pen Testing Tools
	Patch Management
	▪ Patches and Hotfixes
	▪ What is Patch Management?
	▪ Installation of a Patch
	▪ Patch Management Best Practices
	▪ Patch Management Tools
Module 14: Hacking Web Applications	**Module 14: Hacking Web Applications**
Web Application Concepts	**Web Application Concepts**
▪ Introduction to Web Applications	▪ Introduction to Web Applications
▪ Web Application Architecture	▪ Web Application Architecture
▪ Web Services	▪ Web Services
▪ Vulnerability Stack	▪ Vulnerability Stack
Web Application Threats	**Web Application Threats**
▪ OWASP Top 10 Application Security Risks - 2021	▪ OWASP Top 10 Application Security Risks – 2021
○ A01 - Broken Access Control	○ A01 – Broken Access Control
○ A02 - Cryptographic Failures/Sensitive Data Exposure	○ A02 – Cryptographic Failures/Sensitive Data Exposure
○ A03 - Injection Flaws	○ A03 – Injection Flaws
• SQL Injection Attacks	○ A04 – Insecure Design
• Command Injection Attacks	○ A05 – Security Misconfiguration
• Command Injection Example	○ A06 – Vulnerable and Outdated Components/Using Components with Known Vulnerabilities
• File Injection Attack	○ A07 – Identification and Authentication Failures/Broken Authentication
• LDAP Injection Attacks	○ A08 – Software and Data Integrity Failures
• Other Injection Attacks	○ A09 – Security Logging and Monitoring Failures/Insufficient Logging and Monitoring
✓ JNDI Injection	○ A10 – Server-Side Request Forgery (SSRF)
• Cross-Site Scripting (XSS) Attacks	▪ Web Application Attacks
✓ Cross-Site Scripting Attack Scenario: Attack via Email	○ Directory Traversal
✓ XSS Attack in Blog Posting	○ Hidden Field Manipulation Attack

✓ XSS Attack in Comment Field	○ Pass-the-Cookie Attack
○ A04 - Insecure Design	○ Same-Site Attack
○ A05 - Security Misconfiguration	○ SQL Injection Attacks
• XML External Entity (XXE)	○ Command Injection Attacks
○ A06 - Vulnerable and Outdated Components/Using Components with Known Vulnerabilities	○ Command Injection Example
○ A07 - Identification and Authentication Failures/Broken Authentication	○ File Injection Attack
○ A08 - Software and Data Integrity Failures	○ LDAP Injection Attacks
• Insecure Deserialization	○ Other Injection Attacks
○ A09 - Security Logging and Monitoring Failures/Insufficient Logging and Monitoring	○ Cross-Site Scripting (XSS) Attacks
○ A10 - Server-Side Request Forgery (SSRF)	○ Cross-Site Scripting Attack Scenario: Attack via Email
• Types of Server-Side Request Forgery (SSRF) Attack	○ XSS Attack in Blog Posting
✓ Injecting SSRF payload	○ XSS Attack in Comment Field
✓ Cross-Site Port Attack (XSPA)	○ Techniques to Evade XSS Filters
▪ Other Web Application Threats	○ Web-based Timing Attacks
○ Directory Traversal	○ XML External Entity (XXE) Attack
○ Unvalidated Redirects and Forwards	○ Unvalidated Redirects and Forwards
• Open Redirection	○ Magecart Attack
• Header-Based Open Redirection	○ Watering Hole Attack
• JavaScript-Based Open Redirection	○ Cross-Site Request Forgery (CSRF) Attack
○ Watering Hole Attack	○ Cookie/Session Poisoning
○ Cross-Site Request Forgery (CSRF) Attack	○ Insecure Deserialization
○ Cookie/Session Poisoning	○ Web Service Attack
○ Web Service Attack	○ Web Service Footprinting Attack
○ Web Service Footprinting Attack	○ Web Service XML Poisoning
○ Web Service XML Poisoning	○ DNS Rebinding Attack
○ Hidden Field Manipulation Attack	○ Clickjacking Attack
○ Web-based Timing Attacks	○ MarioNet Attack
○ MarioNet Attack	○ Other Web Application Attacks
○ Clickjacking Attack	**Web Application Hacking Methodology**
○ DNS Rebinding Attack	▪ Footprint Web Infrastructure
○ Same-Site Attack	○ Server Discovery
○ Pass-the-cookie Attack	○ Server Discovery: Banner Grabbing
Web Application Hacking Methodology	○ Port and Service Discovery
▪ Web Application Hacking Methodology	○ Detecting Web App Firewalls and Proxies on

	Target Site
▪ Footprint Web Infrastructure	○ WAF Detection with AI
○ Server Discovery	○ Hidden Content Discovery
○ Service Discovery	○ Detect Load Balancers
○ Server Identification/Banner Grabbing	○ Detecting Load Balancers using AI
○ Detecting Web App Firewalls and Proxies on Target Site	○ Detecting Web App Technologies
○ Hidden Content Discovery	○ WebSockets Enumeration
○ Detect Load Balancers	▪ Analyze Web Applications
▪ Analyze Web Applications	○ Website Mirroring
○ Identify Entry Points for User Input	○ Website Mirroring with AI
○ Identify Server-Side Technologies	○ Website Mirroring using Httrack with AI
○ Identify Server-Side Functionality	○ Identify Entry Points for User Input
○ Identify Files and Directories	○ Identify Server-Side Technologies
○ Identify Web Application Vulnerabilities	○ Identify Server Side Technologies using AI
~~○ Map the Attack Surface~~	○ Identify Server-Side Functionality
▪ Bypass Client-side Controls	○ Identify Files and Directories
○ Attack Hidden Form Fields	○ Identify Files and Directories with AI
○ Attack Browser Extensions	○ Identify Web Application Vulnerabilities
• Attack Google Chrome Browser Extensions	○ Identify Web Application Vulnerabilities with AI
○ Perform Source Code Review	▪ Bypass Client-side Controls
○ Evade XSS Filters	○ Attack Hidden Form Fields
▪ Attack Authentication Mechanism	○ Attack Browser Extensions
○ Design and Implementation Flaws in Authentication Mechanism	○ Attack Google Chrome Browser Extensions
○ Username Enumeration	○ Perform Source Code Review
○ Password Attacks: Password Functionality Exploits	▪ Attack Authentication Mechanism
○ Password Attacks: ~~Password Guessing~~ and Brute-forcing	○ Design Flaws in Authentication Mechanism
○ Password Attacks: Attack Password Reset Mechanism	○ Implementation Flaws in Authentication Mechanism
○ Session Attacks: Session ID Prediction/Brute-forcing	○ Username Enumeration
○ Cookie Exploitation: Cookie Poisoning	○ Password Attacks: Password Functionality Exploits
○ Bypass Authentication: Bypass SAML-based SSO	○ Password Attacks: Brute-forcing
▪ Attack Authorization Schemes	○ Password Attacks: Attack Password Reset Mechanism

○ Authorization Attack: HTTP Request Tampering	○ Session Attacks: Session ID Prediction/Brute-forcing
○ Authorization Attack: Cookie Parameter Tampering	○ Cookie Exploitation: Cookie Poisoning
▪ Attack Access Controls	○ Bypass Authentication: Bypass SAML-based SSO
▪ Attack Session Management Mechanism	○ Bypass Authentication: Bypass Rate Limit
○ Attacking Session Token Generation Mechanism	○ Bypass Authentication: Bypass Multi-Factor Authentication
○ Attacking Session Tokens Handling Mechanism: Session Token Sniffing	▪ Attack Authorization Schemes
▪ Perform Injection/Input Validation Attacks	○ Authorization Attack
○ Perform Local File Inclusion (LFI)	○ HTTP Request Tampering
▪ Attack Application Logic Flaws	○ Cookie Parameter Tampering
▪ Attack Shared Environments	▪ Attack Access Controls
▪ Attack Database Connectivity	○ Exploiting Insecure Access Controls
○ Connection String Injection	○ Access Controls Attack Methods
○ Connection String Parameter Pollution (CSPP) Attacks	▪ Attack Session Management Mechanism
○ Connection Pool DoS	○ Session Management Attack
▪ Attack Web Application Client	○ Attacking Session Token Generation Mechanism
▪ Attack Web Services	○ Attacking Session Tokens Handling Mechanism: Session Token Sniffing
○ Web Services Probing Attacks	○ Manipulating WebSocket Traffic
○ Web Service Attacks: SOAP Injection	▪ Perform Injection/Input Validation Attacks
○ Web Service Attacks: SOAPAction Spoofing	○ Injection Attacks/Input Validation Attacks
○ Web Service Attacks: WS-Address Spoofing	○ Perform Local File Inclusion (LFI)
○ Web Service Attacks: XML Injection	▪ Attack Application Logic Flaws
○ Web Services Parsing Attacks	▪ Attack Shared Environments
○ Web Service Attack Tools	▪ Attack Database Connectivity
▪ Additional Web Application Hacking Tools	○ Connection String Injection
○ TIDoS-Framework	○ Connection String Parameter Pollution (CSPP) Attacks
Web API, Webhooks, and Web Shell	○ Connection Pool DoS
▪ What is Web API?	▪ Attack Web Application Client
○ Web Services APIs	▪ Attack Web Services
▪ What are Webhooks?	○ Web Services Probing Attacks
▪ OWASP Top 10 API Security Risks	○ Web Service Attacks: SOAP Injection
▪ API Vulnerabilities	○ Web Service Attacks: SOAPAction Spoofing
▪ Web API Hacking Methodology	○ Web Service Attacks: WS-Address Spoofing

○ Identify the Target	○ Web Service Attacks: XML Injection
○ Detect Security Standards	○ Web Services Parsing Attacks
○ Identify the Attack Surface	○ Web Service Attack Tools
• Analyze Web API Requests and Responses	▪ Additional Web Application Hacking Tools
○ Launch Attacks	▪ Create and Run Custom Scripts to Automate Web Application Hacking Tasks With AI
• Fuzzing and Invalid Input Attacks	**Web API and Webhooks**
• Malicious Input Attacks	▪ Web API
• Injection Attacks	○ Web Service APIs
• Exploiting Insecure Configurations	▪ Webhooks
• Login/ Credential Stuffing Attacks	▪ OWASP Top 10 API Security Risks
• API DDoS Attacks	▪ Webhooks Security Risks
• Authorization Attacks on API: OAuth Attacks	▪ API Vulnerabilities
✓ SSRF using Dynamic Client Registration endpoint	▪ Web API Hacking Methodology
✓ WebFinger User Enumeration	○ Identify the Target
✓ Exploit Flawed Scope Validation	○ Detect Security Standards
• Other Techniques to Hack an API	○ API Enumeration
○ REST API Vulnerability Scanning	○ Identify the Attack Surface
○ Bypassing IDOR via Parameter Pollution	○ Launch Attacks
~~▪ Web Shells~~	• Other Techniques to Hack an API
~~○ Web Shell Tools~~	○ REST API Vulnerability Scanning
~~▪ How to Prevent Installation of a Web Shell~~	○ Bypassing IDOR via Parameter Pollution
~~▪ Web Shell Detection Tools~~	▪ Secure API Architecture
▪ Secure API Architecture	▪ API Security Risks and Solutions
○ Implementing Layered Security in an API	▪ Best Practices for API Security
▪ API Security Risks and Solutions	▪ Best Practices for Securing Webhooks
▪ Best Practices for API Security	**Web Application Security**
▪ Best Practices for Securing Webhooks	▪ Web Application Security Testing
Web Application Security	▪ Web Application Fuzz Testing
▪ Web Application Security Testing	▪ Web Application Fuzz Testing with AI
▪ Web Application Fuzz Testing	▪ AI-Powered Fuzz Testing
▪ Source Code Review	▪ AI-Powered Static Application Security Testing (SAST)
▪ Encoding Schemes	▪ AI-Powered Dynamic Application Security Testing (DAST)
▪ Whitelisting vs. Blacklisting Applications	▪ Source Code Review
○ Application Whitelisting and Blacklisting Tools	▪ Encoding Schemes

