Ethical Hacking and Countermeasures

Version Comparison

	CEHv10	CEHv11
Total Number of Modules	**20**	**20**
Total Number of Slides	**1500**	**1640**
Total Number of Labs	**140**	**200**
Total Number of New Labs	**-**	**92**
Attack Techniques	**340**	**420**
Total Number of Tools	**2285 (Approx.)**	**3500 (Approx.)**
New Technology Added	**IoT**	**OT Technology, Serverless Computing, WPA3 Encryption, APT, Fileless Malware, Web API, and Web Shell**
OS Used for Labs	**Windows 10, Windows Server 2016, Windows Server 2012, Kali Linux 2017.3, Windows 8.1, Android, Ubuntu Linux**	**Windows 10, Windows Server 2019, Windows Server 2016, 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	**NICE 2.0 Draft Framework**	**Final NICE 2.0 Framework**

CEHv11 Change Summary

1. The Module 18: IoT and OT Hacking is a completely modified module in CEHv11 which inclues OT hacking (OT concepts, attacks, hacking methodology, hacking tools, and countermeasures)
2. The Module 19: Cloud Computing is a completely modified module in CEHv11 which inclues container technology, serverless computing, and cloud hacking methodology
3. The Module 14: Hacking Web Applications module includes web API, webhooks and web shell concepts, web API hacking methodology, and web API security in CEHv11
4. The Module 06: System Hacking module includes vulnerability exploitation (buffer overflow) in CEHv11
5. The Module 07: Malware Threats module includes APT and fileless malware concepts in CEHv11
6. The Module 04: Enumeration module includes NFS, Telnet, SMB, FTP, TFTP, IPv6, and BGP enumeration techniques in CEHv11
7. Update information as per the latest developments with a proper flow
8. Latest OS covered and a patched testing environment
9. All the tool screenshots are replaced with the latest version
10. All the tool listing slides are updated with the latest tools

Module Comparison

CEHv10	CEHv11
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 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 CEHv11
2. **Blue** points are substantially modified in CEHv11
3. ~~**Striked**~~ points are removed from CEHv10
4. ~~**Striked**~~ points are moved to self study module in CEHv11

CEHv10	CEHv11
Module 01: Introduction to Ethical Hacking	**Module 01: Introduction to Ethical Hacking**
Information Security Overview	**Information Security Overview**
~~▪ Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds~~	▪ Elements of Information Security
~~▪ Essential Terminology~~	▪ Motives, Goals, and Objectives of Information Security Attacks
~~▪ Elements of Information Security~~	▪ Classification of Attacks
~~▪ The Security, Functionality, and Usability Triangle~~	▪ Information Warfare
Information Security Threats and Attack Vectors	**Cyber Kill Chain Concepts**
▪ Motives, Goals, and Objectives of Information Security Attacks	▪ Cyber Kill Chain Methodology
~~▪ Top Information Security Attack Vectors~~	▪ Tactics, Techniques, and Procedures (TTPs)
~~▪ Information Security Threat Categories~~	▪ Adversary Behavioral Identification
~~▪ Types of Attacks on a System~~	▪ Indicators of Compromise (IoCs)
▪ Information Warfare	○ Categories of Indicators of Compromise
Hacking Concepts	**Hacking Concepts**
▪ What is Hacking?	▪ What is Hacking?
▪ Who is a Hacker?	▪ Who is a Hacker?
▪ Hacker Classes	▪ Hacker Classes
▪ Hacking Phases	▪ Hacking Phases
○ Reconnaissance	○ Reconnaissance
○ Scanning	○ Scanning
○ Gaining Access	○ Gaining Access
○ Maintaining Access	○ Maintaining Access
○ Clearing Tracks	○ Clearing Tracks
Ethical Hacking Concepts	**Ethical Hacking Concepts**
▪ What is Ethical Hacking?	▪ What is Ethical Hacking?
▪ Why Ethical Hacking is Necessary	▪ Why Ethical Hacking is Necessary
▪ Scope and Limitations of Ethical Hacking	▪ Scope and Limitations of Ethical Hacking

▪ Skills of an Ethical Hacker	▪ Skills of an Ethical Hacker
Information Security Controls	**Information Security Controls**
▪ Information Assurance (IA)	▪ Information Assurance (IA)
~~▪ Information Security Management Program~~	▪ Defense-in-Depth
~~▪ Enterprise Information Security Architecture (EISA)~~	▪ What is Risk?
~~▪ Network Security Zoning~~	○ Risk Management
▪ Defense-in-Depth	▪ Cyber Threat Intelligence
~~▪ Information Security Policies~~	▪ Threat Modeling
~~○ Types of Security Policies~~	▪ Incident Management
~~○ Examples of Security Policies~~	○ Incident Handling and Response
~~○ Privacy Policies at Workplace~~	▪ Role of AI and ML in Cyber Security
~~○ Steps to Create and Implement Security Policies~~	○ How Do AI and ML Prevent Cyber Attacks?
~~○ HR/Legal Implications of Security Policy Enforcement~~	**Information Security Laws and Standards**
~~▪ Physical Security~~	▪ Payment Card Industry Data Security Standard (PCI DSS)
~~○ Types of Physical Security Control~~	▪ ISO/IEC 27001:2013
~~○ Physical Security Controls~~	▪ Health Insurance Portability and Accountability Act (HIPAA)
▪ What is Risk?	▪ Sarbanes Oxley Act (SOX)
○ Risk Management	▪ The Digital Millennium Copyright Act (DMCA)
~~○ Key Roles and Responsibilities in Risk Management~~	▪ The Federal Information Security Management Act (FISMA)
▪ Threat Modeling	▪ Cyber Law in Different Countries
▪ Incident Management	
~~○ Incident Management Process~~	
~~○ Responsibilities of an Incident Response Team~~	
~~▪ Security Incident and Event Management (SIEM)~~	
~~○ SIEM Architecture~~	
~~▪ User Behavior Analytics (UBA)~~	
~~▪ Network Security Controls~~	
~~○ Access Control~~	
~~○ Types of Access Control~~	
~~○ User Identification, Authentication, Authorization and Accounting~~	
~~▪ Identity and Access Management (IAM)~~	
~~▪ Data Leakage~~	
~~○ Data Leakage Threats~~	

~~○ What is Data Loss Prevention (DLP)?~~	
~~▪ Data Backup~~	
~~▪ Data Recovery~~	
▪ Role of AI/ML in Cyber Security	
~~**Penetration Testing Concepts**~~	
~~▪ Penetration Testing~~	
~~▪ Why Penetration Testing~~	
~~▪ Comparing Security Audit, Vulnerability Assessment, and Penetration Testing~~	
~~▪ Blue Teaming/Red Teaming~~	
~~▪ Types of Penetration Testing~~	
~~▪ Phases of Penetration Testing~~	
~~▪ Security Testing Methodology~~	
Information Security Laws and Standards	
▪ Payment Card Industry Data Security Standard (PCI-DSS)	
▪ ISO/IEC 27001:2013	
▪ Health Insurance Portability and Accountability Act (HIPAA)	
▪ Sarbanes Oxley Act (SOX)	
▪ The Digital Millennium Copyright Act (DMCA)	
▪ Federal Information Security Management Act (FISMA)	
▪ Cyber Law in Different Countries	
Module 02: Footprinting and Reconnaissance	**Module 02: Footprinting and Reconnaissance**
Footprinting Concepts	**Footprinting Concepts**
▪ What is Footprinting?	▪ What is Footprinting?
▪ Objectives of Footprinting	**Footprinting through Search Engines**
Footprinting through Search Engines	▪ Footprinting through Search Engines
▪ Footprinting through Search Engines	▪ Footprint Using Advanced Google Hacking Techniques
▪ Footprint Using Advanced Google Hacking Techniques	▪ Google Hacking Database
▪ Information Gathering Using Google Advanced Search and Image Search	▪ VoIP and VPN Footprinting through Google Hacking Database
▪ Google Hacking Database	▪ Other Techniques for Footprinting through Search Engines
▪ VoIP and VPN Footprinting through Google Hacking Database	○ Gathering Information Using Google Advanced Search and Advanced Image Search
Footprinting through Web Services	○ Gathering Information Using Reverse Image

	Search
▪ Finding Company's Top-level Domains (TLDs) and Sub-domains	○ Gathering Information Using Video Search Engines
▪ Finding the Geographical Location of the Target	○ Gathering Information Using Meta Search Engines
▪ People Search on Social Networking Sites and People Search Services	○ Gathering Information Using FTP Search Engines
▪ Gathering Information from LinkedIn	○ Gathering Information Using IoT Search Engines
▪ Gather Information from Financial Services	**Footprinting through Web Services**
▪ Footprinting through Job Sites	▪ Finding a Company's Top-Level Domains (TLDs) and Sub-domains
▪ Monitoring Target Using Alerts	▪ Finding the Geographical Location of the Target
▪ Information Gathering Using Groups, Forums, and Blogs	▪ People Search on Social Networking Sites and People Search Services
▪ Determining the Operating System	▪ Gathering Information from LinkedIn
▪ VoIP and VPN Footprinting through SHODAN	▪ Harvesting Email Lists
Footprinting through Social Networking Sites	▪ Gather Information from Financial Services
▪ Collecting Information through Social Engineering on Social Networking Sites	▪ Footprinting through Job Sites
Website Footprinting	▪ Deep and Dark Web Footprinting
▪ Website Footprinting	▪ Determining the Operating System
▪ Website Footprinting using Web Spiders	▪ VoIP and VPN Footprinting through SHODAN
▪ Mirroring Entire Website	▪ Competitive Intelligence Gathering
▪ Extracting Website Information from https://archive.org	○ Competitive Intelligence - When Did this Company Begin? How Did it Develop?
▪ Extracting Metadata of Public Documents	○ Competitive Intelligence - What Are the Company's Plans?
▪ Monitoring Web Pages for Updates and Changes	○ Competitive Intelligence - What Expert Opinions Say About the Company
Email Footprinting	▪ Other Techniques for Footprinting through Web Services
▪ Tracking Email Communications	○ Information Gathering Using Business Profile Sites
▪ Collecting Information from Email Header	○ Monitoring Target Using Alerts
▪ Email Tracking Tools	○ Tracking Online Reputation of the Target
Competitive Intelligence	○ Information Gathering Using Groups, Forums, and Blogs
▪ Competitive Intelligence Gathering	○ Information Gathering Using NNTP Usenet Newsgroups
▪ Competitive Intelligence - When Did this Company Begin? How Did it Develop?	**Footprinting through Social Networking Sites**
▪ Competitive Intelligence - What Are the	▪ Collecting Information through Social Engineering

Company's Plans?	on Social Networking Sites
▪ Competitive Intelligence - What Expert Opinions Say About the Company	▪ General Resources for Locating Information from Social Media Sites
▪ Monitoring Website Traffic of Target Company	▪ Conducting Location Search on Social Media Sites
▪ Tracking Online Reputation of the Target	▪ Tools for Footprinting through Social Networking Sites
Whois Footprinting	**Website Footprinting**
▪ Whois Lookup	▪ Website Footprinting
▪ Whois Lookup Result Analysis	▪ Website Footprinting using Web Spiders
▪ Whois Lookup Tools	▪ Mirroring Entire Website
▪ Finding IP Geolocation Information	▪ Extracting Website Information from https://archive.org
DNS Footprinting	▪ Extracting Website Links
▪ Extracting DNS Information	▪ Gathering Wordlist from the Target Website
▪ DNS Interrogation Tools	▪ Extracting Metadata of Public Documents
Network Footprinting	▪ Other Techniques for Website Footprinting
▪ Locate the Network Range	○ Monitoring Web Pages for Updates and Changes
▪ Traceroute	○ Searching for Contact Information, Email Addresses and Telephone Numbers from Company Website
▪ Traceroute Analysis	○ Searching for Web Pages Posting Patterns and Revision Numbers
▪ Traceroute Tools	○ Monitoring Website Traffic of Target Company
Footprinting through Social Engineering	**Email Footprinting**
▪ Footprinting through Social Engineering	▪ Tracking Email Communications
▪ Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving	▪ Email Tracking Tools
Footprinting Tools	**Whois Footprinting**
▪ Maltego	▪ Whois Lookup
▪ Recon-ng	▪ Finding IP Geolocation Information
▪ FOCA	**DNS Footprinting**
▪ Recon-Dog	▪ Extracting DNS Information
▪ OSRFramework	▪ Reverse DNS Lookup
▪ Additional Footprinting Tools	**Network Footprinting**
Countermeasures	▪ Locate the Network Range
▪ Footprinting Countermeasures	▪ Traceroute
~~**Footprinting Pen Testing**~~	▪ Traceroute Analysis
~~▪ Footprinting Pen Testing~~	▪ Traceroute Tools
~~▪ Footprinting Pen Testing Report Templates~~	**Footprinting through Social Engineering**
	▪ Footprinting through Social Engineering