▪ How to Defend Against Injection Attacks	▪ Whitelisting vs. Blacklisting Applications
▪ Web Application Attack Countermeasures	○ Application Whitelisting and Blacklisting Tools
▪ How to Defend Against Web Application Attacks	▪ Content Filtering Tools
▪ RASP for Protecting Web Servers	▪ How to Defend Against Injection Attacks
▪ Bug Bounty Programs	▪ Web Application Attack Countermeasures
▪ Web Application Security Testing Tools	▪ How to Defend Against Web Application Attacks
▪ Web Application Firewalls	▪ Best Practices for Securing WebSocket Connections
	▪ RASP for Protecting Web Servers
	▪ Web Application Security Testing Tools
	▪ Web Application Firewalls
Module 15: SQL Injection	**Module 15: SQL Injection**
SQL Injection Concepts	**SQL Injection Concepts**
▪ What is SQL Injection?	▪ What is SQL Injection?
▪ SQL Injection and Server-side Technologies	▪ SQL Injection and Server-side Technologies
▪ Understanding HTTP POST Request	▪ Understanding HTTP POST Request
▪ Understanding Normal SQL Query	▪ Understanding Normal SQL Query
▪ Understanding an SQL Injection Query	▪ Understanding an SQL Injection Query
▪ Understanding an SQL Injection Query – Code Analysis	▪ 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: BadProductList.aspx
▪ Example of a Web Application Vulnerable to SQL Injection: Attack Analysis	▪ Example of a Web Application Vulnerable to SQL Injection: Attack Analysis
▪ Examples of SQL Injection	▪ Examples of SQL Injection
Types of SQL Injection	**Types of SQL Injection**
▪ Types of SQL injection	▪ In-Band SQL Injection
○ In-Band SQL Injection	○ Error Based SQL Injection
• Error Based SQL Injection	○ Union SQL Injection
• Union SQL Injection	▪ Blind/Inferential SQL Injection
○ Blind/Inferential SQL Injection	○ No Error Message Returned
• Blind SQL Injection: No Error Message Returned	○ Time-based SQL Injection
• Blind SQL Injection: WAITFOR DELAY (YES or NO Response)	○ Boolean Exploitation
• Blind SQL Injection: Boolean Exploitation and Heavy Query	○ Heavy Query
○ Out-of-Band SQL injection	▪ Out-of-Band SQL injection
SQL Injection Methodology	**SQL Injection Methodology**

▪ Information Gathering and SQL Injection Vulnerability Detection	▪ Information Gathering and SQL Injection Vulnerability Detection
o Information Gathering	o Information Gathering
o Identifying Data Entry Paths	o Identifying Data Entry Paths
o Extracting Information through Error Messages	o Extracting Information through Error Messages
o SQL Injection Vulnerability Detection: Testing for SQL Injection	o SQL Injection Vulnerability Detection
o Additional Methods to Detect SQL Injection	o Additional Methods to Detect SQL Injection
o SQL Injection Black Box Pen Testing	o SQL Injection Black Box Pen Testing
o Source Code Review to Detect SQL Injection Vulnerabilities	o Source Code Review to Detect SQL Injection Vulnerabilities
o Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL	o Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL
▪ Launch SQL Injection Attacks	▪ Launch SQL Injection Attacks
o Perform Union SQL Injection	o Perform Error Based SQL Injection
o Perform Error Based SQL Injection	o Perform Error Based SQL Injection using Stored Procedure Injection
o Perform Error Based SQL Injection using Stored Procedure Injection	o Perform Union SQL Injection
o Bypass Website Logins Using SQL Injection	o Bypass Website Logins Using SQL Injection
o Perform Blind SQL Injection – Exploitation (MySQL)	o Perform Blind SQL Injection – Boolean Exploitation (MySQL)
o Blind SQL Injection - Extract Database User	o Blind SQL Injection—Extract Database User
o Blind SQL Injection - Extract Database Name	o Blind SQL Injection—Extract Database Name
o Blind SQL Injection - Extract Column Name	o Blind SQL Injection—Extract Column Name
o Blind SQL Injection - Extract Data from ROWS	o Blind SQL Injection—Extract Data from ROWS
o Perform Double Blind SQL Injection – Classical Exploitation (MySQL)	o Exporting a Value with Regular Expression Attack
o Perform Blind SQL Injection Using Out-of-Band Exploitation Technique	o Perform Double Blind SQL Injection
o Exploiting Second-Order SQL Injection	o Perform Blind SQL Injection Using Out-of-Band Exploitation Technique
o Bypass Firewall using SQL Injection	o Exploiting Second-Order SQL Injection
o Perform SQL Injection to Insert a New User and Update Password	o Bypass Firewall to Perform SQL Injection
o Exporting a Value with Regular Expression Attack	o Bypassing WAF using JSON-based SQL Injection Attack
▪ Advanced SQL Injection	o Perform SQL Injection to Insert a New User and Update Password
o Database, Table, and Column Enumeration	▪ Advanced SQL Injection
o Advanced Enumeration	o Database, Table, and Column Enumeration

○ Features of Different DBMSs	○ Advanced Enumeration
○ Creating Database Accounts	○ Creating Database Accounts
○ Password Grabbing	○ Password Grabbing
○ Grabbing SQL Server Hashes	○ Grabbing SQL Server Hashes
○ Transfer Database to Attacker's Machine	○ Transfer Database to Attacker's Machine
○ Interacting with the Operating System	○ Interacting with the Operating System
○ Interacting with the File System	○ Interacting with the File System
○ Network Reconnaissance Using SQL Injection	○ Network Reconnaissance Using SQL Injection
○ Network Reconnaissance Full Query	○ Network Reconnaissance Full Query
○ Finding and Bypassing Admin Panel of a Website	○ Finding and Bypassing Admin Panel of a Website
○ PL/SQL Exploitation	○ PL/SQL Exploitation
○ Creating Server Backdoors using SQL Injection	○ Creating Server Backdoors using SQL Injection
○ HTTP Header-Based SQL Injection	○ HTTP Header-Based SQL Injection
○ DNS Exfiltration using SQL Injection	○ DNS Exfiltration using SQL Injection
○ MongoDB Injection/NoSQL Injection Attack	○ MongoDB Injection/NoSQL Injection Attack
~~○ Case Study: SQL Injection Attack and Defense~~	▪ SQL Injection Tools
SQL Injection Tools	▪ Discovering SQL Injection Vulnerabilities with AI
▪ SQL Injection Tools	▪ Checking for Boolean based SQL Injection with AI
▪ SQL Injection Tools for Mobile Devices	▪ Checking for Error based SQL Injection with AI
Evasion Techniques	▪ Checking for Time-based SQL Injection with AI
▪ Evading IDS	▪ Checking for UNION based SQL Injection with AI
▪ Types of Signature Evasion Techniques	**Evasion Techniques**
○ In-line Comment and Char Encoding	▪ Evading IDS
○ String Concatenation and Obfuscated Code	▪ Types of Signature Evasion Techniques
○ Manipulating White Spaces and Hex Encoding	○ Evasion Techniques
○ Sophisticated Matches and URL Encoding	○ In-line Comment
○ Null Byte and Case Variation	○ Char Encoding
○ Declare Variables and IP Fragmentation	○ String Concatenation
○ Variation	○ Obfuscated Code
SQL Injection Countermeasures	○ Manipulating White Spaces
▪ How to Defend Against SQL Injection Attacks	○ Hex Encoding
○ Use Type-Safe SQL Parameters	○ Sophisticated Matches
○ Defenses in the Application	○ URL Encoding
• LIKE Clauses	○ Null Byte
• Wrapping Parameters with QUOTENAME() and REPLACE()	○ Case Variation
▪ Detecting SQL Injection Attacks	○ Declare Variables
▪ SQL Injection Detection Tools	○ IP Fragmentation

○ OWASP ZAP and Damn Small SQLi Scanner (DSSS)	○ Variation
○ Snort	**SQL Injection Countermeasures**
○ SQL Injection Detection Tools	▪ How to Defend Against SQL Injection Attacks
	▪ Defenses in the Application
	▪ Detecting SQL Injection Attacks
	▪ SQL Injection Detection Tools
Module 16: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
Wireless Concepts	**Wireless Concepts**
▪ Wireless Terminology	▪ Wireless Terminology
▪ Wireless Networks	▪ Wireless Networks
▪ Wireless Standards	▪ Wireless Standards
▪ Service Set Identifier (SSID)	▪ Service Set Identifier (SSID)
~~▪ Wi-Fi Authentication Modes~~	▪ Wi-Fi Authentication Process
▪ Wi-Fi Authentication Process Using a Centralized Authentication Server	▪ Types of Wireless Antennas
▪ Types of Wireless Antennas	**Wireless Encryption**
Wireless Encryption	▪ Wireless Encryption
▪ Types of Wireless Encryption	○ Wired Equivalent Privacy (WEP)
○ Wired Equivalent Privacy (WEP) Encryption	○ Wi-Fi Protected Access (WPA)
○ Wi-Fi Protected Access (WPA) Encryption	○ WPA2
○ WPA2 Encryption	○ WPA3
○ WPA3 Encryption	▪ Comparison of WEP, WPA, WPA2, and WPA3
▪ Comparison of WEP, WPA, WPA2, and WPA3	▪ Issues with WEP, WPA, WPA2, and WPA3
▪ Issues in WEP, WPA, and WPA2	**Wireless Threats**
Wireless Threats	▪ Access Control Attacks
▪ Wireless Threats	▪ Integrity Attacks
○ Rogue AP Attack	▪ Confidentiality Attacks
○ Client Mis-association	▪ Availability Attacks
○ Misconfigured AP Attack	▪ Authentication Attacks
○ Unauthorized Association	▪ Honeypot AP Attack
○ Ad-Hoc Connection Attack	▪ Wormhole Attack
○ Honeypot AP Attack	▪ Sinkhole Attack
○ AP MAC Spoofing	▪ Inter-Chip Privilege Escalation/Wireless Co-Existence Attack
○ Denial-of-Service Attack	**Wireless Hacking Methodology**
○ Key Reinstallation Attack (KRACK)	▪ Wi-Fi Discovery
○ Jamming Signal Attack	○ Wireless Network Footprinting

• Wi-Fi Jamming Devices	○ Finding Wi-Fi Networks in Range to Attack
○ aLTEr Attack	○ Wi-Fi Discovery Tools
○ Wormhole and Sinkhole Attacks	○ Mobile-based Wi-Fi Discovery Tools
○ Inter-Chip Privilege Escalation/Wireless Co-Existence Attack	○ Finding WPS-Enabled APs
○ GNSS Spoofing	▪ Wireless Traffic Analysis
Wireless Hacking Methodology	○ Choosing the Optimal Wi-Fi Card
▪ Wireless Hacking Methodology	○ Perform Spectrum Analysis
▪ Wi-Fi Discovery	▪ Launch of Wireless Attacks
○ Wireless Network Footprinting	○ Aircrack-ng Suite
○ Finding Wi-Fi Networks in Range to Attack	○ Detection of Hidden SSIDs
○ Finding WPS-Enabled APs	○ Denial-of-Service
○ Wi-Fi Discovery Tools	○ Man-in-the-Middle Attack
○ Mobile-based Wi-Fi Discovery Tools	○ MITM Attack Using Aircrack-ng
▪ GPS Mapping	○ MAC Spoofing Attack
○ GPS Mapping Tools	○ Wireless ARP Poisoning Attack
○ Wi-Fi Hotspot Finder Tools	○ ARP Poisoning Attack Using Ettercap
○ Wi-Fi Network Discovery Through WarDriving	○ Rogue APs
▪ Wireless Traffic Analysis	○ Creation of a Rogue AP Using MANA Toolkit
○ Choosing the Optimal Wi-Fi Card	○ Evil Twin
○ Sniffing Wireless Traffic	○ Key Reinstallation Attack (KRACK)
○ Perform Spectrum Analysis	○ Jamming Signal Attack
▪ Launch of Wireless Attacks	○ Wi-Fi Jamming Devices
○ Aircrack-ng Suite	○ aLTEr Attack
○ Detection of Hidden SSIDs	○ Wi-Jacking Attack
~~○ Fragmentation Attack~~	○ RFID Cloning Attack
○ MAC Spoofing Attack	○ Wi-Fi Encryption Cracking
~~○ Denial-of-Service: Disassociation and De-authentication Attacks~~	○ WPA/WPA2 Encryption Cracking
○ Man-in-the-Middle Attack	○ Cracking WPA/WPA2 Using Aircrack-ng
○ MITM Attack Using Aircrack-ng	○ WPA Brute Forcing Using Fern Wifi Cracker
○ Wireless ARP Poisoning Attack	○ WPA3 Encryption Cracking
• ARP Poisoning Attack Using Ettercap	○ Cracking WPA3 Using Aircrack-ng and hashcat
○ Rogue APs	○ Cracking WPS Using Reaver
• Creation of a Rogue AP Using MANA Toolkit	**Wireless Attack Countermeasures**
○ Evil Twin	▪ Wireless Security Layers
• Set Up of a Fake Hotspot (Evil Twin)	▪ Defense Against WPA/WPA2/WPA3 Cracking
○ aLTEr Attack	▪ Defense Against KRACK Attacks
○ Wi-Jacking Attack	▪ Defense Against aLTEr Attacks