	▪ Collect Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation
	Footprinting Tools
	▪ Maltego
	▪ Recon-ng
	▪ FOCA
	▪ OSRFramework
	▪ OSINT Framework
	▪ Recon-Dog
	▪ BillCipher
	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
▪ Creating Custom Packet Using TCP Flags	**Scanning Tools**
▪ Scanning in IPv6 Networks	▪ Nmap
Scanning Tools	▪ Hping2/Hping3
▪ Nmap	○ Hping Commands
▪ Hping2 / Hping3	▪ Scanning Tools
○ Hping Commands	▪ Scanning Tools for Mobile
▪ Scanning Tools	**Host Discovery**
▪ Scanning Tools for Mobile	▪ Host Discovery Techniques
Scanning Techniques	○ ARP Ping Scan and UDP Ping Scan
▪ Scanning Techniques	○ ICMP ECHO Ping Scan
○ ICMP Scanning - Checking for Live Systems	○ ICMP ECHO Ping Sweep
○ Ping Sweep - Checking for Live Systems	• Ping Sweep Tools
• Ping Sweep Tools	• Ping Sweep Countermeasures
○ ICMP Echo Scanning	○ Other Host Discovery Techniques
○ TCP Connect / Full Open Scan	• ICMP Timestamp and Address Mask Ping Scan
○ Stealth Scan (Half-open Scan)	• TCP Ping Scan
○ Inverse TCP Flag Scanning	✓ TCP SYN Ping Scan
○ Xmas Scan	✓ TCP ACK Ping Scan
○ ACK Flag Probe Scanning	• IP Protocol Ping Scan

○ IDLE/IPID Header Scan	**Port and Service Discovery**
○ UDP Scanning	▪ Port Scanning Techniques
○ SSDP and List Scanning	○ TCP Scanning
▪ Port Scanning Countermeasures	• TCP Connect/Full Open Scan
Scanning Beyond IDS and Firewall	• Stealth Scan (Half-open Scan)
▪ IDS/Firewall Evasion Techniques	• Inverse TCP Flag Scan
○ Packet Fragmentation	• Xmas Scan
○ Source Routing	• TCP Maimon Scan
○ IP Address Decoy	• ACK Flag Probe Scan
○ IP Address Spoofing	• IDLE/IPID Header Scan
• IP Spoofing Detection Techniques: Direct TTL Probes	○ UDP Scanning
• IP Spoofing Detection Techniques: IP Identification Number	○ SCTP Scanning
• IP Spoofing Detection Techniques: TCP Flow Control Method	• SCTP INIT Scanning
• IP Spoofing Countermeasures	• SCTP COOKIE ECHO Scanning
○ Proxy Servers	○ SSDP and List Scanning
• Proxy Chaining	○ IPv6 Scanning
• Proxy Tools	▪ Service Version Discovery
• Proxy Tools for Mobile	▪ Nmap Scan Time Reduction Techniques
○ Anonymizers	▪ Port Scanning Countermeasures
• Censorship Circumvention Tools: Alkasir and Tails	**OS Discovery (Banner Grabbing/OS Fingerprinting)**
• Anonymizers	▪ OS Discovery/Banner Grabbing
• Anonymizers for Mobile	▪ How to Identify Target System OS
Banner Grabbing	○ OS Discovery using Wireshark
▪ Banner Grabbing	○ OS Discovery using Nmap and Unicornscan
▪ How to Identify Target System OS	○ OS Discovery using Nmap Script Engine
▪ Banner Grabbing Countermeasures	○ OS Discovery using IPv6 Fingerprinting
Draw Network Diagrams	▪ Banner Grabbing Countermeasures
▪ Drawing Network Diagrams	**Scanning Beyond IDS and Firewall**
▪ Network Discovery and Mapping Tools	▪ IDS/Firewall Evasion Techniques
▪ Network Discovery Tools for Mobile	○ Packet Fragmentation
~~**Scanning Pen Testing**~~	○ Source Routing
~~▪ Scanning Pen Testing~~	○ Source Port Manipulation
	○ IP Address Decoy
	○ IP Address Spoofing
	• IP Spoofing Detection Techniques: Direct

	TTL Probes
	• IP Spoofing Detection Techniques: IP Identification Number
	• IP Spoofing Detection Techniques: TCP Flow Control Method
	• IP Spoofing Countermeasures
	○ Creating Custom Packets
	• Using Packet Crafting Tools
	• Appending Custom Binary Data
	• Appending Custom String
	• Appending Random Data
	○ Randomizing Host Order and Sending Bad Checksums
	○ Proxy Servers
	• Proxy Chaining
	• Proxy Tools
	• Proxy Tools for Mobile
	○ Anonymizers
	• Censorship Circumvention Tools: Alkasir and Tails
	• Anonymizers
	• Anonymizers for Mobile
	Draw Network Diagrams
	▪ Drawing Network Diagrams
	▪ Network Discovery and Mapping Tools
	▪ Network Discovery Tools for Mobile
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
▪ NetBIOS Enumeration Tools	▪ NetBIOS Enumeration Tools
▪ Enumerating User Accounts	▪ Enumerating User Accounts
▪ Enumerating Shared Resources Using Net View	▪ Enumerating Shared Resources Using Net View
SNMP Enumeration	**SNMP Enumeration**
▪ SNMP (Simple Network Management Protocol)	▪ SNMP (Simple Network Management Protocol)

Enumeration	Enumeration
▪ Working of SNMP	▪ Working of SNMP
▪ Management Information Base (MIB)	▪ Management Information Base (MIB)
▪ SNMP Enumeration Tools	▪ SNMP Enumeration Tools
LDAP Enumeration	**LDAP Enumeration**
▪ LDAP Enumeration	▪ LDAP Enumeration
▪ LDAP Enumeration Tools	▪ LDAP Enumeration Tools
NTP Enumeration	**NTP and NFS Enumeration**
▪ NTP Enumeration	▪ NTP Enumeration
▪ NTP Enumeration Commands	▪ NTP Enumeration Commands
▪ NTP Enumeration Tools	▪ NTP Enumeration Tools
SMTP and DNS Enumeration	▪ NFS Enumeration
▪ SMTP Enumeration	▪ NFS Enumeration Tools
▪ SMTP Enumeration Tools	**SMTP and DNS Enumeration**
▪ DNS Enumeration Using Zone Transfer	▪ SMTP Enumeration
Other Enumeration Techniques	▪ SMTP Enumeration Tools
▪ IPsec Enumeration	▪ DNS Enumeration Using Zone Transfer
▪ VoIP Enumeration	▪ DNS Cache Snooping
▪ RPC Enumeration	▪ DNSSEC Zone Walking
▪ Unix/Linux User Enumeration	**Other Enumeration Techniques**
Enumeration Countermeasures	▪ IPsec Enumeration
▪ Enumeration Countermeasures	▪ VoIP Enumeration
~~**Enumeration Pen Testing**~~	▪ RPC Enumeration
~~▪ Enumeration Pen Testing~~	▪ Unix/Linux User Enumeration
	▪ Telnet Enumeration
	▪ SMB Enumeration
	▪ FTP Enumeration
	▪ TFTP Enumeration
	▪ IPv6 Enumeration
	▪ BGP Enumeration
	Enumeration Countermeasures
	▪ Enumeration Countermeasures
Module 05: Vulnerability Analysis	**Module 05: Vulnerability Analysis**
Vulnerability Assessment Concepts	**Vulnerability Assessment Concepts**
▪ Vulnerability Research	▪ Vulnerability Research
▪ Vulnerability Classification	▪ Resources for Vulnerability Research
▪ What is Vulnerability Assessment?	▪ What is Vulnerability Assessment?

▪ Types of Vulnerability Assessment	▪ Vulnerability Scoring Systems and Databases
▪ Vulnerability-Management Life Cycle	○ Common Vulnerability Scoring System (CVSS)
○ Pre-Assessment Phase: Creating a Baseline	○ Common Vulnerabilities and Exposures (CVE)
○ Vulnerability Assessment Phase	○ National Vulnerability Database (NVD)
○ Post Assessment Phase	○ Common Weakness Enumeration (CWE)
Vulnerability Assessment Solutions	▪ Vulnerability-Management Life Cycle
▪ Comparing Approaches to Vulnerability Assessment	○ Pre-Assessment Phase
▪ Working of Vulnerability Scanning Solutions	○ Vulnerability Assessment Phase
▪ Types of Vulnerability Assessment Tools	○ Post Assessment Phase
▪ Characteristics of a Good Vulnerability Assessment Solution	**Vulnerability Classification and Assessment Types**
▪ Choosing a Vulnerability Assessment Tool	▪ Vulnerability Classification
▪ Criteria for Choosing a Vulnerability Assessment Tool	▪ Types of Vulnerability Assessment
▪ Best Practices for Selecting Vulnerability Assessment Tools	**Vulnerability Assessment Solutions and Tools**
Vulnerability Scoring Systems	▪ Comparing Approaches to Vulnerability Assessment
▪ Common Vulnerability Scoring System (CVSS)	▪ Characteristics of a Good Vulnerability Assessment Solution
▪ Common Vulnerabilities and Exposures (CVE)	▪ Working of Vulnerability Scanning Solutions
▪ National Vulnerability Database (NVD)	▪ Types of Vulnerability Assessment Tools
▪ Resources for Vulnerability Research	▪ Choosing a Vulnerability Assessment Tool
Vulnerability Assessment Tools	▪ Criteria for Choosing a Vulnerability Assessment Tool
▪ Vulnerability Assessment Tools	▪ Best Practices for Selecting Vulnerability Assessment Tools
○ Qualys Vulnerability Management	▪ Vulnerability Assessment Tools
○ Nessus Professional	○ Qualys Vulnerability Management
○ GFI LanGuard	○ Nessus Professional
○ Qualys FreeScan	○ GFI LanGuard
○ Nikto	○ OpenVAS
○ OpenVAS	○ Nikto
○ Retina CS	○ Other Vulnerability Assessment Tools
○ SAINT	▪ Vulnerability Assessment Tools for Mobile
○ Microsoft Baseline Security Analyzer (MBSA)	**Vulnerability Assessment Reports**
○ AVDS - Automated Vulnerability Detection System	▪ Vulnerability Assessment Reports
○ Vulnerability Assessment Tools	▪ Analyzing Vulnerability Scanning Report
▪ Vulnerability Assessment Tools for Mobile	