○ RFID Cloning Attack	▪ Detection and Blocking of Rogue APs
▪ Wi-Fi Encryption Cracking	▪ Defense Against Wireless Attacks
~~○ WEP Encryption Cracking~~	▪ Wireless Intrusion Prevention Systems
~~○ Cracking WEP Using Aircrack-ng~~	▪ WIPS Deployment
○ WPA/WPA2 Encryption Cracking	▪ Wi-Fi Security Auditing Tools
~~○ Cracking WPA-PSK Using Aircrack-ng~~	▪ Wi-Fi IPSs
○ Cracking WPA/WPA2 Using Wifiphisher	
○ Cracking WPS Using Reaver	
○ WPA3 Encryption Cracking	
~~○ WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker~~	
Wireless Hacking Tools	
~~▪ WEP/WPA/WPA2 Cracking Tools~~	
~~▪ WEP/WPA/WPA2 Cracking Tools for Mobile~~	
~~▪ Wi-Fi Packet Sniffers~~	
~~▪ Wi-Fi Traffic Analyzer Tools~~	
~~▪ Other Wireless Hacking Tools~~	
~~**Bluetooth Hacking**~~	
~~▪ Bluetooth Stack~~	
~~▪ Bluetooth Hacking~~	
~~▪ Bluetooth Threats~~	
~~▪ Bluejacking~~	
~~▪ Bluetooth Reconnaissance Using Bluez~~	
~~▪ Btlejacking Using BtleJack~~	
~~▪ Cracking BLE Encryption Using crackle~~	
~~▪ Bluetooth Hacking Tools~~	
Wireless Attack Countermeasures	
▪ Wireless Security Layers	
▪ Defense Against WPA/WPA2/WPA3 Cracking	
▪ Defense Against KRACK and aLTEr Attacks	
▪ Detection and Blocking of Rogue APs	
▪ Defense Against Wireless Attacks	
▪ Defense Against Bluetooth Hacking	
Wireless Security Tools	
▪ Wireless Intrusion Prevention Systems	
▪ WIPS Deployment	
▪ Wi-Fi Security Auditing Tools	
▪ Wi-Fi IPSs	
~~▪ Wi-Fi Predictive Planning Tools~~	

~~▪ Wi-Fi Vulnerability Scanning Tools~~	
~~▪ Bluetooth Security Tools~~	
~~▪ Wi-Fi Security Tools for Mobile~~	
Module 17: Hacking Mobile Platforms	**Module 17: Hacking Mobile Platforms**
Mobile Platform Attack Vectors	**Mobile Platform Attack Vectors**
▪ Vulnerable Areas in Mobile Business Environment	▪ Vulnerable Areas in Mobile Business Environment
~~▪ OWASP Top 10 Mobile Risks – 2016~~	▪ OWASP Top 10 Mobile Risks - 2024
▪ Anatomy of a Mobile Attack	▪ Anatomy of a Mobile Attack
▪ How a Hacker can Profit from Mobile Devices that are Successfully Compromised	▪ How a Hacker can Profit from Mobile Devices that are Successfully Compromised
▪ Mobile Attack Vectors and Mobile Platform Vulnerabilities	▪ Mobile Attack Vectors and Mobile Platform Vulnerabilities
▪ Security Issues Arising from App Stores	▪ Security Issues Arising from App Stores
▪ App Sandboxing Issues	▪ App Sandboxing Issues
▪ Mobile Spam	▪ Mobile Spam
▪ SMS Phishing Attack (SMiShing) (Targeted Attack Scan)	▪ SMS Phishing Attack (SMiShing) (Targeted Attack Scan)
○ SMS Phishing Attack Examples	▪ SMS Phishing Attack Examples
▪ Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections	▪ Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
▪ Agent Smith Attack	▪ Agent Smith Attack
▪ Exploiting SS7 Vulnerability	▪ Exploiting SS7 Vulnerability
▪ Simjacker: SIM Card Attack	▪ Simjacker: SIM Card Attack
▪ OTP Hijacking/Two-Factor Authentication Hijacking	▪ Call Spoofing
▪ Camera/Microphone Capture Attacks	▪ OTP Hijacking/Two-Factor Authentication Hijacking
○ Camfecting Attack	▪ OTP Hijacking Tools
○ Android Camera Hijack Attack	▪ Camera/Microphone Capture Attacks
Hacking Android OS	▪ Camera/Microphone Hijacking Tools
▪ Android OS	**Hacking Android OS**
○ Android Device Administration API	▪ Android OS
▪ Android Rooting	○ Android Device Administration API
○ Rooting Android Using KingoRoot	▪ Android Rooting
○ Android Rooting Tools	○ Rooting Android Using KingoRoot
▪ Hacking Android Devices	○ Android Rooting Tools
○ Blocking Wi-Fi Access Using NetCut	▪ Hacking Android Devices
○ Identifying Attack Surfaces Using drozer	○ Identifying Attack Surfaces Using drozer
○ Hacking with zANTI and Network Spoofer	○ Bypassing FRP on Android Phones Using 4ukey

○ Launch DoS Attack using Low Orbit Ion Cannon (LOIC)	○ Hacking with zANTI and Kali NetHunter
○ Session Hijacking Using DroidSheep	○ Launch DoS Attack using Low Orbit Ion Cannon (LOIC)
○ Hacking with Orbot Proxy	○ Hacking with Orbot Proxy
○ Exploiting Android Device through ADB Using PhoneSploit	○ Exploiting Android Device through ADB Using PhoneSploit Pro
○ Android-based Sniffers	○ Launching Man-in-the-Disk Attack
○ Launching Man-in-the-Disk Attack	○ Launching Spearphone Attack
○ Launching Sphearphone Attack	○ Exploiting Android Devices Using Metasploit
○ Exploiting Android Devices Using Metasploit	○ Analyzing Android Devices
○ Other Techniques for Hacking Android Devices	○ Other Techniques for Hacking Android Devices
○ Android Trojans	○ Android Malware
▪ OTP Hijacking Tools	▪ Android Hacking Tools
▪ Camera/Microphone Hijacking Tools	▪ Android-based Sniffers
▪ Android Hacking Tools	▪ Securing Android Devices
▪ Securing Android Devices	▪ Android Security Tools
▪ Android Security Tools	○ Android Device Tracking Tools
○ Android Device Tracking Tools: Google Find My Device	○ Android Vulnerability Scanners
○ Android Device Tracking Tools	○ Static Analysis of Android APK
○ Android Vulnerability Scanners	○ Online Android Analyzers
○ Online Android Analyzers	**Hacking iOS**
Hacking iOS	▪ Apple iOS
▪ Apple iOS	▪ Jailbreaking iOS
▪ Jailbreaking iOS	○ Jailbreaking Techniques
○ Jailbreaking Techniques	○ Jailbreaking iOS Using Hexxa Plus
○ Jailbreaking iOS Using Hexxa Plus	○ Jailbreaking Tools
○ Jailbreaking Tools	▪ Hacking iOS Devices
▪ Hacking iOS Devices	○ Hacking using Spyzie
○ Hacking using Spyzie	○ iOS Trustjacking
○ Hacking Network using Network Analyzer Pro	○ Post-exploitation on iOS Devices Using SeaShell Framework
○ iOS Trustjacking	○ Analyzing and Manipulating iOS Applications
○ Analyzing and Manipulating iOS Applications	○ Analyzing iOS Devices
• Manipulating an iOS Application Using cycript	○ iOS Malware
• iOS Method Swizzling	○ iOS Hacking Tools
• Extracting Secrets Using Keychain Dumper	▪ Securing iOS Devices
• Analyzing an iOS Application Using	▪ iOS Device Security Tools

objection	
○ iOS Malware	○ iOS Device Tracking Tools
○ iOS Hacking Tools	**Mobile Device Management**
▪ Securing iOS Devices	▪ Mobile Device Management (MDM)
▪ iOS Device Security Tools	▪ Mobile Device Management Solutions
▪ iOS Device Tracking Tools	▪ Bring Your Own Device (BYOD)
Mobile Device Management	○ BYOD Risks
▪ Mobile Device Management (MDM)	○ BYOD Policy Implementation
▪ Mobile Device Management Solutions: IBM MaaS360	○ BYOD Security Guidelines
○ Mobile Device Management Solutions	**Mobile Security Guidelines and Tools**
▪ Bring Your Own Device (BYOD)	▪ Mobile Security Guidelines
○ BYOD Risks	▪ OWASP Top 10 Mobile Risks and Solutions
○ BYOD Policy Implementation	▪ General Guidelines for Mobile Platform Security
○ BYOD Security Guidelines	▪ Mobile Device Security Guidelines for the Administrator
Mobile Security Guidelines and Tools	▪ SMS Phishing Countermeasures
▪ OWASP Top 10 Mobile Controls	▪ OTP Hijacking Countermeasures
▪ General Guidelines for Mobile Platform Security	▪ Critical Data Storage in Android and iOS: KeyStore and Keychain Recommendations
▪ Mobile Device Security Guidelines for Administrator	▪ Reverse Engineering Mobile Applications
▪ SMS Phishing Countermeasures	▪ Mobile Security Tools
▪ Critical Data Storage in Android and iOS: KeyStore and Keychain Recommendations	○ Source Code Analysis Tools
▪ Mobile Security Tools	○ Reverse Engineering Tools
○ Source Code Analysis Tools	○ App Repackaging Detectors
○ Reverse Engineering Tools	○ Mobile Protection Tools
○ App Repackaging Detector	○ Mobile Anti-Spyware
○ Mobile Protection Tools	○ Mobile Pen Testing Toolkits
○ Mobile Anti-Spyware	
○ Mobile Pen Testing Toolkit: ImmuniWeb® MobileSuite	
Module 18: IoT and OT Hacking	**Module 18: IoT and OT Hacking**
IoT Hacking	**IoT Hacking**
IoT Concepts	**IoT Concepts and Attacks**
▪ What is the IoT?	▪ What is the IoT?
▪ How the IoT Works	▪ How the IoT Works
▪ IoT Architecture	▪ IoT Architecture