Vulnerability Assessment Reports	
▪ Vulnerability Assessment Reports	
▪ Analyzing Vulnerability Scanning Report	
Module 06: System Hacking	**Module 06: System Hacking**
System Hacking Concepts	**System Hacking Concepts**
▪ CEH Hacking Methodology (CHM)	▪ CEH Hacking Methodology (CHM)
▪ System Hacking Goals	▪ System Hacking Goals
Cracking Passwords	**Gaining Access**
▪ Password Cracking	▪ Cracking Passwords
▪ Types of Password Attacks	○ Microsoft Authentication
○ Non-Electronic Attacks	○ How Hash Passwords Are Stored in Windows SAM?
○ Active Online Attack	○ NTLM Authentication Process
• Dictionary, Brute Forcing and Rule-based Attack	○ Kerberos Authentication
• Password Guessing	○ Password Cracking
• Default Passwords	○ Types of Password Attacks
• Trojan/Spyware/Keylogger	• Non-Electronic Attacks
• Example of Active Online Attack Using USB Drive	• Active Online Attacks
• Hash Injection Attack	✓ Dictionary, Brute-Force and Rule-based Attack
• LLMNR/NBT-NS Poisoning	✓ Password Guessing
○ Passive Online Attack	✓ Default Passwords
• Wire Sniffing	✓ Trojans/Spyware/Keyloggers
• Man-in-the-Middle and Replay Attack	✓ Hash Injection/Pass-the-Hash (PtH) Attack
○ Offline Attack	✓ LLMNR/NBT-NS Poisoning
• Rainbow Table Attack	✓ Internal Monologue Attack
• Tools to Create Rainbow Tables: rtgen and Winrtgen	✓ Cracking Kerberos Password
• Distributed Network Attack	✓ Pass the Ticket Attack
▪ Password Recovery Tools	✓ Other Active Online Attacks
▪ Microsoft Authentication	➢ Combinator Attack
▪ How Hash Passwords Are Stored in Windows SAM?	➢ Fingerprint Attack
▪ NTLM Authentication Process	➢ PRINCE Attack
▪ Kerberos Authentication	➢ Toggle-Case Attack
▪ Password Salting	➢ Markov Chains Attack

▪ Tools to Extract the Password Hashes	• Passive Online Attacks
▪ Password Cracking Tools	✓ Wire Sniffing
▪ How to Defend against Password Cracking	✓ Man-in-the-Middle and Replay Attacks
▪ How to Defend against LLMNR/NBT-NS Poisoning	• Offline Attacks
Escalating Privileges	✓ Rainbow Table Attack
▪ Privilege Escalation	✓ Distributed Network Attack
▪ Privilege Escalation Using DLL Hijacking	○ Password Recovery Tools
▪ Privilege Escalation by Exploiting Vulnerabilities	○ Tools to Extract the Password Hashes
▪ Privilege Escalation Using Dylib Hijacking	○ Password Cracking Tools
▪ Privilege Escalation using Spectre and Meltdown Vulnerabilities	○ Password Salting
▪ Other Privilege Escalation Techniques	○ How to Defend against Password Cracking
▪ How to Defend Against Privilege Escalation	○ How to Defend against LLMNR/NBT-NS Poisoning
Executing Applications	○ Tools to Detect LLMNR/NBT-NS Poisoning
▪ Executing Applications	▪ Vulnerability Exploitation
○ Tools for Executing Applications	○ Exploit Sites
▪ Keylogger	○ Buffer Overflow
○ Types of Keystroke Loggers	• Types of Buffer Overflow
○ Hardware Keyloggers	✓ Stack-Based Buffer Overflow
○ Keyloggers for Windows	✓ Heap-Based Buffer Overflow
○ Keyloggers for Mac	• Simple Buffer Overflow in C
▪ Spyware	• Windows Buffer Overflow Exploitation
○ Spyware	✓ Perform Spiking
○ USB Spyware	✓ Perform Fuzzing
○ Audio Spyware	✓ Identify the Offset
○ Video Spyware	✓ Overwrite the EIP Register
○ Telephone/Cellphone Spyware	✓ Identify Bad Characters
○ GPS Spyware	✓ Identify the Right Module
▪ How to Defend Against Keyloggers	✓ Generate Shellcode and Gain Shell Access
○ Anti-Keylogger	• Buffer Overflow Detection Tools
▪ How to Defend Against Spyware	• Defending against Buffer Overflows
○ Anti-Spyware	**Escalating Privileges**
Hiding Files	▪ Privilege Escalation
▪ Rootkits	▪ Privilege Escalation Using DLL Hijacking
○ Types of Rootkits	▪ Privilege Escalation by Exploiting Vulnerabilities
○ How Rootkit Works	▪ Privilege Escalation Using Dylib Hijacking
○ Rootkits	▪ Privilege Escalation using Spectre and Meltdown

	Vulnerabilities
• Horse Pill	▪ Privilege Escalation using Named Pipe Impersonation
• GrayFish	▪ Privilege Escalation by Exploiting Misconfigured Services
• Sirefef	○ Unquoted Service Paths
• Necurs	○ Service Object Permissions
○ Detecting Rootkits	○ Unattended Installs
○ Steps for Detecting Rootkits	▪ Pivoting and Relaying to Hack External Machines
○ How to Defend against Rootkits	▪ Other Privilege Escalation Techniques
○ Anti-Rootkits	▪ Privilege Escalation Tools
▪ NTFS Data Stream	▪ How to Defend Against Privilege Escalation
○ How to Create NTFS Streams	○ Tools for Defending against DLL and Dylib Hijacking
○ NTFS Stream Manipulation	○ Defending against Spectre and Meltdown Vulnerabilities
○ How to Defend against NTFS Streams	○ Tools for Detecting Spectre and Meltdown Vulnerabilities
○ NTFS Stream Detectors	**Maintaining Access**
▪ What is Steganography?	▪ Executing Applications
○ Classification of Steganography	○ Remote Code Execution Techniques
○ Types of Steganography based on Cover Medium	• Tools for Executing Applications
• Whitespace Steganography	○ Keylogger
• Image Steganography	• Types of Keystroke Loggers
✓ Image Steganography Tools	• Hardware Keyloggers
• Document Steganography	• Keyloggers for Windows
• Video Steganography	• Keyloggers for Mac
• Audio Steganography	○ Spyware
• Folder Steganography	• Spyware: Spytech SpyAgent and Power Spy
• Spam/Email Steganography	• Desktop and Child Monitoring Spyware
○ Steganography Tools for Mobile Phones	• USB Spyware
○ Steganalysis	• Audio Spyware
○ Steganalysis Methods/Attacks on Steganography	• Video Spyware
○ Detecting Steganography (Text, Image, Audio, and Video Files)	• Telephone/Cellphone Spyware
○ Steganography Detection Tools	• GPS Spyware
Covering Tracks	○ How to Defend Against Keyloggers
▪ Covering Tracks	• Anti-Keyloggers

▪ Disabling Auditing: Auditpol	○ How to Defend Against Spyware
▪ Clearing Logs	• Anti-Spyware
▪ Manually Clearing Event Logs	▪ Hiding Files
▪ Ways to Clear Online Tracks	○ Rootkits
▪ Covering BASH Shell Tracks	• Types of Rootkits
▪ Covering Tracks on Network	• How a Rootkit Works
▪ Covering Tracks on OS	• Popular Rootkits
▪ Covering Tracks Tools	✓ LoJax
~~**Penetration Testing**~~	✓ Scranos
~~▪ Password Cracking~~	✓ Horse Pill
~~▪ Privilege Escalation~~	✓ Necurs
~~▪ Executing Applications~~	• Detecting Rootkits
~~▪ Hiding Files~~	• Steps for Detecting Rootkits
~~▪ Covering Tracks~~	• How to Defend against Rootkits
	• Anti-Rootkits
	○ NTFS Data Stream
	• How to Create NTFS Streams
	• NTFS Stream Manipulation
	• How to Defend against NTFS Streams
	• NTFS Stream Detectors
	○ What is Steganography?
	• Classification of Steganography
	• Types of Steganography based on Cover Medium
	✓ Whitespace Steganography
	✓ Image Steganography
	➢ Image Steganography Tools
	✓ Document Steganography
	✓ Video Steganography
	✓ Audio Steganography
	✓ Folder Steganography
	✓ Spam/Email Steganography
	• Steganography Tools for Mobile Phones
	• Steganalysis
	• Steganalysis Methods/Attacks on Steganography
	• Detecting Steganography (Text, Image, Audio, and Video Files)

	• Steganography Detection Tools
	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
	○ Disabling the Last Access Timestamp
	○ Disabling Windows Hibernation
	○ Disabling Windows Virtual Memory (Paging File)
	○ Disabling System Restore Points
	○ Disabling Windows Thumbnail Cache
	○ Disabling Windows Prefetch Feature
	▪ 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 a Malware can Get into 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
▪ Components of Malware	▪ Components of Malware
Trojan Concepts	**APT Concepts**
▪ What is a Trojan?	▪ What are Advanced Persistent Threats?
▪ How Hackers Use Trojans	▪ Characteristics of Advanced Persistent Threats
▪ Common Ports used by Trojans	▪ Advanced Persistent Threat Lifecycle
▪ How to Infect Systems Using a Trojan	**Trojan Concepts**
▪ Trojan Horse Construction Kit	▪ What is a Trojan?
▪ Wrappers	▪ How Hackers Use Trojans
▪ Crypters	▪ Common Ports used by Trojans
▪ How Attackers Deploy a Trojan	▪ Types of Trojans
▪ Exploit Kits	○ Remote Access Trojans

▪ Evading Anti-Virus Techniques	○ Backdoor Trojans
▪ Types of Trojans	○ Botnet Trojans
○ Remote Access Trojans	○ Rootkit Trojans
○ Backdoor Trojans	○ E-banking Trojans
○ Botnet Trojans	• Working of E-banking Trojans
○ Rootkit Trojans	• E-banking Trojan: Dreambot
○ E-banking Trojans	○ Point-of-Sale Trojans
• Working of E-banking Trojans	○ Defacement Trojans
• E-banking Trojan: ZeuS	○ Service Protocol Trojans
○ Proxy Server Trojans	○ Mobile Trojans
○ Covert Channel Trojans	○ IoT Trojans
○ Defacement Trojans	○ Other Trojans
○ Service Protocol Trojans	• Security Software Disabler Trojans
○ Mobile Trojans	• Destructive Trojans
○ IoT Trojans	• DDoS Trojans
○ Other Trojans	• Command Shell Trojans
Virus and Worm Concepts	▪ How to Infect Systems Using a Trojan
▪ Introduction to Viruses	○ Creating a Trojan
▪ Stages of Virus Life	○ Employing a Dropper or Downloader
▪ Working of Viruses	○ Employing a Wrapper
▪ Indications of Virus Attack	○ Employing a Crypter
▪ How does a Computer Get Infected by Viruses	○ Propagating and Deploying a Trojan
▪ Virus Hoaxes	• Deploy a Trojan through Emails
▪ Fake Antiviruses	• Deploy a Trojan through Covert Channels
▪ Ransomware	• Deploy a Trojan through Proxy Servers
▪ Types of Viruses	• Deploy a Trojan through USB/Flash Drives
○ System and File Viruses	• Evading Anti-Virus Software
○ Multipartite and Macro Viruses	○ Exploit Kits
○ Cluster and Stealth Viruses	**Virus and Worm Concepts**
○ Encryption and Sparse Infector Viruses	▪ Introduction to Viruses
○ Polymorphic Viruses	▪ Stages of Virus Lifecycle
○ Metamorphic Viruses	▪ Working of Viruses
○ Overwriting File or Cavity Viruses	○ How does a Computer Get Infected by Viruses?
○ Companion/Camouflage and Shell Viruses	▪ Types of Viruses
○ File Extension Viruses	○ System and File Viruses
○ FAT and Logic Bomb Viruses	○ Multipartite and Macro Viruses
○ Web Scripting and E-mail Viruses	○ Cluster and Stealth Viruses
○ Other Viruses	○ Encryption and Sparse Infector Viruses