▪ IoT Application Areas and Devices	▪ IoT Application Areas and Devices
▪ IoT Technologies and Protocols	▪ IoT Technologies and Protocols
▪ IoT Communication Models	▪ IoT Communication Models
▪ Challenges of IoT	▪ Challenges of IoT
▪ Threat vs Opportunity	▪ Threat vs Opportunity
IoT Attacks	▪ IoT Security Problems
▪ IoT Security Problems	▪ OWASP Top 10 IoT Threats
▪ OWASP Top 10 IoT Threats	▪ OWASP IoT Attack Surface Areas
▪ OWASP IoT Attack Surface Areas	▪ IoT Vulnerabilities
▪ IoT Vulnerabilities	▪ IoT Threats
▪ IoT Threats	▪ Hacking IoT Devices: General Scenario
▪ Hacking IoT Devices: General Scenario	▪ DDoS Attack
▪ IoT Attacks	▪ Exploit HVAC
○ DDoS Attack	▪ Rolling Code Attack
○ Exploit HVAC	▪ BlueBorne Attack
○ Rolling Code Attack	▪ Jamming Attack
○ BlueBorne Attack	▪ Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor
○ Jamming Attack	▪ SDR-Based Attacks on IoT
○ Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor	▪ Identifying and Accessing Local IoT Devices
○ SDR-Based Attacks on IoT	▪ Fault Injection Attacks
○ Identifying and Accessing Local IoT Devices	▪ Other IoT Attacks
○ Fault Injection Attacks	▪ IoT Attacks in Different Sectors
○ Other IoT Attacks	▪ IoT Malware
▪ IoT Attacks in Different Sectors	▪ Case Study: IZ1H9
▪ Case Study~~: Enemybot~~	**IoT Hacking Methodology**
IoT Hacking Methodology	▪ What is IoT Device Hacking?
▪ What is IoT Device Hacking?	▪ IoT Hacking Methodology
▪ IoT Hacking Methodology	○ Information Gathering
○ Information Gathering Using Shodan	○ Information Gathering using Shodan
○ Information Gathering using MultiPing	○ Information Gathering using MultiPing
○ Information Gathering using FCC ID Search	○ Information Gathering using FCC ID Search
○ Discovering IoT Devices with Default Credentials using IoTSeeker	○ Information-Gathering Tools
○ Vulnerability Scanning using Nmap	○ Information Gathering through Sniffing
○ Vulnerability Scanning using RIoT Vulnerability Scanner	○ Sniffing using Cascoda Packet Sniffer
○ Sniffing using Foren6	○ Sniffing Tools

○ Sniffing using Wireshark	○ Vulnerability Scanning
○ Analyzing Spectrum and IoT Traffic	○ Vulnerability Scanning using IoTSeeker
○ Rolling code Attack using RFCrack	○ Vulnerability Scanning using Genzai
~~○ Hacking Zigbee Devices with Attify Zigbee Framework~~	○ Vulnerability Scanning using Nmap
○ BlueBorne Attack Using HackRF One	○ Vulnerability-Scanning Tools
○ Replay Attack using HackRF One	○ Analyzing Spectrum and IoT Traffic
○ SDR-Based Attacks using RTL-SDR and GNU Radio	○ Tools to Perform SDR-Based Attacks
○ Side Channel Attack using ChipWhisperer	▪ Launch Attacks
○ Identifying IoT Communication Buses and Interfaces	○ Rolling Code Attack using RFCrack
○ NAND Glitching	○ Hacking Zigbee Devices with Open Sniffer
○ Gaining Remote Access using Telnet	○ BlueBorne Attack Using HackRF One
○ Maintain Access by Exploiting Firmware	○ Replay Attack using HackRF One
• Firmware Analysis and Reverse Engineering	○ SDR-Based Attacks using RTL-SDR and GNU Radio
✓ Emulate Firmware for Dynamic Testing	○ Side-Channel Attack using ChipWhisperer
▪ IoT Hacking Tools	○ Identifying IoT Communication Buses and Interfaces
○ Information-Gathering Tools	○ NAND Glitching
○ Sniffing Tools	○ Exploiting Cameras using CamOver
○ Vulnerability-Scanning Tools	▪ Gain Remote Access
○ Tools to Perform SDR-Based Attacks	○ Gaining Remote Access using Telnet
○ IoT Hacking Tools	○ Maintain Access
IoT Attack Countermeasures	○ Maintain Access by Exploiting Firmware
▪ How to Defend Against IoT Hacking	○ Firmware Analysis and Reverse Engineering
▪ General Guidelines for IoT Device Manufacturing Companies	▪ IoT Hacking Tools
▪ OWASP Top 10 IoT Vulnerabilities Solutions	○ IoT Hacking Tools
▪ IoT Framework Security Considerations	**IoT Attack Countermeasures**
▪ IoT Hardware Security Best Practices	▪ How to Defend Against IoT Hacking
▪ IoT Device Management	▪ General Guidelines for IoT Device Manufacturers
▪ IoT Security Tools	▪ OWASP Top 10 IoT Vulnerabilities Solutions
OT Hacking	▪ IoT Framework Security Considerations
OT Concepts	▪ IoT Hardware Security Best Practices
▪ What is OT?	▪ Secure Development Practices for IoT Applications
▪ Essential Terminology	▪ IoT Device Management
▪ IT/OT Convergence (IIOT)	▪ IoT Security Tools
▪ The Purdue Model	**OT Hacking**

▪ Challenges of OT	**OT Concepts and Attacks**
▪ Introduction to ICS	▪ What is OT?
▪ Components of an ICS	▪ Essential Terminology
○ Distributed Control System (DCS)	▪ Introduction to ICS
○ Supervisory Control and Data Acquisition (SCADA)	▪ Components of an ICS
○ Programmable Logic Controller (PLC)	▪ IT/OT Convergence (IIOT)
○ Basic Process Control System (BPCS)	▪ The Purdue Model
○ Safety Instrumented Systems (SIS)	▪ OT Technologies and Protocols
▪ OT Technologies and Protocols	▪ Challenges of OT
OT Attacks	▪ OT Vulnerabilities
▪ OT Vulnerabilities	▪ MITRE ATT&CK for ICS
▪ MITRE ATT&CK for ICS	▪ OT Threats
▪ OT Threats	▪ HMI-based Attacks
▪ OT Attacks	▪ Side-Channel Attacks
○ HMI-based Attacks	▪ Hacking Programmable Logic Controller (PLC)
○ Side-Channel Attacks	▪ Evil PLC Attack
○ Hacking Programmable Logic Controller (PLC)	▪ Hacking Industrial Systems through RF Remote Controllers
○ Hacking Industrial Systems through RF Remote Controllers	▪ OT Supply Chain Attacks
○ OT Malware	▪ OT Malware
▪ OT Malware Analysis: INDUSTROYER.V2	▪ OT Malware Analysis: COSMICENERGY
OT Hacking Methodology	**OT Hacking Methodology**
▪ What is OT Hacking?	▪ What is OT Hacking?
▪ OT Hacking Methodology	▪ OT Hacking Methodology
○ Identifying ICS/SCADA Systems using Shodan	▪ Information Gathering
○ Gathering Default Passwords using CRITIFENCE	○ Identifying ICS/SCADA Systems using Shodan
○ Scanning ICS/SCADA Systems using Nmap	○ Gathering Default Passwords using CIRT.net
○ Vulnerability Scanning using Nessus	○ Information-Gathering Tools
○ Vulnerability Scanning using Skybox Vulnerability Control	○ Scanning ICS/SCADA Systems using Nmap
○ Fuzzing ICS Protocols	○ Sniffing using NetworkMiner
○ Sniffing using NetworkMiner	○ Analyzing Modbus/TCP Traffic using Wireshark
○ Analyzing Modbus/TCP Traffic Using Wireshark	○ Discovering ICS/SCADA Network Protocols using Malcolm
○ Discovering ICS/SCADA Network Topology using GRASSMARLIN	○ Vulnerability Scanning
○ Hacking ICS Hardware	○ Vulnerability Scanning Using Nessus
○ Hacking Modbus Slaves using Metasploit	○ Vulnerability Scanning using Skybox

	Vulnerability Control
○ Hacking PLC using modbus-cli	○ Sniffing and Vulnerability-Scanning Tools
○ Gaining Remote Access using DNP3	○ Fuzzing ICS Protocols
▪ OT Hacking Tools	▪ Launch Attacks
○ Information-Gathering Tools	○ Hacking ICS Hardware
○ Sniffing and Vulnerability-Scanning Tools	○ Hacking Modbus Slaves using Metasploit
○ OT Hacking Tools	○ Hacking PLC using modbus-cli
OT Attack Countermeasures	▪ Gain and Maintain Remote Access
▪ How to Defend Against OT Hacking	○ Gaining Remote Access using DNP3
▪ OT Vulnerabilities and Solutions	▪ OT Hacking Tools
▪ How to Secure an IT/OT Environment	○ OT Hacking Tools
▪ Implementing a Zero-Trust Model for ICS/SCADA	**OT Attack Countermeasures**
▪ International OT Security Organizations and Frameworks	▪ How to Defend Against OT Hacking
○ OTCSA	▪ OT Vulnerabilities and Solutions
○ OT-ISAC	▪ How to Secure an IT/OT Environment
○ NERC	▪ Implementing a Zero-Trust Model for ICS/SCADA
○ Industrial Internet Security Framework (IISF)	▪ International OT Security Organizations
○ ISA/IEC-62443	▪ OT Security Solutions
▪ OT Security Solutions	▪ OT Security Tools
▪ OT Security Tools	
Module 19: Cloud Computing	**Module 19: Cloud Computing**
Cloud Computing Concepts	**Cloud Computing Concepts**
▪ Introduction to Cloud Computing	▪ Introduction to Cloud Computing
▪ Types of Cloud Computing Services	▪ Types of Cloud Computing Services
○ Infrastructure-as-a-Service (IaaS)	▪ Shared Responsibilities in Cloud
○ Platform-as-a-Service (PaaS)	▪ Cloud Deployment Models
○ Software-as-a-Service (SaaS)	▪ NIST Cloud Deployment Reference Architecture
○ Identity-as-a-Service (IDaaS)	▪ Cloud Storage Architecture
○ Security-as-a-Service (SECaaS)	▪ Virtual Reality and Augmented Reality on Cloud
○ Container-as-a-Service (CaaS)	▪ Fog Computing
○ Function-as-a-Service (FaaS)	▪ Edge Computing
○ Anything-as-a-Service (XaaS)	▪ Cloud vs. Fog Computing vs. Edge Computing
○ Firewalls-as-a-Service (FWaaS)	▪ Cloud Computing vs. Grid Computing
○ Desktop-as-a-Service (DaaS)	▪ Cloud Service Providers
○ Mobile Backend-as-a-Service (MBaaS)	**Container Technology**
○ Machines-as-a-Service (MaaS) Business Model	▪ What is a Container?
▪ Separation of Responsibilities in Cloud	○ Containers Vs. Virtual Machines

▪ Cloud Deployment Models	▪ What is Docker?
○ Public Cloud	○ Microservices Vs. Docker
○ Private Cloud	▪ Docker Networking
○ Community Cloud	▪ Container Orchestration
○ Hybrid Cloud	▪ What is Kubernetes?
○ Multi Cloud	▪ Clusters and Containers
○ Distributed Cloud	▪ Container Security Challenges
○ Poly Cloud	▪ Container Management Platforms
▪ NIST Cloud Deployment Reference Architecture	▪ Kubernetes Platforms
▪ Cloud Storage Architecture	**Serverless Computing**
▪ Role of AI in Cloud Computing	▪ What is Serverless Computing?
▪ Virtual Reality and Augmented Reality on Cloud	▪ Serverless Vs. Containers
▪ Fog Computing	▪ Serverless Computing Frameworks
▪ Edge Computing	**Cloud Computing Threats**
▪ Cloud vs. Fog Computing vs. Edge Computing	▪ OWASP Top 10 Cloud Security Risks
▪ Cloud Computing vs. Grid Computing	▪ OWASP Top 10 Kubernetes Risks
▪ Cloud Service Providers	▪ OWASP Top 10 Serverless Security Risks
Container Technology	▪ Cloud Computing Threats
▪ What is a Container?	○ Data Security
▪ Containers Vs. Virtual Machines	○ Cloud Service Misuse
▪ What is Docker?	○ Interface and API Security
○ Microservices Vs. Docker	○ Operational Security
○ Docker Networking	○ Infrastructure and System Configuration
▪ Container Orchestration	○ Network Security
▪ What is Kubernetes?	○ Governance and Legal Risks
○ Kubernetes Vs. Docker	○ Development and Resource Management
▪ Clusters and Containers	▪ Container Vulnerabilities
▪ Container Security Challenges	▪ Kubernetes Vulnerabilities
▪ Container Management Platforms	▪ Cloud Attacks
▪ Kubernetes Platforms	○ Service Hijacking using Social Engineering
Serverless Computing	○ Service Hijacking using Network Sniffing
▪ What is Serverless Computing?	○ Side-Channel Attacks or Cross-guest VM Breaches
▪ Serverless Vs. Containers	○ Wrapping Attack
▪ Serverless Computing Frameworks	○ Man-in-the-Cloud (MITC) Attack
Cloud Computing Threats	○ Cloud Hopper Attack
▪ OWASP Top 10 Cloud Security Risks	○ Cloud Cryptojacking
▪ OWASP Top 10 Serverless Security Risks	○ Cloudborne Attack
▪ Cloud Computing Threats	○ Instance Metadata Service (IMDS) Attack