▪ Creating Virus	○ Polymorphic Viruses
▪ Computer Worms	○ Metamorphic Viruses
▪ Worm Makers	○ Overwriting File or Cavity Viruses
Malware Analysis	○ Companion/Camouflage and Shell Viruses
▪ What is Sheep Dip Computer?	○ File Extension Viruses
▪ Anti-Virus Sensor Systems	○ FAT and Logic Bomb Viruses
▪ Introduction to Malware Analysis	○ Other Viruses
▪ Malware Analysis Procedure: Preparing Testbed	• Web Scripting Viruses
▪ Static Malware Analysis	• E-mail Viruses
○ File Fingerprinting	• Armored Viruses
○ Local and Online Malware Scanning	• Add-on Viruses
○ Performing Strings Search	• Intrusive Viruses
○ Identifying Packing/ Obfuscation Methods	• Direct Action or Transient Viruses
○ Finding the Portable Executables (PE) Information	• Terminate and Stay Resident (TSR) Viruses
○ Identifying File Dependencies	○ Ransomware
○ Malware Disassembly	▪ How to Infect Systems Using a Virus
▪ Dynamic Malware Analysis	○ Creating a Virus
○ Port Monitoring	○ Propagating and Deploying a Virus
○ Process Monitoring	• Virus Hoaxes
○ Registry Monitoring	• Fake Antiviruses
○ Windows Services Monitoring	▪ Computer Worms
○ Startup Programs Monitoring	○ Worm Makers
○ Event Logs Monitoring/Analysis	**Fileless Malware Concepts**
○ Installation Monitoring	▪ What is Fileless Malware?
○ Files and Folder Monitoring	▪ Taxomony of Fileless Malware Threats
○ Device Drivers Monitoring	▪ How does Fileless Malware Work?
○ Network Traffic Monitoring/Analysis	▪ Launching Fileless Malware through Document Exploits and In-Memory Exploits
○ DNS Monitoring/ Resolution	▪ Lanching Fileless Malware through Script-based Injection
○ API Calls Monitoring	▪ Lanching Fileless Malware by Exploiting System Admin Tools
▪ Virus Detection Methods	▪ Launching Fileless Malware through Phishing
▪ Trojan Analysis: ZeuS/Zbot	▪ Maintaining Persistence with Fileless Techniques
▪ Virus Analysis: WannaCry	▪ Fileless Malware
Countermeasures	▪ Fileless Malware Obfuscation Techniques to Bypass Antivirus
▪ Trojan Countermeasures	**Malware Analysis**

▪ Backdoor Countermeasures	▪ What is Sheep Dip Computer?
▪ Virus and Worms Countermeasures	▪ Antivirus Sensor Systems
Anti-Malware Software	▪ Introduction to Malware Analysis
▪ Anti-Trojan Software	▪ Malware Analysis Procedure: Preparing Testbed
▪ Antivirus Software	▪ Static Malware Analysis
~~**Malware Penetration Testing**~~	○ File Fingerprinting
~~▪ Malware Penetration Testing~~	○ Local and Online Malware Scanning
	○ Performing Strings Search
	○ Identifying Packing/Obfuscation Methods
	○ Finding the Portable Executables (PE) Information
	○ Identifying File Dependencies
	○ Malware Disassembly
	▪ Dynamic Malware Analysis
	○ Port Monitoring
	○ Process Monitoring
	○ Registry Monitoring
	○ Windows Services Monitoring
	○ Startup Programs Monitoring
	○ Event Logs Monitoring/Analysis
	○ Installation Monitoring
	○ Files and Folders Monitoring
	○ Device Drivers Monitoring
	○ Network Traffic Monitoring/Analysis
	○ DNS Monitoring/Resolution
	○ API Calls Monitoring
	▪ Virus Detection Methods
	▪ Trojan Analysis: Emotet
	Emotet Malware Attack Phases:
	Infection Phase
	Maintaining Persistence Phase
	System Compromise Phase
	Network Propagation Phase
	▪ Virus Analysis: SamSam Ransomware
	SamSam Ransomware Attack Stages
	▪ Fileless Malware Analysis: Astaroth Attack
	Countermeasures
	▪ Trojan Countermeasures
	▪ Backdoor Countermeasures

	▪ Virus and Worm Countermeasures
	▪ Fileless Malware Countermeasures
	Anti-Malware Software
	▪ Anti-Trojan Software
	▪ Antivirus Software
	▪ Fileless Malware Detection Tools
	▪ Filesless Malware Protection Tools
Module 08: Sniffing	**Module 08: Sniffing**
Sniffing Concepts	**Sniffing Concepts**
▪ Network Sniffing	▪ Network Sniffing
▪ Types of Sniffing	▪ Types of Sniffing
▪ How an Attacker Hacks the Network Using Sniffers	▪ How an Attacker Hacks the Network Using Sniffers
▪ Protocols Vulnerable to Sniffing	▪ Protocols Vulnerable to Sniffing
▪ Sniffing in the Data Link Layer of the OSI Model	▪ Sniffing in the Data Link Layer of the OSI Model
▪ Hardware Protocol Analyzers	▪ Hardware Protocol Analyzers
▪ SPAN Port	▪ SPAN Port
▪ Wiretapping	▪ Wiretapping
▪ Lawful Interception	▪ Lawful Interception
Sniffing Technique: MAC Attacks	**Sniffing Technique: MAC Attacks**
▪ MAC Address/CAM Table	▪ MAC Address/CAM Table
▪ How CAM Works	▪ How CAM Works
▪ What Happens When CAM Table Is Full?	▪ What Happens When a CAM Table Is Full?
▪ MAC Flooding	▪ MAC Flooding
▪ Switch Port Stealing	▪ Switch Port Stealing
▪ How to Defend against MAC Attacks	▪ How to Defend against MAC Attacks
Sniffing Technique: DHCP Attacks	**Sniffing Technique: DHCP Attacks**
▪ How DHCP Works	▪ How DHCP Works
▪ DHCP Request/Reply Messages	▪ DHCP Request/Reply Messages
▪ DHCP Starvation Attack	▪ DHCP Starvation Attack
▪ Rogue DHCP Server Attack	▪ Rogue DHCP Server Attack
▪ How to Defend Against DHCP Starvation and Rogue Server Attack	▪ How to Defend Against DHCP Starvation and Rogue Server Attacks
Sniffing Technique: ARP Poisoning	**Sniffing Technique: ARP Poisoning**
▪ What Is Address Resolution Protocol (ARP)?	▪ What Is Address Resolution Protocol (ARP)?
▪ ARP Spoofing Attack	▪ ARP Spoofing Attack
▪ Threats of ARP Poisoning	▪ Threats of ARP Poisoning
▪ ARP Poisoning Tools	▪ ARP Poisoning Tools

▪ How to Defend Against ARP Poisoning	▪ How to Defend Against ARP Poisoning
▪ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches	▪ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
▪ ARP Spoofing Detection Tools	▪ ARP Spoofing Detection Tools
Sniffing Technique: Spoofing Attacks	**Sniffing Technique: Spoofing Attacks**
▪ MAC Spoofing/Duplicating	▪ MAC Spoofing/Duplicating
▪ MAC Spoofing Technique: Windows	▪ MAC Spoofing Technique: Windows
▪ MAC Spoofing Tools	▪ MAC Spoofing Tools
▪ IRDP Spoofing	▪ IRDP Spoofing
▪ How to Defend Against MAC Spoofing	▪ VLAN Hopping
Sniffing Technique: DNS Poisoning	○ Switch Spoofing
▪ DNS Poisoning Techniques	○ Double Tagging
○ Intranet DNS Spoofing	▪ STP Attack
○ Internet DNS Spoofing	▪ How to Defend Against MAC Spoofing
○ Proxy Server DNS Poisoning	▪ How to Defend Against VLAN Hopping
○ DNS Cache Poisoning	▪ How to Defend Against STP Attacks
▪ How to Defend Against DNS Spoofing	**Sniffing Technique: DNS Poisoning**
Sniffing Tools	▪ DNS Poisoning Techniques
▪ Sniffing Tool: Wireshark	○ Intranet DNS Spoofing
○ Follow TCP Stream in Wireshark	○ Internet DNS Spoofing
○ Display Filters in Wireshark	○ Proxy Server DNS Poisoning
○ Additional Wireshark Filters	○ DNS Cache Poisoning
▪ Sniffing Tools	▪ DNS Poisoning Tools
▪ Packet Sniffing Tools for Mobile	▪ How to Defend Against DNS Spoofing
Countermeasures	**Sniffing Tools**
▪ How to Defend Against Sniffing	▪ Sniffing Tool: Wireshark
Sniffing Detection Techniques	○ Follow TCP Stream in Wireshark
▪ How to Detect Sniffing	○ Display Filters in Wireshark
▪ Sniffer Detection Techniques	○ Additional Wireshark Filters
○ Ping Method	▪ Sniffing Tools
○ DNS Method	▪ Packet Sniffing Tools for Mobile Phones
○ ARP Method	**Countermeasures**
▪ Promiscuous Detection Tools	▪ How to Defend Against Sniffing
~~**Sniffing Pen Testing**~~	**Sniffing Detection Techniques**
~~▪ Sniffing Penetration Testing~~	▪ How to Detect Sniffing
	▪ Sniffer Detection Techniques
	○ Ping Method
	○ 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	▪ Phases of a Social Engineering Attack
Social Engineering Techniques	**Social Engineering Techniques**
▪ Types of Social Engineering	▪ Types of Social Engineering
▪ Human-based Social Engineering	▪ Human-based Social Engineering
○ Impersonation	○ Impersonation
○ Impersonation (Vishing)	○ Impersonation (Vishing)
○ Eavesdropping	○ Eavesdropping
○ Shoulder Surfing	○ Shoulder Surfing
○ Dumpster Diving	○ Dumpster Diving
○ Reverse Social Engineering	○ Reverse Social Engineering
○ Piggybacking	○ Piggybacking
○ Tailgating	○ Tailgating
▪ Computer-based Social Engineering	○ Diversion Theft
○ Phishing	○ Honey Trap
▪ Mobile-based Social Engineering	○ Baiting
○ Publishing Malicious Apps	○ Quid Pro Quo
○ Repackaging Legitimate Apps	○ Elicitation
○ Fake Security Applications	▪ Computer-based Social Engineering
○ SMiShing (SMS Phishing)	○ Phishing
Insider Threats	• Examples of Phishing Emails
▪ Insider Threat / Insider Attack	• Types of Phishing
▪ Type of Insider Threats	• Phishing Tools
Impersonation on Social Networking Sites	▪ Mobile-based Social Engineering
▪ Social Engineering Through Impersonation on Social Networking Sites	○ Publishing Malicious Apps
▪ Impersonation on Facebook	○ Repackaging Legitimate Apps
▪ Social Networking Threats to Corporate Networks	○ Fake Security Applications
Identity Theft	○ SMiShing (SMS Phishing)
▪ Identity Theft	**Insider Threats**
Countermeasures	▪ Insider Threats/Insider Attacks
▪ Social Engineering Countermeasures	▪ Types of Insider Threats
▪ Insider Threats Countermeasures	▪ Behavioral Indications of an Insider Threat
▪ Identity Theft Countermeasures	**Impersonation on Social Networking Sites**