▪ Container Vulnerabilities	○ Cache Poisoned Denial of Service (CPDoS)/Content Delivery Network (CDN) Cache Poisoning Attack
▪ Kubernetes Vulnerabilities	○ Cloud Snooper Attack
▪ Cloud Attacks	○ Golden SAML Attack
○ Service Hijacking using Social Engineering	○ Living Off the Cloud Attack (LotC)
○ Service Hijacking using Network Sniffing	○ Other Cloud Attacks
○ Side-Channel Attacks or Cross-guest VM Breaches	▪ Cloud Malware
○ Wrapping Attack	**Cloud Hacking**
○ Man-in-the-Cloud (MITC) Attack	▪ Cloud Hacking
○ Cloud Hopper Attack	▪ Cloud Hacking Methodology
○ Cloud Cryptojacking	○ Identifying Target Cloud Environment
○ Cloudborne Attack	○ Discovering Open Ports and Services Using Masscan
○ Instance Metadata Service (IMDS) Attack	○ Vulnerability Scanning Using Prowler
○ Cache Poisoned Denial of Service (CPDoS)/Content Delivery Network (CDN) Cache Poisoning Attack	○ Identifying Misconfigurations in Cloud Resources Using CloudSploit
○ Cloud Snooper Attack	○ Cleanup and Maintaining Stealth
○ Golden SAML Attack	**AWS Hacking**
○ Other Cloud Attacks	▪ Enumerating S3 Buckets
▪ Cloud Malware	○ Enumerating S3 Buckets using SScanner
Cloud Hacking	○ Enumerating S3 Bucket Permissions using BucketLoot
▪ What is Cloud Hacking?	○ Enumerating S3 Buckets using CloudBrute
▪ Hacking Cloud	▪ Enumerating EC2 Instances
○ Container Vulnerability Scanning using Trivy	▪ Enumerating AWS RDS Instances
○ Kubernetes Vulnerability Scanning using Sysdig	▪ Enumerating AWS Account IDs
○ Enumerating S3 Buckets	▪ Enumerating IAM Roles
○ Identifying Open S3 Buckets using S3Scanner	▪ Enumerating Weak IAM Policies Using Cloudsplaining
○ Enumerating AWS Account IDs	▪ Enumerating AWS Cognito
○ Enumerating IAM Roles	▪ Enumerating DNS Records of AWS Accounts using Ghostbuster
○ Enumerating Bucket Permissions using S3Inspector	▪ Enumerating Serverless Resources in AWS
○ Enumerating Kubernetes etcd	▪ Discovering Attack Paths using Cartography
○ Enumerating Azure Active Directory (AD) Accounts	▪ Discovering Attack Paths using CloudFox
○ Gathering Cloud Keys Through IMDS Attack	▪ Identify Security Groups Exposed to the Internet

~~o Exploiting Amazon Cloud Infrastructure using Nimbostratus~~	▪ AWS Threat Emulation using Stratus Red Team
o Exploiting Misconfigured AWS S3 Buckets	▪ Gathering Cloud Keys Through IMDS Attack
o Compromising AWS IAM Credentials	▪ Exploiting Misconfigured AWS S3 Buckets
o Hijacking Misconfigured IAM Roles using Pacu	▪ Compromising AWS IAM Credentials
o Cracking AWS Access Keys using DumpsterDiver	▪ Hijacking Misconfigured IAM Roles using Pacu
o Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)	▪ Scanning AWS Access Keys using DumpsterDiver
o Serverless-Based Attacks on AWS Lambda	▪ Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)
o Exploiting Shadow Admins in AWS	▪ Exploiting Shadow Admins in AWS
o Exploiting Docker Remote API	▪ Gaining Access by Exploiting SSRF Vulnerabilities
o Hacking Container Volumes	▪ Attacks on AWS Lambda
~~o CloudGoat 2 – Vulnerable by Design AWS Deployment Tool~~	▪ AWS IAM Privilege Escalation Techniques
o Gaining Access by Exploiting SSRF Vulnerability	▪ Creating Backdoor Accounts in AWS
o AWS IAM Privilege Escalation Techniques	▪ Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating the CloudTrail Service
o Escalating Privileges of Google Storage Buckets using GCPBucketBrute	▪ Establishing Persistence on EC2 Instances
o Privilege Escalation Using Misconfigured User Accounts in Azure AD	▪ Lateral Movement: Moving Between AWS Accounts and Regions
o Creating Backdoor Accounts in AWS	▪ AWSGoat: A Damn Vulnerable AWS Infrastructure
~~o Backdooring Docker Images using dockerscan~~	**Microsoft Azure Hacking**
o Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating CloudTrial Service	▪ Azure Reconnaissance Using AADInternals
▪ AWS Hacking Tool: AWS pwn	▪ Identifying Azure Services and Resources
Cloud Security	▪ Enumerating Azure Active Directory (AD) Accounts
▪ Cloud Security Control Layers	▪ Identifying Attack Surface using Stormspotter
▪ Cloud Security is the Responsibility of both Cloud Provider and Consumer	▪ Collecting Data from AzureAD and AzureRM using AzureHound
▪ Cloud Computing Security Considerations	▪ Accessing Publicly Exposed Blob Storage using Goblob
▪ Placement of Security Controls in the Cloud	▪ Identifying Open Network Security Groups (NSGs) in Azure
▪ Best Practices for Securing Cloud	▪ Exploiting Managed Identities and Azure Functions
▪ NIST Recommendations for Cloud Security	▪ Privilege Escalation Using Misconfigured User Accounts in Azure AD

▪ Security Assertion Markup Language (SAML)	▪ Creating Persistent Backdoors in Azure AD Using Service Principals
▪ Cloud Network Security	▪ Exploiting VNet Peering Connections
○ Virtual Private Cloud (VPC)	▪ AzureGoat – Vulnerable by Design Azure Infrastructure
○ Public and Private Subnets	**Google Cloud Hacking**
○ Transit Gateways	▪ Enumerating GCP Resources using Google Cloud CLI
○ VPC Endpoint	○ Enumerating GCP Organizations, Projects, and Cloud Storage Buckets
▪ Cloud Security Controls	○ Enumerating Google Cloud Service Accounts
○ Cloud Application Security	○ Enumerating Google Cloud resources
○ High Availability Across Zones	○ Enumerating Google Cloud IAM Roles and Policies
○ Cloud Integration and Auditing	○ Enumerating Google Cloud Services using gcp_service_enum
○ Security Groups	○ Enumerating GCP Resources using GCP Scanner
○ Instance Awareness	○ Enumerating Google Cloud Storage Buckets using cloud_enum
▪ Kubernetes Vulnerabilities and Solutions	▪ Enumerating Privilege Escalation Vulnerabilities using GCP Privilege Escalation Scanner
▪ Serverless Security Risks and Solutions	▪ Escalating Privileges of Google Storage Buckets using GCPBucketBrute
▪ Best Practices for Container Security	▪ Maintaining Access: Creating Backdoors with IAM Roles in GCP
▪ Best Practices for Docker Security	▪ GCPGoat: Vulnerable by Design GCP Infrastructure
▪ Best Practices for Kubernetes Security	**Container Hacking**
▪ Best Practices for Serverless Security	▪ Information Gathering using kubectl
▪ Zero Trust Networks	▪ Enumerating Registries
▪ Organization/Provider Cloud Security Compliance Checklist	▪ Container/Kubernetes Vulnerability Scanning
▪ International Cloud Security Organizations	▪ Exploiting Docker Remote API
▪ Shadow Cloud Asset Discovery Tools	▪ Hacking Container Volumes
▪ Cloud Security Tools	▪ LXD/LXC Container Group Privilege Escalation
▪ Container Security Tools	▪ Post Enumeration on Kubernetes etcd
▪ Kubernetes Security Tools	**Cloud Security**
▪ Serverless Application Security Solutions	▪ Cloud Security Control Layers
▪ Cloud Access Security Broker (CASB)	▪ Cloud Security is the Responsibility of both Cloud Provider and Consumer
○ CASB Solutions	▪ Cloud Computing Security Considerations

• Forcepoint CASB	▪ Placement of Security Controls in the Cloud
▪ Next-Generation Secure Web Gateway (NG SWG)	▪ Assessing Cloud Security using Scout Suite
○ NG SWG Solutions	▪ 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	**Module 20: Cryptography**
Cryptography Concepts	**Cryptography Concepts and Encryption Algorithms**
▪ Cryptography	▪ Cryptography
▪ Government Access to Keys (GAK)	▪ Government Access to Keys (GAK)
Encryption Algorithms	▪ Ciphers
▪ Ciphers	▪ Symmetric Encryption Algorithms
▪ Data Encryption Standard (DES) and Advanced Encryption Standard (AES)	▪ Data Encryption Standard (DES)
▪ RC4, RC5, and RC6 Algorithms	▪ Triple Data Encryption Standard (DES)
▪ Twofish and Threefish	▪ Advanced Encryption Standard (AES)

▪ Serpent and TEA	▪ RC4, RC5, and RC6 Algorithms
▪ CAST-128	▪ Blowfish
▪ GOST Block Cipher and Camellia	▪ Twofish
▪ DSA and Related Signature Schemes	▪ Threefish
▪ Rivest Shamir Adleman (RSA)	▪ Serpent
▪ Diffie-Hellman	▪ TEA
▪ YAK	▪ CAST-128
▪ Message Digest (One-Way Hash) Functions	▪ GOST Block Cipher
○ Message Digest Function: MD5 and MD6	▪ Camellia
○ Message Digest Function: Secure Hashing Algorithm (SHA)	▪ Asymmetric Encryption Algorithms
○ RIPEMD – 160 and HMAC	▪ DSA and Related Signature Schemes
▪ Other Encryption Techniques	▪ Rivest Shamir Adleman (RSA)
○ Post-quantum Cryptography	▪ Diffie–Hellman
○ Lightweight Cryptography	▪ Elliptic Curve Cryptography (ECC)
▪ Comparison of Cryptographic Algorithms	▪ YAK
▪ Cipher Modes of Operation	▪ Message Digest (One-way Hash) Functions
○ Electronic Code Book (ECB) Mode	▪ Message Digest Functions
○ Cipher Block Chaining (CBC) Mode	▪ Message Digest Function: MD5 and MD6
○ Cipher Feedback (CFB) Mode	▪ Message Digest Function: Secure Hashing Algorithm (SHA)
○ Counter Mode	▪ RIPEMD-160
▪ Modes of Authenticated Encryption	▪ HMAC
○ Authenticated Encryption with Message Authentication Code (MAC)	▪ CHAP
○ Authenticated Encryption with Associated Data (AEAD)	▪ EAP
▪ Applications of Cryptography - Blockchain	▪ GOST – Hash Function
○ Types of Blockchain	▪ Message Digest Functions Calculators
Cryptography Tools	▪ Multi-layer Hashing Calculators
▪ MD5 and MD6 Hash Calculators	▪ Hardware-Based Encryption
▪ Hash Calculators for Mobile	▪ Quantum Cryptography
▪ Cryptography Tools	▪ Other Encryption Techniques
▪ Cryptography Tools for Mobile	▪ Cipher Modes of Operation
Public Key Infrastructure (PKI)	▪ Modes of Authenticated Encryption
▪ Public Key Infrastructure (PKI)	▪ Cryptography Tools
○ Certification Authorities	**Applications of Cryptography**
○ Signed Certificate (CA) Vs. Self Signed Certificate	▪ Public Key Infrastructure (PKI)
Email Encryption	▪ Certification Authorities

▪ Digital Signature	▪ Signed Certificate (CA) vs. Self-Signed Certificate
▪ Secure Sockets Layer (SSL)	▪ Digital Signature
▪ Transport Layer Security (TLS)	▪ Secure Sockets Layer (SSL)
▪ Cryptography Toolkits	▪ Transport Layer Security (TLS)
▪ Pretty Good Privacy (PGP)	▪ Cryptography Toolkits
▪ GNU Privacy Guard (CPG)	▪ Pretty Good Privacy (PGP)
▪ Web of Trust (WOT)	▪ GNU Privacy Guard (GPG)
▪ Encrypting Email Messages in Outlook	▪ Web of Trust (WOT)
○ S/MIME Encryption	▪ Encrypting Email Messages in Outlook
○ Microsoft 365 Message Encryption	▪ Signing/Encrypting Email Messages on Mac
▪ Signing/Encrypting Email Messages on Mac	▪ Encrypting/Decrypting Email Messages Using OpenPGP
▪ Encrypting/Decrypting Email Messages Using OpenPGP	▪ Email Encryption Tools
▪ Email Encryption Tools	▪ Disk Encryption
Disk Encryption	▪ Disk Encryption Tools
▪ Disk Encryption	▪ Disk Encryption Tools for Linux
▪ Disk Encryption Tools: VeraCrypt and Symantec Drive Encryption	▪ Disk Encryption Tools for macOS
▪ Disk Encryption Tools	▪ Blockchain
▪ Disk Encryption Tools for Linux	**Cryptanalysis**
▪ Disk Encryption Tools for macOS	▪ Cryptanalysis Methods
Cryptanalysis	▪ Cryptography Attacks
▪ Cryptanalysis Methods	▪ Code Breaking Methodologies
○ Quantum Cryptanalysis	▪ Brute-Force Attack
▪ Code Breaking Methodologies	▪ Birthday Attack
▪ Cryptography Attacks	▪ Birthday Paradox: Probability
○ Brute-Force Attack	▪ Brute-Forcing VeraCrypt Encryption
○ Birthday Attack	▪ Meet-in-the-Middle Attack on Digital Signature Schemes
○ Birthday Paradox: Probability	▪ Side-Channel Attack
○ Meet-in-the-Middle Attack on Digital Signature Schemes	▪ Hash Collision Attack
○ Side-Channel Attack	▪ DUHK Attack
○ Hash Collision Attack	▪ DROWN Attack
○ DUHK Attack	▪ Rainbow Table Attack
○ Rainbow Table Attack	▪ Related-Key Attack
○ Related-Key Attack	▪ Padding Oracle Attack
○ Padding Oracle Attack	▪ Attacks on Blockchain
○ DROWN Attack	▪ Quantum Computing Risks

▪ Cryptanalysis Tools	▪ Quantum Computing Attacks
▪ Online MD5 Decryption Tools	▪ Cryptanalysis Tools
Cryptography Attack Countermeasures	▪ Online MD5 Decryption Tools
▪ How to Defend Against Cryptographic Attacks	**Cryptography Attack Countermeasures**
▪ Key Stretching	▪ How to Defend Against Cryptographic Attacks
	▪ Key Stretching

Labs Comparison

The notations used:

1. **Red** points are new labs in CEHv13
2. **Blue** points are substantially modified labs in CEHv13
3. ~~**Striked**~~ labs are removed from CEHv12
4. Labs marked as **(Self-study)** will be available separately as the **CEH Self Study Upgrade Lab Pack**

CEHv12	CEHv13
Module 01: Introduction to Ethical Hacking	**Module 01: Introduction to Ethical Hacking**
Module 02: Footprinting and Reconnaissance	**Module 02: Footprinting and Reconnaissance**
1. Perform Footprinting Through Search Engines	1. Perform Footprinting Through Search Engines
1.1 Gather Information using Advanced Google Hacking Techniques	1.1 Gather Information using Advanced Google Hacking Techniques
1.2 Gather Information from Video Search Engines	1.2 Gather Information from Video Search Engines (Self-study)
1.3 Gather Information from FTP Search Engines	1.3 Gather Information from FTP Search Engines (Self-study)
1.4 Gather Information from IoT Search Engines	1.4 Gather Information from IoT Search Engines (Self-study)
2. Perform Footprinting Through Web Services	2. Perform Footprinting Through Internet Research Services
2.1 Find the Company's Domains and Sub-domains using Netcraft	2.1 Find the Company's Domains, Sub-domains and Hosts using Netcraft and DNSDumpster
2.2 Gather Personal Information using PeekYou Online People Search Service	2.2 Gather Personal Information using PeekYou Online People Search Service (Self-study)
~~2.3 Gather an Email List using theHarvester~~	2.3 Gather Information using Deep and Dark Web Searching (Self-study)
2.4 Gather Information using Deep and Dark Web Searching	2.4 Determine Target OS Through Passive Footprinting (Self-study)
2.5 Determine Target OS Through Passive Footprinting	3. Perform Footprinting Through Social Networking Sites
3. Perform Footprinting Through Social Networking Sites	3.1 Gather Personal Information from Various Social Networking Sites using Sherlock
~~3.1 Gather Employees' Information from LinkedIn using theHarvester~~	4. Perform Whois Footprinting
3.2 Gather Personal Information from Various Social Networking Sites using Sherlock	4.1 Perform Whois Lookup using DomainTools
~~3.3 Gather Information using Followerwonk~~	5. Perform DNS Footprinting

4. Perform Website Footprinting	5.1 Gather DNS Information using nslookup Command Line Utility and Online Tool
~~4.1 Gather Information About a Target Website using Ping Command Line Utility~~	5.2 Gather Information of Subdomain and DNS Records using SecurityTrails (Self-study)
~~4.2 Gather Information of a Target Website using Photon~~	5.3 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon (Self-study)
~~4.3 Gather information about a target website using Central Ops~~	6. Perform Network Footprinting
~~4.4 Extract a Company's Data using Web Data Extractor~~	6.1 Locate the Network Range (Self-study)
~~4.5 Mirror a Target Website using HTTrack Web Site Copier~~	6.2 Perform Network Tracerouting in Windows and Linux Machines
~~4.6 Gather Information About a Target Website using GRecon~~	7. Perform Email Footprinting
~~4.7 Gather a Wordlist from the Target Website using CeWL~~	7.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro
5. Perform Email Footprinting	7.2 Gather information About a Target Email using Holehe (Self-study)
5.6 Gather Information About a Target by Tracing Emails using eMailTrackerPro	8. Perform Footprinting using Various Footprinting Tools
6. Perform Whois Footprinting	8.1 Footprinting a Target using Recon-ng
6.3 Perform Whois Lookup using DomainTools	8.2 Footprinting a Target using Maltego (Self-study)
7. Perform DNS Footprinting	8.3 Footprinting a Target using FOCA (Self-study)
7.3 Gather DNS Information using nslookup Command Line Utility and Online Tool	8.4 Footprinting a Target using OSINT Framework (Self-study)
7.4 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon	8.5 Footprinting a Target using OSINT.SH (Self-study)
7.5 Gather Information of Subdomain and DNS Records using SecurityTrails	8.6 Footprinting a Target using Web Check (Self-study)
8. Perform Network Footprinting	9. Perform Footprinting using AI
8.1 Locate the Network Range	9.1 Footprinting a Target using Shellgpt
8.2 Perform Network Tracerouting in Windows and Linux Machines	
~~8.3 Perform Advanced Network Route Tracing using Path Analyzer Pro~~	
9. Perform Footprinting using Various Footprinting Tools	
9.2 Footprinting a Target using Recon-ng	
9.3 Footprinting a Target using Maltego	
~~9.4 Footprinting a Target using OSRFramework~~	

9.5 Footprinting a Target using FOCA	
~~9.6 Footprinting a Target using BillCipher~~	
9.7 Footprinting a Target using OSINT Framework	
Module 03: Scanning Networks	**Module 03: Scanning Networks**
1. Perform Host Discovery	1. Perform Host Discovery
1.1 Perform Host Discovery using Nmap	1.1 Perform Host Discovery using Nmap
1.2 Perform Host Discovery using Angry IP Scanner	1.2 Perform Host Discovery using Angry IP Scanner (Self-study)
2. Perform Port and Service Discovery	2. Perform Port and Service Discovery
2.1 Perform Port and Service Discovery using MegaPing	2.1 Perform Port and Service Discovery using MegaPing (Self-study)
2.2 Perform Port and Service Discovery using NetScanTools Pro	2.2 Perform Port and Service Discovery using NetScanTools Pro (Self-study)
2.3 Perform Port Scanning using sx Tool	2.3 Perform Port Scanning using sx Tool (Self-study)
2.4 Explore Various Network Scanning Techniques using Nmap	2.4 Explore Various Network Scanning Techniques using Nmap
2.5 Explore Various Network Scanning Techniques using Hping3	2.5 Explore Various Network Scanning Techniques using Hping3 (Self-study)
3. Perform OS Discovery	2.6 Scan a Target Network using Rustscan (Self-study)
3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark	3. Perform OS Discovery
3.2 Perform OS Discovery using Nmap Script Engine (NSE)	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark (Self-study)
~~3.3 Perform OS Discovery using Unicornscan~~	3.2 Perform OS Discovery using Nmap Script Engine (NSE)
4. Scan beyond IDS and Firewall	4. Scan beyond IDS and Firewall
4.1 Scan beyond IDS/Firewall using various Evasion Techniques	4.1 Scan beyond IDS/Firewall using various Evasion Techniques
4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall (Self-study)
4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond the IDS/Firewall (Self-study)
~~4.4 Browse Anonymously using Proxy Switcher~~	5. Perform Network Scanning using Various Scanning Tools

~~4.5 Browse Anonymously using CyberGhost VPN~~	5.1 Scan a Target Network using Metasploit
5. Perform Network Scanning using Various Scanning Tools	6. Perform Network Scanning using AI
5.1 Scan a Target Network using Metasploit	6.1 Scan a Target using ShellGPT
Module 04: Enumeration	**Module 04: Enumeration**
1. Perform NetBIOS Enumeration	1. Perform NetBIOS Enumeration
1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities
1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator (Self-study)
1.3 Perform NetBIOS Enumeration using an NSE Script	1.3 Perform NetBIOS Enumeration using an NSE Script (Self-study)
2. Perform SNMP Enumeration	2. Perform SNMP Enumeration
2.1 Perform SNMP Enumeration using snmp-check	2.1 Perform SNMP Enumeration using snmp-check (Self-study)
2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner (Self-study)
2.3 Perform SNMP Enumeration using SnmpWalk	2.3 Perform SNMP Enumeration using SnmpWalk
2.4 Perform SNMP Enumeration using Nmap	2.4 Perform SNMP Enumeration using Nmap (Self-study)
3. Perform LDAP Enumeration	3. Perform LDAP Enumeration
3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)
3.2 Perform LDAP Enumeration using Python and Nmap	3.2 Perform LDAP Enumeration using Python and Nmap (Self-study)
~~3.3 Perform LDAP Enumeration using ldapsearch~~	4. Perform NFS Enumeration
4. Perform NFS Enumeration	4.1 Perform NFS Enumeration using RPCScan and SuperEnum
4.1 Perform NFS Enumeration using RPCScan and SuperEnum	5. Perform DNS Enumeration
5. Perform DNS Enumeration	5.1 Perform DNS Enumeration using Zone Transfer
5.1 Perform DNS Enumeration using Zone Transfer	5.2 Perform DNS Enumeration using DNSSEC Zone Walking (Self-study)
5.2 Perform DNS Enumeration using DNSSEC Zone Walking	5.3 Perform DNS Enumeration using Nmap (Self-study)
5.3 Perform DNS Enumeration using Nmap	6. Perform SMTP Enumeration
6. Perform SMTP Enumeration	6.1 Perform SMTP Enumeration using Nmap
6.1 Perform SMTP Enumeration using Nmap	7. Perform RPC, SMB, and FTP Enumeration