▪ How to Detect Phishing Emails?	▪ Social Engineering through Impersonation on Social Networking Sites
▪ Anti-Phishing Toolbar	▪ Impersonation on Facebook
▪ Common Social Engineering Targets and Defense Strategies	▪ Social Networking Threats to Corporate Networks
~~**Social Engineering Pen Testing**~~	**Identity Theft**
~~▪ Social Engineering Pen Testing~~	▪ Identity Theft
~~○ Using Emails~~	**Countermeasures**
~~○ Using Phone~~	▪ Social Engineering Countermeasures
~~○ In Person~~	▪ Detecting Insider Threats
▪ Social Engineering Pen Testing Tools	▪ Insider Threats Countermeasures
	▪ Identity Theft Countermeasures
	▪ How to Detect Phishing Emails?
	▪ Anti-Phishing Toolbar
	▪ Common Social Engineering Targets and Defense Strategies
	▪ Social Engineering Tools
	▪ Audit Organization's Security for Phishing Attacks using OhPhish
Module 10: Denial-of-Service	**Module 10: Denial-of-Service**
DoS/DDoS Concepts	**DoS/DDoS Concepts**
▪ What is a Denial-of-Service Attack?	▪ What is a DoS Attack?
▪ What is Distributed Denial-of-Service Attack?	▪ What is a DDoS Attack?
DoS/DDoS Attack Techniques	**DoS/DDoS Attack Techniques**
▪ Basic Categories of DoS/DDoS Attack Vectors	▪ Basic Categories of DoS/DDoS Attack Vectors
▪ UDP Flood Attack	○ Volumetric Attacks
▪ ICMP Flood Attack	• UDP Flood Attack
▪ Ping of Death and Smurf Attack	• ICMP Flood Attack
▪ SYN Flood Attack	• Ping of Death and Smurf Attacks
▪ Fragmentation Attack	• Pulse Wave and Zero-Day DDoS Attacks
▪ HTTP GET/POST and Slowloris Attacks	○ Protocol Attacks
▪ Multi-Vector Attack	• SYN Flood Attack
▪ Peer-to-Peer Attacks	• Fragmentation Attack
▪ Permanent Denial-of-Service Attack	• Spoofed Session Flood Attack
▪ Distributed Reflection Denial-of-Service (DRDoS)	○ Application Layer Attacks
Botnets	• HTTP GET/POST and Slowloris Attacks
▪ Organized Cyber Crime: Organizational Chart	• UDP Application Layer Flood Attack
▪ Botnet	▪ Multi-Vector Attack

▪ A Typical Botnet Setup	▪ Peer-to-Peer Attack
▪ Botnet Ecosystem	▪ Permanent Denial-of-Service Attack
▪ Scanning Methods for Finding Vulnerable Machines	▪ Distributed Reflection Denial-of-Service (DRDoS) Attack
▪ How Malicious Code Propagates?	**Botnets**
▪ Botnet Trojans	▪ Organized Cyber Crime: Organizational Chart
DDoS Case Study	▪ Botnets
▪ DDoS Attack	▪ A Typical Botnet Setup
▪ Hackers Advertise Links to Download Botnet	▪ Botnet Ecosystem
▪ Use of Mobile Devices as Botnets for Launching DDoS Attacks	▪ Scanning Methods for Finding Vulnerable Machines
▪ DDoS Case Study: Dyn DDoS Attack	▪ How Does Malicious Code Propagate?
DoS/DDoS Attack Tools	**DDoS Case Study**
▪ DoS/DDoS Attack Tools	▪ DDoS Attack
▪ DoS and DDoS Attack Tool for Mobile	▪ Hackers Advertise Links for Downloading Botnets
Countermeasures	▪ Use of Mobile Devices as Botnets for Launching DDoS Attacks
▪ Detection Techniques	▪ DDoS Case Study: DDoS Attack on GitHub
▪ DoS/DDoS Countermeasure Strategies	**DoS/DDoS Attack Tools**
▪ DDoS Attack Countermeasures	▪ DoS/DDoS Attack Tools
○ Protect Secondary Victims	▪ DoS and DDoS Attack Tools for Mobiles
○ Detect and Neutralize Handlers	**Countermeasures**
○ Prevent Potential Attacks	▪ Detection Techniques
○ Deflect Attacks	▪ DoS/DDoS Countermeasure Strategies
○ Mitigate Attacks	▪ DDoS Attack Countermeasures
○ Post-Attack Forensics	○ Protect Secondary Victims
▪ Techniques to Defend against Botnets	○ Detect and Neutralize Handlers
▪ DoS/DDoS Countermeasures	○ Prevent Potential Attacks
▪ DoS/DDoS Protection at ISP Level	○ Deflect Attacks
▪ Enabling TCP Intercept on Cisco IOS Software	○ Mitigate Attacks
DoS/DDoS Protection Tools	○ Post-Attack Forensics
▪ Advanced DDoS Protection Appliances	▪ Techniques to Defend against Botnets
▪ DoS/DDoS Protection Tools	▪ Additional DoS/DDoS Countermeasures
~~**DoS/DDoS Penetration Testing**~~	▪ DoS/DDoS Protection at ISP Level
~~▪ Denial-of-Service (DoS) Attack Pen Testing~~	▪ Enabling TCP Intercept on Cisco IOS Software
	DoS/DDoS Protection Tools
	▪ Advanced DDoS Protection Appliances
	▪ DoS/DDoS Protection Tools
	▪ DoS/DDoS Protection Services

Module 11: Session Hijacking	**Module 11: Session Hijacking**
Session Hijacking Concepts	**Session Hijacking Concepts**
▪ What is Session Hijacking?	▪ What is Session Hijacking?
▪ Why Session Hijacking is 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	▪ Application Level Session Hijacking
▪ Compromising Session IDs using Sniffing and by Predicting Session Token	▪ Compromising Session IDs using Sniffing and by Predicting Session Token
○ How to Predict a Session Token	○ How to Predict a Session Token
▪ Compromising Session IDs Using Man-in-the-Middle Attack	▪ Compromising Session IDs Using Man-in-the-Middle Attack
▪ Compromising Session IDs Using Man-in-the-Browser Attack	▪ Compromising Session IDs Using Man-in-the-Browser Attack
○ Steps to Perform Man-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 Attack	▪ 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
Network Level Session Hijacking	▪ Session Hijacking Using Session Donation Attack
▪ TCP/IP Hijacking	**Network Level Session Hijacking**
▪ IP Spoofing: Source Routed Packets	▪ Network Level Session Hijacking
▪ RST Hijacking	▪ TCP/IP Hijacking
▪ Blind Hijacking	▪ IP Spoofing: Source Routed Packets
▪ UDP Hijacking	▪ RST Hijacking
▪ MiTM Attack Using Forged ICMP and ARP Spoofing	▪ Blind Hijacking
Session Hijacking Tools	▪ UDP Hijacking

▪ Session Hijacking Tools	▪ MiTM Attack Using Forged ICMP and ARP Spoofing
▪ Session Hijacking Tools for Mobile	**Session Hijacking Tools**
Countermeasures	▪ Session Hijacking Tools
▪ Session Hijacking Detection Methods	▪ Session Hijacking Tools for Mobile Phones
▪ Protecting against Session Hijacking	**Countermeasures**
▪ Methods to Prevent Session Hijacking: To be Followed by Web Developers	▪ Session Hijacking Detection Methods
▪ Methods to Prevent Session Hijacking: To be Followed by Web Users	▪ Protecting against Session Hijacking
▪ Session Hijacking Detection Tools	▪ Web Development Guidelines to Prevent Session Hijacking
▪ Approaches Vulnerable to Session Hijacking and their Preventative Solutions	▪ Web User Guidelines to Prevent Session Hijacking
▪ Approaches to Prevent Session Hijacking	▪ Session Hijacking Detection Tools
▪ IPSec	▪ Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions
○ Components of IPsec	▪ Approaches to Prevent Session Hijacking
○ Benefits of IPsec	▪ Approaches to Prevent MITM Attacks
○ Modes of IPsec	▪ IPSec
○ IPsec Architecture	○ IPsec Authentication and Confidentiality
○ IPsec Authentication and Confidentiality	▪ Session Hijacking Prevention Tools
▪ Session Hijacking Prevention Tools	
~~**Penetration Testing**~~	
~~▪ Session Hijacking Pen Testing~~	
Module 12: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
IDS, Firewall and Honeypot Concepts	**IDS, IPS, Firewall, and Honeypot Concepts**
▪ Intrusion Detection System (IDS)	▪ Intrusion Detection System (IDS)
○ How IDS Detects an Intrusion	○ How an IDS Detects an Intrusion?
○ General Indications of Intrusions	○ General Indications of Intrusions
○ Types of Intrusion Detection Systems	○ Types of Intrusion Detection Systems
○ Types of IDS Alerts	○ Types of IDS Alerts
▪ Firewall	▪ Intrusion Prevention System (IPS)
○ Firewall Architecture	▪ Firewall
○ DeMilitarized Zone (DMZ)	○ Firewall Architecture
○ Types of Firewalls	○ Demilitarized Zone (DMZ)
○ Firewall Technologies	○ Types of Firewalls
• Packet Filtering Firewall	○ Firewall Technologies
• 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	○ Firewall Limitations
○ Types of Honeypots	▪ Honeypot
IDS, Firewall and Honeypot Solutions	○ Types of Honeypots
▪ Intrusion Detection Tool	**IDS, IPS, Firewall, and Honeypot Solutions**
○ Snort	▪ Intrusion Detection Tools
• Snort Rules	○ Snort
• Snort Rules: Rule Actions and IP Protocols	• Snort Rules
• Snort Rules: The Direction Operator and IP Addresses	• Snort Rules: Rule Actions and IP Protocols
• Snort Rules: Port Numbers	• Snort Rules: The Direction Operator and IP Addresses
○ Intrusion Detection Tools: TippingPoint and AlienVault® OSSIM™	• Snort Rules: Port Numbers
○ Intrusion Detection Tools	○ Intrusion Detection Tools
○ Intrusion Detection Tools for Mobile	○ Intrusion Detection Tools for Mobile Devices
▪ Firewalls	▪ Intrusion Prevention Tools
○ ZoneAlarm Free Firewall 2018 and Firewall Analyzer	▪ Firewalls
○ Firewalls	○ Firewalls for Mobile Devices
○ Firewalls for Mobile	▪ Honeypot Tools
▪ Honeypot Tools	**Evading IDS**
○ KFSensor and SPECTER	▪ IDS Evasion Techniques
○ Honeypot Tools	○ Insertion Attack
○ Honeypot Tools for Mobile	○ Evasion
Evading IDS	○ Denial-of-Service Attack (DoS)
▪ IDS Evasion Techniques	○ Obfuscating
○ Insertion Attack	○ False Positive Generation
○ Evasion	○ Session Splicing
○ Denial-of-Service Attack (DoS)	○ Unicode Evasion Technique
○ Obfuscating	○ Fragmentation Attack
○ False Positive Generation	○ Overlapping Fragments
○ Session Splicing	○ Time-To-Live Attacks
○ Unicode Evasion	○ Invalid RST Packets

○ Fragmentation Attack	○ Urgency Flag
○ Overlapping Fragments	○ Polymorphic Shellcode
○ Time-To-Live Attacks	○ ASCII Shellcode
○ Invalid RST Packets	○ Application-Layer Attacks
○ Urgency Flag	○ Desynchronization
○ Polymorphic Shellcode	○ Other Types of Evasion
○ ASCII Shellcode	**Evading Firewalls**
○ Application-Layer Attacks	▪ Firewall Evasion Techniques
○ Desynchronization	○ Firewall Identification
○ Other Types of Evasion	○ IP Address Spoofing
Evading Firewalls	○ Source Routing
▪ Firewall Evasion Techniques	○ Tiny Fragments
○ Firewall Identification	○ Bypass Blocked Sites Using an IP Address in Place of a URL
○ IP Address Spoofing	○ Bypass Blocked Sites Using Anonymous Website Surfing Sites
○ Source Routing	○ Bypass a Firewall Using a Proxy Server
○ Tiny Fragments	○ Bypassing Firewalls through the ICMP Tunneling Method
○ Bypass Blocked Sites Using IP Address in Place of URL	○ Bypassing Firewalls through the ACK Tunneling Method
○ Bypass Blocked Sites Using Anonymous Website Surfing Sites	○ Bypassing Firewalls through the HTTP Tunneling Method
○ Bypass a Firewall Using Proxy Server	• Why do I Need HTTP Tunneling?
○ Bypassing Firewall through ICMP Tunneling Method	• HTTP Tunneling Tools
○ Bypassing Firewall through ACK Tunneling Method	○ Bypassing Firewalls through the SSH Tunneling Method
○ Bypassing Firewall through HTTP Tunneling Method	• SSH Tunneling Tools: Bitvise and Secure Pipes
• Why do I Need HTTP Tunneling	○ Bypassing Firewalls through the DNS Tunneling Method
• HTTP Tunneling Tools	○ Bypassing Firewalls through External Systems
○ Bypassing Firewall through SSH Tunneling Method	○ Bypassing Firewalls through MITM Attacks
• SSH Tunneling Tool: Bitvise and Secure Pipes	○ Bypassing Firewalls through Content
○ Bypassing Firewall through External Systems	○ Bypassing the WAF using an XSS Attack
○ Bypassing Firewall through MITM Attack	**IDS/Firewall Evading Tools**
○ Bypassing Firewall through Content	IDS/Firewall Evading Tools
○ Bypassing WAF using XSS Attack	Packet Fragment Generator Tools