7. Perform RPC, SMB, and FTP Enumeration	7.1 Perform SMB and RPC Enumeration using NetScanTools Pro (Self-study)
7.1 Perform RPC and SMB Enumeration using NetScanTools Pro	7.2 Perform SMB Enumeration using SMBeagle (Self-study)
7.2 Perform RPC, SMB, and FTP Enumeration using Nmap	7.3 Perform RPC, SMB, and FTP Enumeration using Nmap (Self-study)
8. Perform Enumeration using Various Enumeration Tools	8. Perform Enumeration using Various Enumeration Tools
8.1 Enumerate Information using Global Network Inventory	8.1 Enumerate Information using Global Network Inventory
~~8.2 Enumerate Network Resources using Advanced IP Scanner~~	8.2 Enumerate Information from Windows and Samba Hosts using Enum4linux (Self-study)
8.3 Enumerate Information from Windows and Samba Hosts using Enum4linux	9. Perform Enumeration using AI
	9.1 Perform Enumeration using ShellGPT
Module 05: Vulnerability Analysis	**Module 05: Vulnerability Analysis**
1. Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	1. Perform Vulnerability Research with Vulnerability Scoring Systems and Databases
1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)
1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE) (Self-study)
1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD) (Self-study)
2. Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	1.4 Perform Vulnerability Research using Searchsploit (Self-study)
2.1 Perform Vulnerability Analysis using OpenVAS	1.5 Perform Vulnerability Research using Vuldb (Self-study)
2.2 Perform Vulnerability Scanning using Nessus	2. Perform Vulnerability Assessment using Various Vulnerability Assessment Tools
~~2.3 Perform Vulnerability Scanning using GFI LanGuard~~	2.1 Perform Vulnerability Analysis using OpenVAS
~~2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto~~	2.2 Perform Vulnerability Scanning using Nessus (Self-study)
	2.2 Perform Vulnerability Scanning using Sniper (Self-study)
	3. Perform Vulnerability Analysis using AI
	3.1 Perform Vulnerability Analysis using ShellGPT

Module 06: System Hacking	Module 06: System Hacking
1. Gain Access to the System	1. Gain Access to the System
1.1 Perform Active Online Attack to Crack the System's Password using Responder	1.1 Perform Active Online Attack to Crack the System's Password using Responder
1.2 Audit System Passwords using L0phtCrack	1.2 Perform Active Online Attack to Crack the System's Password using NTLM Theft (Self-study)
1.3 Find Vulnerabilities on Exploit Sites	1.3 Audit System Passwords using L0phtCrack (Self-study)
1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	1.4 Find Vulnerabilities on Exploit Sites (Self-study)
~~1.5 Gain Access to a Remote System using Armitage~~	1.5 Exploit Client-Side Vulnerabilities and Establish a VNC Session (Self-study)
~~1.6 Gain Access to a Remote System using Ninja Jonin~~	1.6 Gain Access to a Remote System using Reverse Shell Generator
1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	1.7 Gain Access to a Remote System using Image File Dropper (Self-study)
2. Perform Privilege Escalation to Gain Higher Privileges	1.8 Perform Buffer Overflow Attack to Gain Access to a Remote System
2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities	2. Perform Privilege Escalation to Gain Higher Privileges
2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities (Self-study)
~~2.3 Escalate Privileges by Exploiting Vulnerability in pkexec~~	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter (Self-study)
~~2.4 Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS~~	2.3 Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys
2.5 Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys	2.4 Perform SSH-bruteforce Attack and Escalate Privileges by Exploiting Client-Side Vulnerabilities (Self-study)
2.6 Escalate Privileges to Gather Hashdump using Mimikatz	2.5 Escalate Privileges to Gather Hashdump using Mimikatz (Self-study)
3. Maintain Remote Access and Hide Malicious Activities	3. Maintain Remote Access and Hide Malicious Activities
~~3.1 User System Monitoring and Surveillance using Power Spy~~	3.1 User System Monitoring and Surveillance using Spyrix
~~3.2 User System Monitoring and Surveillance using Spytech SpyAgent~~	3.2 Hide Files using NTFS Streams (Self-study)
3.3 Hide Files using NTFS Streams	3.3 Image Steganography using OpenStego and StegOnline (Self-study)
~~3.4 Hide Data using White Space Steganography~~	3.4 Maintain Persistence by Abusing Boot or Logon Autostart Execution (Self-study)

3.5 Image Steganography using OpenStego and StegOnline	3.5 Maintain Persistence by Modifying Registry Run Keys
3.6 Maintain Persistence by Abusing Boot or Logon Autostart Execution	3.6 Gain Access using Havoc and Maintain Persistence using SharPersist (Self-study)
3.7 Maintain Domain Persistence by Exploiting Active Directory Objects	3.7 Maintain Domain Persistence by Exploiting Active Directory Objects (Self-study)
3.8 Privilege Escalation and Maintain Persistence using WMI	3.8 Privilege Escalation and Maintain Persistence using WMI (Self-study)
~~3.9 Covert Channels using Covert_TCP~~	4. Clear Logs to Hide the Evidence of Compromise
4. Clear Logs to Hide the Evidence of Compromise	4.1 View, Enable, and Clear Audit Policies using Auditpol (Self-study)
4.1 View, Enable, and Clear Audit Policies using Auditpol	4.2 Clear Windows Machine Logs using Various Utilities
4.2 Clear Windows Machine Logs using Various Utilities	4.3 Clear Linux Machine Logs using the BASH Shell
4.3 Clear Linux Machine Logs using the BASH Shell	4.4 Hiding Artifacts in Windows and Linux Machines (Self-study)
4.4 Hiding Artifacts in Windows and Linux Machines	5. Perform Various Attacks on AD Range
~~4.5 Clear Windows Machine Logs using CCleaner~~	5.1 Perform AD Attacks using various tools
	6. System Hacking using AI
	6.1 Perform System Hacking using ShellGPT
Module 07: Malware Threats	**Module 07: Malware Threats**
1. Gain Access to the Target System using Trojans	1. Gain Access to the Target System using Trojans
1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan
1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs (Self-study)
1.3 Create a Trojan Server using Theef RAT Trojan	1.3 Create a Trojan Server using Theef RAT Trojan (Self-study)
2. Infect the Target System using a Virus	2. Infect the Target System using Malware
2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System
3. Perform Static Malware Analysis	2.2 Create a Ransomware using Chaos Ransomware Builder and Infect the Target System (Self-study)
3.1 Perform Malware Scanning using Hybrid Analysis	3. Perform Static Malware Analysis
3.2 Perform a Strings Search using BinText	3.1 Perform Malware Scanning using Hybrid Analysis

3.3 Identify Packaging and Obfuscation Methods using PEid	3.2 Perform a Strings Search using BinText (Self-study)
3.4 Analyze ELF Executable File using Detect It Easy (DIE)	3.3 Identify Packaging and Obfuscation Methods using PEid (Self-study)
3.5 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer	3.4 Analyze ELF Executable File using Detect It Easy (DIE)
~~3.6 Identify File Dependencies using Dependency Walker~~	3.5 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer (Self-study)
3.7 Perform Malware Disassembly using IDA and OllyDbg	3.6 Extract and Analyze PE Headers using Pestudio (Self-study)
3.8 Perform Malware Disassembly using Ghidra	3.7 Perform Malware Disassembly using IDA and OllyDbg
4. Perform Dynamic Malware Analysis	3.8 Analyze Executable Files using capa (Self-study)
4.1 Perform Port Monitoring using TCPView and CurrPorts	3.9 Perform Malware Disassembly using Ghidra (Self-study)
4.2 Perform Process Monitoring using Process Monitor	4. Perform Dynamic Malware Analysis
4.3 Perform Registry Monitoring using Reg Organizer	4.1 Perform Port Monitoring using TCPView and CurrPorts
~~4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)~~	4.2 Perform Process Monitoring using Process Monitor
4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol	4.3 Perform Registry Monitoring using Reg Organizer (Self-study)
~~4.6 Perform Installation Monitoring using Mirekusoft Install Monitor~~	4.4 Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol (Self-study)
4.7 Perform Files and Folder Monitoring using PA File Sight	4.5 Perform Files and Folder Monitoring using PA File Sight (Self-study)
4.8 Perform Device Driver Monitoring using DriverView and Driver Reviver	4.6 Perform Device Driver Monitoring using DriverView and Driver Reviver (Self-study)
4.9 Perform DNS Monitoring using DNSQuerySniffer	4.7 Perform DNS Monitoring using DNSQuerySniffer (Self-study)
Module 08: Sniffing	**Module 08: Sniffing**
1. Perform Active Sniffing	1. Perform Active Sniffing
1.1 Perform MAC Flooding using macof	1.1 Perform MAC Flooding using macof
1.2 Perform a DHCP Starvation Attack using Yersinia	1.2 Perform a DHCP Starvation Attack using Yersinia
1.3 Perform ARP Poisoning using arpspoof	1.3 Perform ARP Poisoning using arpspoof (Self-study)
1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel (Self-study)

1.5 Spoof a MAC Address using TMAC and SMAC	1.5 Spoof a MAC Address using TMAC and SMAC (Self-study)
1.6 Spoof a MAC Address of Linux Machine using macchanger	1.6 Spoof a MAC Address of Linux Machine using macchanger (Self-study)
2. Perform Network Sniffing using Various Sniffing Tools	2. Perform Network Sniffing using Various Sniffing Tools
2.1 Perform Password Sniffing using Wireshark	2.1 Perform Password Sniffing using Wireshark
2.2 Analyze a Network using the Omnipeek Network Protocol Analyzer	2.2 Analyze a Network using the Omnipeek Network Protocol Analyzer (Self-study)
~~2.3 Analyze a Network using the SteelCentral Packet Analyzer~~	3. Detect Network Sniffing
3. Detect Network Sniffing	3.1 Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network
3.1 Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network	3.2 Detect ARP Poisoning using the Capsa Network Analyzer (Self-study)
3.2 Detect ARP Poisoning using the Capsa Network Analyzer	
Module 09: Social Engineering	**Module 09: Social Engineering**
1. Perform Social Engineering using Various Techniques	1. Perform Social Engineering using Various Techniques
1.1 Sniff Credentials using the Social-Engineer Toolkit (SET)	1.1 Sniff Credentials using the Social-Engineer Toolkit (SET)
2. Detect a Phishing Attack	1.2 Sniff Credentials using Dark-Phish (Self-study)
2.1 Detect Phishing using Netcraft	2. Detect a Phishing Attack
2.2 Detect Phishing using PhishTank	2.1 Detect Phishing using Netcraft
~~3. Audit Organization's Security for Phishing Attacks~~	2.2 Detect Phishing using PhishTank (Self-study)
~~3.1 Audit Organization's Security for Phishing Attacks using OhPhish~~	3. Social Engineering using AI
	3.1 Craft Phishing Emails with ChatGPT
Module 10: Denial-of-Service	**Module 10: Denial-of-Service**
1. Perform DoS and DDoS Attacks using Various Techniques	1. Perform DoS and DDoS Attacks using Various Techniques
1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit (Self-study)
1.2 Perform a DoS Attack on a Target Host using hping3	1.2 Perform a DoS Attack on a Target Host using hping3 (Self-study)
~~1.3 Perform a DoS Attack using Raven-storm~~	1.3 Perform a DDoS Attack using HOIC (Self-study)