IDS/Firewall Evading Tools	**Detecting Honeypots**
▪ IDS/Firewall Evasion Tools	▪ Detecting Honeypots
▪ Packet Fragment Generator Tools	○ Detecting and Defeating Honeypots
Detecting Honeypots	▪ Honeypot Detection Tools: Send-Safe Honeypot Hunter
▪ Detecting Honeypots	**IDS/Firewall Evasion Countermeasures**
▪ Detecting and Defeating Honeypots	▪ How to Defend Against IDS Evasion
▪ Honeypot Detection Tool: Send-Safe Honeypot Hunter	▪ How to Defend Against Firewall Evasion
IDS/Firewall Evasion Countermeasures	
▪ How to Defend Against IDS Evasion	
▪ How to Defend Against Firewall Evasion	
~~**Penetration Testing**~~	
~~▪ Firewall/IDS Penetration Testing~~	
~~○ Firewall Penetration Testing~~	
~~○ IDS Penetration Testing~~	
Module 13: Hacking Web Servers	**Module 13: Hacking Web Servers**
Web Server Concepts	**Web Server Concepts**
▪ Web Server Operations	▪ Web Server Operations
▪ Open Source Web Server Architecture	▪ Web Server Security Issues
▪ IIS Web Server Architecture	▪ Why are Web Servers Compromised?
▪ Web Server Security Issue	**Web Server Attacks**
▪ Why Web Servers Are Compromised?	▪ DoS/DDoS Attacks
▪ Impact of Web Server Attacks	▪ DNS Server Hijacking
Web Server Attacks	▪ DNS Amplification Attack
▪ DoS/DDoS Attacks	▪ Directory Traversal Attacks
▪ DNS Server Hijacking	▪ Man-in-the-Middle/Sniffing Attack
▪ DNS Amplification Attack	▪ Phishing Attacks
▪ Directory Traversal Attacks	▪ Website Defacement
▪ Man-in-the-Middle/Sniffing Attack	▪ Web Server Misconfiguration
▪ Phishing Attacks	▪ HTTP Response-Splitting Attack
▪ Website Defacement	▪ Web Cache Poisoning Attack
▪ Web Server Misconfiguration	▪ SSH Brute Force Attack
▪ HTTP Response Splitting Attack	▪ Web Server Password Cracking
▪ Web Cache Poisoning Attack	▪ Server-Side Request Forgery (SSRF) Attack
▪ SSH Brute Force Attack	▪ Web Application Attacks
▪ Web Server Password Cracking	**Web Server Attack Methodology**
▪ Web Application Attacks	▪ Information Gathering

Web Server Attack Methodology	○ Information Gathering from Robots.txt File
▪ Information Gathering	▪ Web Server Footprinting/Banner Grabbing
○ Information Gathering from Robots.txt File	○ Web Server Footprinting Tools
▪ Web Server Footprinting/Banner Grabbing	○ Enumerating Web Server Information Using Nmap
○ Web Server Footprinting Tools	▪ Website Mirroring
○ Enumerating Web Server Information Using Nmap	○ Finding Default Credentials of Web Server
▪ Website Mirroring	○ Finding Default Content of Web Server
○ Finding Default Credentials of Web Server	○ Finding Directory Listings of Web Server
○ Finding Default Content of Web Server	▪ Vulnerability Scanning
○ Finding Directory Listings of Web Server	○ Finding Exploitable Vulnerabilities
▪ Vulnerability Scanning	▪ Session Hijacking
○ Finding Exploitable Vulnerabilities	▪ Web Server Password Hacking
▪ Session Hijacking	▪ Using Application Server as a Proxy
▪ Web Server Passwords Hacking	**Web Server Attack Tools**
▪ Using Application Server as a Proxy	▪ Metasploit
Web Server Attack Tools	○ Metasploit Exploit Module
▪ Metasploit	○ Metasploit Payload and Auxiliary Modules
○ Metasploit Exploit Module	○ Metasploit NOPS Module
○ Metasploit Payload and Auxiliary Module	▪ Web Server Attack Tools
○ Metasploit NOPS Module	**Countermeasures**
▪ Web Server Attack Tools	▪ Place Web Servers in Separate Secure Server Security Segment on Network
Countermeasures	▪ Countermeasures
▪ Place Web Servers in Separate Secure Server Security Segment on Network	○ Patches and Updates
▪ Countermeasures	○ Protocols and Accounts
○ Patches and Updates	○ Files and Directories
○ Protocols	▪ Detecting Web Server Hacking Attempts
○ Accounts	▪ How to Defend Against Web Server Attacks
○ Files and Directories	▪ How to Defend against HTTP Response-Splitting and Web Cache Poisoning
▪ Detecting Web Server Hacking Attempts	▪ How to Defend against DNS Hijacking
▪ How to Defend Against Web Server Attacks	**Patch Management**
▪ How to Defend against HTTP Response Splitting and Web Cache Poisoning	▪ Patches and Hotfixes
▪ How to Defend against DNS Hijacking	▪ What is Patch Management?
Patch Management	▪ Installation of a Patch
▪ Patches and Hotfixes	▪ Patch Management Tools

▪ What is Patch Management	**Web Server Security Tools**
▪ Installation of a Patch	▪ Web Application Security Scanners
▪ Patch Management Tools	▪ Web Server Security Scanners
Web Server Security Tools	▪ Web Server Malware Infection Monitoring Tools
▪ Web Application Security Scanners	▪ Web Server Security Tools
▪ Web Server Security Scanners	▪ Web Server Pen Testing Tools
▪ Web Server Security Tools	
~~**Web Server Pen Testing**~~	
~~▪ Web Server Penetration Testing~~	
▪ Web Server Pen Testing Tools	
Module 14: Hacking Web Applications	**Module 14: Hacking Web Applications**
Web App Concepts	**Web Application Concepts**
▪ Introduction to Web Applications	▪ Introduction to Web Applications
▪ Web Application Architecture	▪ Web Application Architecture
~~▪ Web 2.0 Applications~~	▪ Web Services
▪ Vulnerability Stack	▪ Vulnerability Stack
Web App Threats	**Web Application Threats**
▪ OWASP Top 10 Application Security Risks – 2017	▪ OWASP Top 10 Application Security Risks – 2017
○ A1 - Injection Flaws	○ A1 - Injection Flaws
• SQL Injection Attacks	• SQL Injection Attacks
• Command Injection Attacks	• Command Injection Attacks
✓ Command Injection Example	✓ Command Injection Example
• File Injection Attack	• File Injection Attack
• LDAP Injection Attacks	• LDAP Injection Attacks
○ A2 - Broken Authentication	• Other Injection Attacks
○ A3 - Sensitive Data Exposure	✓ Server-Side JS Injection
○ A4 - XML External Entity (XXE)	✓ Server-Side Include Injection
○ A5 - Broken Access Control	✓ Server-Side Template Injection
○ A6 - Security Misconfiguration	✓ Log Injection
○ A7 - Cross-Site Scripting (XSS) Attacks	✓ HTML Injection
• Cross-Site Scripting Attack Scenario: Attack via Email	✓ CRLF Injection
• XSS Attack in Blog Posting	○ A2 - Broken Authentication
• XSS Attack in Comment Field	○ A3 - Sensitive Data Exposure
• Websites Vulnerable to XSS Attack	○ A4 - XML External Entity (XXE)
○ A8 - Insecure Deserialization	○ A5 - Broken Access Control
○ A9 - Using Components with Known	○ A6 - Security Misconfiguration

Vulnerabilities	
○ A10 - Insufficient Logging and Monitoring	○ A7 - Cross-Site Scripting (XSS) Attacks
▪ Other Web Application Threats	• Cross-Site Scripting Attack Scenario: Attack via Email
○ Directory Traversal	• XSS Attack in Blog Posting
○ Unvalidated Redirects and Forwards	• XSS Attack in Comment Field
○ Watering Hole Attack	○ A8 - Insecure Deserialization
○ Cross-Site Request Forgery (CSRF) Attack	○ A9 - Using Components with Known Vulnerabilities
○ Cookie/Session Poisoning	○ A10 - Insufficient Logging and Monitoring
○ Web Services Architecture	▪ Other Web Application Threats
○ Web Services Attack	○ Directory Traversal
○ Web Services Footprinting Attack	○ Unvalidated Redirects and Forwards
○ Web Services XML Poisoning	○ Watering Hole Attack
○ Hidden Field Manipulation Attack	○ Cross-Site Request Forgery (CSRF) Attack
Hacking Methodology	○ Cookie/Session Poisoning
▪ Web App Hacking Methodology	○ Web Service Attack
▪ Footprint Web Infrastructure	○ Web Service Footprinting Attack
○ Server Discovery	○ Web Service XML Poisoning
○ Service Discovery	○ Hidden Field Manipulation Attack
○ Server Identification/Banner Grabbing	○ Web-based Timing Attacks
○ Detecting Web App Firewalls and Proxies on Target Site	○ MarioNet Attack
○ Hidden Content Discovery	○ Clickjacking Attack
○ Web Spidering Using Burp Suite	○ DNS Rebinding Attack
○ Web Crawling Using Mozenda Web Agent Builder	**Web Application Hacking Methodology**
▪ Attack Web Servers	▪ Web Application Hacking Methodology
▪ Analyze Web Applications	▪ Footprint Web Infrastructure
○ Identify Entry Points for User Input	○ Server Discovery
○ Identify Server- Side Technologies	○ Service Discovery
○ Identify Server- Side Functionality	○ Server Identification/Banner Grabbing
○ Map the Attack Surface	○ Detecting Web App Firewalls and Proxies on Target Site
▪ Bypass Client-Side Controls	○ Hidden Content Discovery
○ Attack Hidden Form Fields	○ Detect Load Balancers
○ Attack Browser Extensions	▪ Analyze Web Applications
○ Perform Source Code Review	○ Identify Entry Points for User Input
▪ Attack Authentication Mechanism	○ Identify Server-Side Technologies
○ User Name Enumeration	○ Identify Server-Side Functionality

○ Password Attacks: Password Functionality Exploits	○ Identify Files and Directories
○ Password Attacks: Password Guessing and Brute-forcing	○ Identify Web Application Vulnerabilities
○ Session Attacks: Session ID Prediction/Brute-forcing	○ Map the Attack Surface
○ Cookie Exploitation: Cookie Poisoning	▪ Bypass Client-side Controls
▪ Attack Authorization Schemes	○ Attack Hidden Form Fields
○ HTTP Request Tampering	○ Attack Browser Extensions
○ Cookie Parameter Tampering	○ Perform Source Code Review
▪ Attack Access Controls	○ Evade XSS Filters
▪ Attack Session Management Mechanism	▪ Attack Authentication Mechanism
○ Attacking Session Token Generation Mechanism	○ Design and Implementation Flaws in Authentication Mechanism
○ Attacking Session Tokens Handling Mechanism: Session Token Sniffing	○ Username Enumeration
▪ Perform Injection/Input Validation Attacks	○ Password Attacks: Password Functionality Exploits
▪ Attack Application Logic Flaws	○ Password Attacks: Password Guessing and Brute-forcing
▪ Attack Database Connectivity	○ Password Attacks: Attack Password Reset Mechanism
○ Connection String Injection	○ Session Attacks: Session ID Prediction/Brute-forcing
○ Connection String Parameter Pollution (CSPP) Attacks	○ Cookie Exploitation: Cookie Poisoning
○ Connection Pool DoS	○ Bypass Authentication: Bypass SAML-based SSO
▪ Attack Web App Client	▪ Attack Authorization Schemes
▪ Attack Web Services	○ Authorization Attack: HTTP Request Tampering
○ Web Services Probing Attacks	○ Authorization Attack: Cookie Parameter Tampering
○ Web Service Attacks: SOAP Injection	▪ Attack Access Controls
○ Web Service Attacks: XML Injection	▪ Attack Session Management Mechanism
○ Web Services Parsing Attacks	○ Attacking Session Token Generation Mechanism
○ Web Service Attack Tools	○ Attacking Session Tokens Handling Mechanism: Session Token Sniffing
Web App Hacking Tools	▪ Perform Injection/Input Validation Attacks
▪ Web Application Hacking Tools	○ Perform Local File Inclusion (LFI)
Countermeasures	▪ Attack Application Logic Flaws
▪ Web Application Fuzz Testing	▪ Attack Shared Environments