1.4 Perform a DDoS Attack using HOIC	1.4 Perform a DDoS Attack using LOIC (Self-study)
1.5 Perform a DDoS Attack using LOIC	1.5 Perform a DDoS Attack using PyDDos and PyFloodder (Self-study)
2. Detect and Protect Against DoS and DDoS Attacks	1.6 Perform a DDoS attack using ISB and UltraDDOS-v2 tools
2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian	1.7 Perform a DDoS Attack using Botnet
	2. Detect and Protect Against DoS and DDoS Attacks
	2.1 Detect and Protect against DDoS Attacks using Anti DDoS Guardian
Module 11: Session Hijacking	**Module 11: Session Hijacking**
1. Perform Session Hijacking	1. Perform Session Hijacking
~~1.1 Hijack a Session using Zed Attack Proxy (ZAP)~~	1.1 Hijack a Session using Caido
1.2 Intercept HTTP Traffic using bettercap	1.2 Intercept HTTP Traffic using bettercap (Self-study)
1.3 Intercept HTTP Traffic using Hetty	1.3 Intercept HTTP Traffic using Hetty
2. Detect Session Hijacking	2. Detect Session Hijacking
2.1 Detect Session Hijacking using Wireshark	2.1 Detect Session Hijacking using Wireshark
Module 12: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
1. Perform Intrusion Detection using Various Tools	1. Perform Intrusion Detection using Various Tools
1.1 Detect Intrusions using Snort	1.1 Detect Intrusions using Snort
1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL (Self-study)
1.3 Detect Malicious Network Traffic using HoneyBOT	1.3 Detect Malicious Network Traffic using HoneyBOT (Self-study)
2. Evade Firewalls using Various Evasion Techniques	1.4 Deploy Cowrie Honeypot to Detect Malicious Network Traffic
~~2.1 Bypass Windows Firewall using Nmap Evasion Techniques~~	2. Evade IDS/Firewalls using Various Evasion Techniques
2.2 Bypass Firewall Rules using HTTP/FTP Tunneling	2.1 Bypass Firewall Rules using HTTP/FTP Tunneling (Self-study)
2.3 Bypass Antivirus using Metasploit Templates	2.2 Bypass Antivirus using Metasploit Templates (Self-study)
	2.3 Evade Firewall through Windows BITSAdmin

Module 13: Hacking Web Servers	**Module 13: Hacking Web Servers**
1. Footprint the Web Server	1. Footprint the Web Server
1.1 Information Gathering using Ghost Eye	1.1 Information Gathering using Ghost Eye (Self-study)
1.2 Perform Web Server Reconnaissance using Skipfish	1.2 Perform Web Server Reconnaissance using Skipfish (Self-study)
~~1.3 Footprint a Web Server using the httprecon Tool~~	1.3 Footprint a Web Server using Netcat and Telnet
~~1.4 Footprint a Web Server using ID Serve~~	1.4 Enumerate Web Server Information using Nmap Scripting Engine (NSE)
1.5 Footprint a Web Server using Netcat and Telnet	1.5 Uniscan Web Server Fingerprinting in Parrot Security (Self-study)
1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	2. Perform a Web Server Attack
1.7 Uniscan Web Server Fingerprinting in Parrot Security	2.1 Crack FTP Credentials using a Dictionary Attack
2. Perform a Web Server Attack	2.2 Exploit the MSSQL Service using xp_cmdshell Function (Self-study)
2.1 Crack FTP Credentials using a Dictionary Attack	2.3 Gain Access to Target Web Server by Exploiting Log4j Vulnerability
	3. Perform a Web Server Hacking using AI
	3.1 Perform webserver footprinting and attacks using ShellGPT
Module 14: Hacking Web Applications	**Module 14: Hacking Web Applications**
1. Footprint the Web Infrastructure	1. Footprint the Web Infrastructure
1.1 Perform Web Application Reconnaissance using Nmap and Telnet	1.1 Perform Web Application Reconnaissance using Nmap and Telnet
1.2 Perform Web Application Reconnaissance using WhatWeb	1.2 Perform Web Application Reconnaissance using WhatWeb (Self-study)
1.3 Perform Web Spidering using OWASP ZAP	1.3 Perform Web Spidering using OWASP ZAP
1.4 Detect Load Balancers using Various Tools	1.4 Detect Load Balancers using Various Tools (Self-study)
1.5 Identify Web Server Directories using Various Tools	1.5 Identify Web Server Directories using Various Tools (Self-study)
~~1.6 Perform Web Application Vulnerability Scanning using Vega~~	1.6 Perform Web Application Vulnerability Scanning using SmartScanner
1.7 Identify Clickjacking Vulnerability using ClickjackPoc	1.7 Identify Clickjacking Vulnerability using ClickjackPoc (Self-study)
2. Perform Web Application Attacks	2. Perform Web Application Attacks
2.1 Perform a Brute-force Attack using Burp Suite	2.1 Perform a Brute-force Attack using Burp Suite
2.2 Perform Parameter Tampering using Burp Suite	2.2 Perform Parameter Tampering using Burp Suite (Self-study)

2.3 Identifying XSS Vulnerabilities in Web Applications using PwnXSS	2.3 Identify XSS Vulnerabilities in Web Applications using PwnXSS (Self-study)
2.4 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications	2.4 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications (Self-study)
2.5 Perform Cross-Site Request Forgery (CSRF) Attack	2.5 Perform Cross-site Request Forgery (CSRF) Attack (Self-study)
2.6 Enumerate and Hack a Web Application using WPScan and Metasploit	2.6 Perform Remote Code Execution (RCE) Attack
2.7 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server	2.7 Enumerate and Hack a Web Application using WPScan and Metasploit (Self-study)
2.8 Exploit a File Upload Vulnerability at Different Security Levels	2.8 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server (Self-study)
2.9 Gain Access by exploiting Log4j Vulnerability	2.9 Exploit a File Upload Vulnerability at Different Security Levels (Self-study)
3. Detect Web Application Vulnerabilities using Various Web Application Security Tools	2.10 Perform JWT Token Attack (Self-study)
3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner	3. Detect Web Application Vulnerabilities using Various Web Application Security Tools
	3.1 Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner
	4. Perform Web Application Hacking using AI
	4.1 Perform Web Application Hacking using ShellGPT
Module 15: SQL Injection	**Module 15: SQL Injection**
1. Perform SQL Injection Attacks	1. Perform SQL Injection Attacks
1.1 Perform an SQL Injection Attack on an MSSQL Database	1.1 Perform an SQL Injection Attack on an MSSQL Database (Self-study)
1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap
2. Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	1.3 Perform an SQL Injection to Launch File Inclusion Attack on bWAPP (Self-study)
~~2.1 Detect SQL Injection Vulnerabilities using DSSS~~	2. Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools
2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP	2.1 Detect SQL Injection Vulnerabilities using OWASP ZAP
	2.2 Detect SQL Injection Vulnerabilities using Ghauri (Self-study)

	3. Perform SQL Injection using AI
	3.1 Perform SQL Injection using ShellGPT
Module 16: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
1. Footprint a Wireless Network	1. Footprint a Wireless Network
~~1.1 Find Wi-Fi Networks in Range using NetSurveyor~~	1.1 Find Wi-Fi Networks in Range using Sparrow-wifi (Self-study)
2. Perform Wireless Traffic Analysis	2. Perform Wireless Traffic Analysis
2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark
3. Perform Wireless Attacks	3. Perform Wireless Attacks
~~3.1 Find Hidden SSIDs using Aircrack-ng~~	3.1 Find Hidden SSID using MDK (Self-study)
~~3.2 Crack a WEP Network using Wifiphisher~~	3.2 Crack a WPA2 Network using Aircrack-ng
~~3.3 Crack a WEP Network using Aircrack-ng~~	3.3 Create a Rogue Access Point to Capture Data Packets (Self-study)
~~3.4 Crack a WPA Network using Fern Wifi Cracker~~	
3.5 Crack a WPA2 Network using Aircrack-ng	
3.6 Create a Rogue Access Point to Capture Data Packets	
Module 17: Hacking Mobile Platforms	**Module 17: Hacking Mobile Platforms**
1. Hack Android Devices	1. Hack Android Devices
1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security (Self-study)
1.2 Harvest Users' Credentials using the Social-Engineer Toolkit	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit (Self-study)
1.3 Launch a DoS Attack on a Target Machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform	1.3 Launch a DoS Attack on a Target Machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform (Self-study)
1.4 Exploit the Android Platform through ADB using PhoneSploit	1.4 Exploit the Android Platform through ADB using PhoneSploit-Pro
1.5 Hack an Android Device by Creating APK File using AndroRAT	1.5 Hack an Android Device by Creating APK File using AndroRAT
2. Secure Android Devices using Various Android Security Tools	2. Secure Android Devices using Various Android Security Tools
~~2.1 Analyze a Malicious App using Online Android Analyzers~~	2.1 Secure Android Devices from Malicious Apps using AVG
~~2.2 Secure Android Devices from Malicious Apps using Malwarebytes Security~~	

Module 18: IoT and OT Hacking	**Module 18: IoT and OT Hacking**
1. Perform Footprinting using Various Footprinting Techniques	1. Perform Footprinting using Various Footprinting Techniques
1.1 Gather Information using Online Footprinting Tools	1.1 Gather Information using Online Footprinting Tools
2. Capture and Analyze IoT Device Traffic	2. Capture and Analyze IoT Device Traffic
2.1 Capture and Analyze IoT Traffic using Wireshark	2.1 Capture and Analyze IoT Traffic using Wireshark
	3. Perform IoT Attacks
	3.1 Hacking into VoIP based device (Self-study)
	3.2 Perform Replay Attack on CAN Protocol
Module 19: Cloud Computing	**Module 19: Cloud Computing**
1. Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools	1. Perform Reconnaissance
1.1 Enumerate S3 Buckets using lazys3	1.1 Azure Reconnaissance with AADInternals
~~1.2 Enumerate S3 Buckets using S3Scanner~~	2. Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools
~~1.3 Enumerate S3 Buckets using Firefox Extension~~	2.1 Enumerate S3 Buckets using lazys3 (Self-study)
2. Exploit S3 Buckets	2.2 Enumerate S3 Buckets using Grayhatwarfare (Self-study)
2.1 Exploit Open S3 Buckets using AWS CLI	2.3 Enumerate S3 Buckets using Cloudbrute (Self-study)
3. Perform Privilege Escalation to Gain Higher Privileges	3. Exploit S3 Buckets
3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy	3.1 Exploit Open S3 Buckets using AWS CLI
	3.2 Exploit Open S3 Buckets using Bucket Flaws (Self-study)
	4. Perform Privilege Escalation to Gain Higher Privileges
	4.1 Enumeration for Privilege Escalation using Cloudfox (Self-study)
	4.2 Escalate IAM User Privileges by Exploiting Misconfigured User Policy
	5. Perform vulnerability assessment on docker images
	5.1 Vulnerability Assessment on Docker Images using Trivy

Module 20: Cryptography	**Module 20: Cryptography**
1. Encrypt the Information using Various Cryptography Tools	1. Encrypt the Information using Various Cryptography Tools
~~1.1 Calculate One-way Hashes using HashCalc~~	1.1 Perform Multi-layer Hashing using CyberChef
1.2 Calculate MD5 Hashes using MD5 Calculator	1.2 Calculate MD5 Hashes using MD5 Calculator (Self-study)
1.3 Calculate MD5 Hashes using HashMyFiles	1.3 Calculate MD5 Hashes using HashMyFiles (Self-study)
1.4 Perform File and Text Message Encryption using CryptoForge	1.4 Perform File and Text Message Encryption using CryptoForge
~~1.5 Perform File Encryption using Advanced Encryption Package~~	1.5 Encrypt and Decrypt Data using BCTextEncoder (Self-study)
1.6 Encrypt and Decrypt Data using BCTextEncoder	2. Create a Self-Signed Certificate
2. Create a Self-Signed Certificate	2.1 Create and Use Self-signed Certificates
2.1 Create and Use Self-signed Certificates	3. Perform Email Encryption
3. Perform Email Encryption	3.1 Perform Email Encryption using RMail (Self-study)
3.1 Perform Email Encryption using Rmail	3.2 Perform Email Encryption using Mailvelope (Self-study)
4. Perform Disk Encryption	4. Perform Disk Encryption
4.1 Perform Disk Encryption using VeraCrypt	4.1 Perform Disk Encryption using VeraCrypt
4.2 Perform Disk Encryption using BitLocker Drive Encryption	4.2 Perform Disk Encryption using BitLocker Drive Encryption (Self-study)
4.3 Perform Disk Encryption using Rohos Disk Encryption	4.3 Perform Disk Encryption using Rohos Disk Encryption (Self-study)
5. Perform Cryptanalysis using Various Cryptanalysis Tools	5. Perform Cryptanalysis using Various Cryptanalysis Tools
5.1 Perform Cryptanalysis using CrypTool	5.1 Perform Cryptanalysis using CrypTool (Self-study)
~~5.2 Perform Cryptanalysis using AlphaPeeler~~	6. Perform Cryptography using AI
	6.1 Perform Cryptographic Techniques using ShellGPT