▪ Source Code Review	▪ Attack Database Connectivity
▪ Encoding Schemes	○ Connection String Injection
▪ How to Defend Against Injection Attacks	○ Connection String Parameter Pollution (CSPP) Attacks
▪ Web Application Attack Countermeasures	○ Connection Pool DoS
▪ How to Defend Against Web Application Attacks	▪ Attack Web Application Client
Web App Security Testing Tools	▪ Attack Web Services
▪ Web Application Security Testing Tools	○ Web Services Probing Attacks
▪ Web Application Firewall	○ Web Service Attacks: SOAP Injection
~~**Web App Pen Testing**~~	○ Web Service Attacks: SOAPAction Spoofing
~~▪ Web Application Pen Testing~~	○ Web Service Attacks: WS-Address Spoofing
~~○ Information Gathering~~	○ Web Service Attacks: XML Injection
~~○ Configuration Management Testing~~	○ Web Services Parsing Attacks
~~○ Authentication Testing~~	○ Web Service Attack Tools
~~○ Session Management Testing~~	▪ Additional Web Application Hacking Tools
~~○ Authorization Testing~~	**Web API, Webhooks, and Web Shell**
~~○ Data Validation Testing~~	▪ What is Web API?
~~○ Denial-of-Service Testing~~	○ Web Services APIs
~~○ Web Services Testing~~	▪ What are Webhooks?
~~○ AJAX Testing~~	○ Webhooks Vs. APIs
▪ Web Application Pen Testing Framework	▪ OWASP Top 10 API Security Risks
	▪ API Vulnerabilities
	▪ Web API Hacking Methodology
	○ Identify the Target
	○ Detect Security Standards
	○ Identify the Attack Surface
	○ Launch Attacks
	• Fuzzing
	• Invalid Input Attacks
	• Malicious Input Attacks
	• Injection Attacks
	• Exploiting Insecure Configurations
	✓ Insecure SSL Configuration
	✓ Insecure Direct Object References (IDOR)
	✓ Insecure Session/Authentication Handling
	• Login/ Credential Stuffing Attacks
	• API DDoS Attacks

	• Authorization Attacks on API: OAuth Attacks
	• Other Techniques to Hack an API
	✓ Reverse Engineering
	✓ User Spoofing
	✓ Man-in-the-Middle Attack
	✓ Session Replay Attack
	✓ Social Engineering
	○ REST API Vulnerability Scanning
	○ Bypassing IDOR via Parameter Pollution
	▪ Web Shells
	○ Web Shell Tools
	▪ Gaining Backdoor Access via Web Shell
	▪ How to Prevent Installation of a Web Shell
	▪ Web Shell Detection Tools
	▪ Secure API Architecture
	▪ API Security Risks and Solutions
	▪ Best Practices for API Security
	▪ Best Practices for Securing Webhooks
	Web Application Security
	▪ Web Application Security Testing
	○ Manual Web App Security Assessment
	○ Automated Web App Security Assessment
	○ Static Application Security Testing (SAST)
	○ Dynamic Application Security Testing (DAST)
	▪ Web Application Fuzz Testing
	▪ Source Code Review
	▪ Encoding Schemes
	▪ Whitelisting vs. Blacklisting Applications
	○ Application Whitelisting and Blacklisting Tools
	▪ How to Defend Against Injection Attacks
	▪ Web Application Attack Countermeasures
	▪ How to Defend Against Web Application Attacks
	▪ RASP for Protecting Web Servers
	▪ Bug Bounty Programs
	▪ Web Application Security Testing Tools
	▪ Web Application Firewalls

Module 15: SQL Injection	**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	▪ 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 Messages Returned	• Blind SQL Injection: No Error Message Returned
• Blind SQL Injection: WAITFOR DELAY (YES or NO Response)	• Blind SQL Injection: WAITFOR DELAY (YES or NO Response)
• Blind SQL Injection: Boolean Exploitation and Heavy Query	• Blind SQL Injection: Boolean Exploitation and Heavy Query
○ Out-of-Band SQL injection	○ Out-of-Band SQL injection
SQL Injection Methodology	**SQL Injection Methodology**
▪ SQL Injection Methodology	▪ Information Gathering and SQL Injection Vulnerability Detection
○ Information Gathering and SQL Injection Vulnerability Detection	○ Information Gathering
• Information Gathering	○ Identifying Data Entry Paths
• Identifying Data Entry Paths	○ Extracting Information through Error Messages
• Extracting Information through Error Messages	○ SQL Injection Vulnerability Detection: Testing for SQL Injection
• Testing for SQL Injection	○ Additional Methods to Detect SQL Injection
• Additional Methods to Detect SQL Injection	○ SQL Injection Black Box Pen Testing
• SQL Injection Black Box Pen Testing	○ Source Code Review to Detect SQL Injection Vulnerabilities

• Source Code Review to Detect SQL Injection Vulnerabilities	○ Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL
• Testing for Blind SQL Injection Vulnerability in MySQL and MSSQL	▪ Launch SQL Injection Attacks
○ Launch SQL Injection Attacks	○ Perform Union SQL Injection
• Perform Union SQL Injection	○ Perform Error Based SQL Injection
• Perform Error Based SQL Injection	○ Perform Error Based SQL Injection using Stored Procedure Injection
• Perform Error Based SQL Injection using Stored Procedure Injection	○ Bypass Website Logins Using SQL Injection
• Bypass Website Logins Using SQL Injection	○ Perform Blind SQL Injection – Exploitation (MySQL)
• Perform Blind SQL Injection – Exploitation (MySQL)	○ Blind SQL Injection - Extract Database User
• Blind SQL Injection - Extract Database User	○ Blind SQL Injection - Extract Database Name
• Blind SQL Injection - Extract Database Name	○ Blind SQL Injection - Extract Column Name
• Blind SQL Injection - Extract Column Name	○ Blind SQL Injection - Extract Data from ROWS
• Blind SQL Injection - Extract Data from ROWS	○ Perform Double Blind SQL Injection – Classical Exploitation (MySQL)
• Perform Double Blind SQL Injection – Classical Exploitation (MySQL)	○ Perform Blind SQL Injection Using Out-of-Band Exploitation Technique
• Perform Blind SQL Injection Using Out of Band Exploitation Technique	○ Exploiting Second-Order SQL Injection
• Exploiting Second-Order SQL Injection	○ Bypass Firewall using SQL Injection
• Bypass Firewall using SQL Injection	○ Perform SQL Injection to Insert a New User and Update Password
• Perform SQL Injection to Insert a New User and Update Password	○ Exporting a Value with Regular Expression Attack
• Exporting a Value with Regular Expression Attack	▪ Advanced SQL Injection
○ Advanced SQL Injection	○ Database, Table, and Column Enumeration
• Database, Table, and Column Enumeration	○ Advanced Enumeration
• Advanced Enumeration	○ Features of Different DBMSs
• Features of Different DBMSs	○ Creating Database Accounts
• Creating Database Accounts	○ Password Grabbing
• Password Grabbing	○ Grabbing SQL Server Hashes
• Grabbing SQL Server Hashes	○ Transfer Database to Attacker's Machine
• Extracting SQL Hashes (In a Single Statement	○ Interacting with the Operating System
• Transfer Database to Attacker's Machine	○ Interacting with the File System
• Interacting with the Operating System	○ Network Reconnaissance Using SQL Injection

• Interacting with the File System	○ Network Reconnaissance Full Query
• Network Reconnaissance Using SQL Injection	○ Finding and Bypassing Admin Panel of a Website
• Network Reconnaissance Full Query	○ PL/SQL Exploitation
• Finding and Bypassing Admin Panel of a Website	○ Creating Server Backdoors using SQL Injection
• PL/SQL Exploitation	○ HTTP Header-Based SQL Injection
• Creating Server Backdoors using SQL Injection	○ DNS Exfiltration using SQL Injection
SQL Injection Tools	○ Case Study: SQL Injection Attack and Defense
▪ SQL Injection Tools	**SQL Injection Tools**
○ SQL Power Injector and sqlmap	▪ SQL Injection Tools
○ The Mole and jSQL Injection	▪ SQL Injection Tools for Mobile Devices
▪ SQL Injection Tools	**Evasion Techniques**
▪ SQL Injection Tools for Mobile	▪ Evading IDS
Evasion Techniques	▪ Types of Signature Evasion Techniques
▪ Evading IDS	○ In-line Comment
▪ Types of Signature Evasion Techniques	○ Char Encoding
○ In-line Comment	○ String Concatenation
○ Char Encoding	○ Obfuscated Codes
○ String Concatenation	○ Manipulating White Spaces
○ Obfuscated Codes	○ Hex Encoding
○ Manipulating White Spaces	○ Sophisticated Matches
○ Hex Encoding	○ URL Encoding
○ Sophisticated Matches	○ Null Byte
○ URL Encoding	○ Case Variation
○ Null Byte	○ Declare Variables
○ Case Variation	○ IP Fragmentation
○ Declare Variable	○ Variations
○ IP Fragmentation	**Countermeasures**
Countermeasures	▪ How to Defend Against SQL Injection Attacks
▪ How to Defend Against SQL Injection Attacks	○ Use Type-Safe SQL Parameters
○ Use Type-Safe SQL Parameters	○ Defenses in the Application
▪ SQL Injection Detection Tools	• Input Validation
○ IBM Security AppScan and Acunetix Web Vulnerability Scanner	• Output Encoding
○ Snort Rule to Detect SQL Injection Attacks	• Enforcing Least Privilege
▪ SQL Injection Detection Tools	▪ Detecting SQL Injection Attacks
	▪ SQL Injection Detection Tools

	○ OWASP ZAP
	○ Damn Small SQLi Scanner (DSSS)
	○ Snort
	○ SQL Injection Detection Tools
Module 16: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
Wireless Concepts	**Wireless Concepts**
▪ Wireless Terminologies	▪ 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 Modes
▪ Wi-Fi Authentication Process Using a Centralized Authentication Server	▪ Wi-Fi Authentication Process Using a Centralized Authentication Server
▪ Types of Wireless Antennas	▪ Types of Wireless Antennas
Wireless Encryption	**Wireless Encryption**
▪ Types of Wireless Encryption	▪ Types of Wireless Encryption
○ WEP (Wired Equivalent Privacy) Encryption	○ Wired Equivalent Privacy (WEP) Encryption
○ WPA (Wi-Fi Protected Access) Encryption	○ Wi-Fi Protected Access (WPA) Encryption
○ WPA2 (Wi-Fi Protected Access 2) Encryption	○ WPA2 Encryption
▪ WEP vs. WPA vs. WPA2	○ WPA3 Encryption
▪ WEP Issues	▪ Comparison of WEP, WPA, WPA2, and WPA3
▪ Weak Initialization Vectors (IV)	▪ Issues in WEP, WPA, and WPA2
Wireless Threats	**Wireless Threats**
▪ Wireless Threats	▪ Wireless Threats
○ Rogue Access Point Attack	○ Rogue AP Attack
○ Client Mis-association	○ Client Mis-association
○ Misconfigured Access Point Attack	○ Misconfigured AP Attack
○ Unauthorized Association	○ Unauthorized Association
○ Ad Hoc Connection Attack	○ Ad-Hoc Connection Attack
○ Honeypot Access Point Attack	○ Honeypot AP Attack
○ AP MAC Spoofing	○ AP MAC Spoofing
○ Denial-of-Service Attack	○ Denial-of-Service Attack
○ Key Reinstallation Attack (KRACK)	○ Key Reinstallation Attack (KRACK)
○ Jamming Signal Attack	○ Jamming Signal Attack
• Wi-Fi Jamming Devices	• Wi-Fi Jamming Devices
Wireless Hacking Methodology	○ aLTEr Attack
▪ Wireless Hacking Methodology	○ Wormhole Attack

○ Wi-Fi Discovery	○ Sinkhole Attack
• Footprint the Wireless Network	**Wireless Hacking Methodology**
• Find Wi-Fi Networks in Range to Attack	▪ Wireless Hacking Methodology
• Wi-Fi Discovery Tools	▪ Wi-Fi Discovery
• Mobile-based Wi-Fi Discovery Tools	○ Wireless Network Footprinting
○ GPS Mapping	○ Finding Wi-Fi Networks in Range to Attack
• GPS Mapping Tools	○ Finding WPS-Enabled APs
• Wi-Fi Hotspot Finder Tools	○ Wi-Fi Discovery Tools
• How to Discover Wi-Fi Network Using Wardriving	○ Mobile-based Wi-Fi Discovery Tools
○ Wireless Traffic Analysis	▪ GPS Mapping
• Choosing the Right Wi-Fi Card	○ GPS Mapping Tools
• Wi-Fi USB Dongle: AirPcap	○ Wi-Fi Hotspot Finder Tools
• Wi-Fi Packet Sniffer	○ Wi-Fi Network Discovery Through WarDriving
• Perform Spectrum Analysis	▪ Wireless Traffic Analysis
○ Launch Wireless Attacks	○ Choosing the Optimal Wi-Fi Card
• Aircrack-ng Suite	○ Sniffing Wireless Traffic
• How to Reveal Hidden SSIDs	○ Perform Spectrum Analysis
• Fragmentation Attack	▪ Launch of Wireless Attacks
• How to Launch MAC Spoofing Attack	○ Aircrack-ng Suite
• Denial-of-Service: Disassociation and Deauthentication Attacks	○ Detection of Hidden SSIDs
• Man-in-the-Middle Attack	○ Fragmentation Attack
• MITM Attack Using Aircrack-ng	○ MAC Spoofing Attack
• Wireless ARP Poisoning Attack	○ Denial-of-Service: Disassociation and De-authentication Attacks
• Rogue Access Points	○ Man-in-the-Middle Attack
• Evil Twin	○ MITM Attack Using Aircrack-ng
• How to Set Up a Fake Hotspot (Evil Twin)	○ Wireless ARP Poisoning Attack
○ Crack Wi-Fi Encryption	• ARP Poisoning Attack Using Ettercap
• How to Break WEP Encryption	○ Rogue APs
• How to Crack WEP Using Aircrack-ng	• Creation of a Rogue AP Using MANA Toolkit
• How to Break WPA/WPA2 Encryption	○ Evil Twin
• How to Crack WPA-PSK Using Aircrack-ng	• Set Up of a Fake Hotspot (Evil Twin)
• WEP Cracking and WPA Brute Forcing Using Cain & Abel	○ aLTEr Attack
Wireless Hacking Tools	○ Wi-Jacking Attack
▪ WEP/WPA Cracking Tools	▪ Wi-Fi Encryption Cracking

▪ WEP/WPA Cracking Tool for Mobile	○ WEP Encryption Cracking
▪ Wi-Fi Sniffer	○ Cracking WEP Using Aircrack-ng
▪ Wi-Fi Traffic Analyzer Tools	○ WPA/WPA2 Encryption Cracking
▪ Other Wireless Hacking Tools	○ Cracking WPA-PSK Using Aircrack-ng
Bluetooth Hacking	○ Cracking WPA/WPA2 Using Wifiphisher
▪ Bluetooth Stack	○ Cracking WPS Using Reaver
▪ Bluetooth Hacking	○ WPA3 Encryption Cracking
▪ Bluetooth Threats	○ WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker
▪ How to BlueJack a Victim	**Wireless Hacking Tools**
▪ Bluetooth Hacking Tools	▪ WEP/WPA/WPA2 Cracking Tools
Countermeasures	▪ WEP/WPA/WPA2 Cracking Tools for Mobile
▪ Wireless Security Layers	▪ Wi-Fi Packet Sniffers
▪ How to Defend Against WPA/WPA2 Cracking	▪ Wi-Fi Traffic Analyzer Tools
▪ How to Defend Against KRACK Attacks	▪ Other Wireless Hacking Tools
▪ How to Detect and Block Rogue AP	**Bluetooth Hacking**
▪ How to Defend Against Wireless Attacks	▪ Bluetooth Stack
▪ How to Defend Against Bluetooth Hacking	▪ Bluetooth Hacking
Wireless Security Tools	▪ Bluetooth Threats
▪ Wireless Intrusion Prevention Systems	▪ Bluejacking
▪ Wireless IPS Deployment	▪ Bluetooth Reconnaissance Using Bluez
▪ Wi-Fi Security Auditing Tools	▪ Btlejacking Using BtleJack
▪ Wi-Fi Intrusion Prevention System	▪ Bluetooth Hacking Tools
▪ Wi-Fi Predictive Planning Tools	**Countermeasures**
▪ Wi-Fi Vulnerability Scanning Tools	▪ Wireless Security Layers
▪ Bluetooth Security Tools	▪ Defense Against WPA/WPA2/WPA3 Cracking
▪ Wi-Fi Security Tools for Mobile	▪ Defense Against KRACK Attacks
~~**Wireless Pen Testing**~~	▪ Defense Against aLTEr Attacks
~~▪ Wireless Penetration Testing~~	▪ Detection and Blocking of Rogue APs
~~▪ Wireless Penetration Testing Framework~~	▪ Defense Against Wireless Attacks
~~○ Pen Testing for General Wi-Fi Network Attack~~	▪ Defense Against Bluetooth Hacking
~~○ Pen Testing WEP Encrypted WLAN~~	**Wireless Security Tools**
~~○ Pen Testing WPA/WPA2 Encrypted WLAN~~	▪ Wireless Intrusion Prevention Systems
~~○ Pen Testing LEAP Encrypted WLAN~~	▪ WIPS Deployment
~~○ Pen Testing Unencrypted WLAN~~	▪ 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 – 2016
▪ Anatomy of a Mobile Attack	▪ Anatomy of a Mobile Attack
▪ How a Hacker can Profit from Mobile when 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
Hacking Android OS	▪ Agent Smith Attack
▪ Android OS	▪ Exploiting SS7 Vulnerability
○ Android Device Administration API	▪ Simjacker: SIM Card Attack
▪ Android Rooting	**Hacking Android OS**
○ Rooting Android Using KingoRoot	▪ Android OS
○ Android Rooting Tools	○ Android Device Administration API
▪ Blocking Wi-Fi Access using NetCut	▪ Android Rooting
▪ Hacking with zANTI	○ Rooting Android Using KingoRoot
▪ Hacking Networks Using Network Spoofer	○ Android Rooting Tools
▪ Launching DoS Attack using Low Orbit Ion Cannon (LOIC)	▪ Hacking Android Devices
▪ Performing Session Hijacking Using DroidSheep	○ Blocking Wi-Fi Access Using NetCut
▪ Hacking with Orbot Proxy	○ Identifying Attack Surfaces Using drozer
▪ Android-based Sniffers	○ Hacking with zANTI and Network Spoofer
▪ Android Trojans	○ Launch DoS Attack using Low Orbit Ion Cannon (LOIC)
▪ Securing Android Devices	○ Session Hijacking Using DroidSheep
▪ Android Security Tool: Find My Device	○ Hacking with Orbot Proxy
▪ Android Security Tools	○ Exploiting Android Device through ADB Using PhoneSploit

▪ Android Vulnerability Scanner	○ Android-based Sniffers
▪ Android Device Tracking Tools	○ Launching Man-in-the-Disk Attack
Hacking iOS	○ Launching Sphearphone Attack
▪ Apple iOS	○ Other Techniques for Hacking Android Devices
▪ Jailbreaking iOS	• Advanced SMS Phishing
○ Jailbreaking Techniques	• Bypass SSL Pinning
○ Jailbreaking of iOS 11.2.1 Using Cydia	• Tap ’n Ghost Attack
○ Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang	○ Android Trojans
○ Jailbreaking Tools	▪ Android Hacking Tools
▪ iOS Trojans	▪ Securing Android Devices
▪ Guidelines for Securing iOS Devices	▪ Android Security Tools
▪ iOS Device Tracking Tools	○ Android Device Tracking Tools: Google Find My Device
▪ iOS Device Security Tools	○ Android Device Tracking Tools
~~**Mobile Spyware**~~	○ Android Vulnerability Scanners
~~▪ Mobile Spyware~~	○ Online Android Analyzers
~~▪ Mobile Spyware: mSpy~~	**Hacking iOS**
~~▪ Mobile Spywares~~	▪ Apple iOS
Mobile Device Management	▪ Jailbreaking iOS
▪ Mobile Device Management (MDM)	○ Jailbreaking Techniques
▪ Mobile Device Management Solutions	○ Jailbreaking of iOS 13.2 Using Cydia
▪ Bring Your Own Device (BYOD)	○ Jailbreaking of iOS 13.2 Using Hexxa Plus
○ BYOD Risks	○ Jailbreaking Tools
○ BYOD Policy Implementation	▪ Hacking iOS Devices
○ BYOD Security Guidelines	○ Hacking using Spyzie
Mobile Security Guidelines and Tools	○ Hacking Network using Network Analyzer Pro
▪ General Guidelines for Mobile Platform Security	○ iOS Trustjacking
▪ Mobile Device Security Guidelines for Administrator	○ iOS Malware
▪ SMS Phishing Countermeasures	○ iOS Hacking Tools
▪ Mobile Protection Tools	▪ Securing iOS Devices
▪ Mobile Anti-Spyware	▪ iOS Device Security Tools
~~**Mobile Pen Testing**~~	▪ iOS Device Tracking Tools
~~▪ Android Phone Pen Testing~~	**Mobile Device Management**
~~▪ iPhone Pen Testing~~	▪ Mobile Device Management (MDM)
▪ Mobile Pen Testing Toolkit: Hackode	▪ Mobile Device Management Solutions
	○ IBM MaaS360
	○ Citrix Endpoint Management

	▪ Bring Your Own Device (BYOD)
	○ BYOD Risks
	○ BYOD Policy Implementation
	○ BYOD Security Guidelines
	Mobile Security Guidelines and Tools
	▪ OWASP Top 10 Mobile Controls
	▪ General Guidelines for Mobile Platform Security
	▪ Mobile Device Security Guidelines for Administrator
	▪ SMS Phishing Countermeasures
	▪ Reverse Engineering Mobile Applications
	▪ Mobile Security Tools
	○ Source Code Analysis Tools
	○ Reverse Engineering Tools
	○ App Repackaging Detector
	○ Mobile Protection Tools
	○ Mobile Anti-Spyware
	○ Mobile Pen Testing Toolkit: ImmuniWeb® MobileSuite
Module 18: IoT Hacking	**Module 18: IoT and OT Hacking**
IoT Concepts	**IoT Hacking**
▪ What is IoT	**IoT Concepts**
▪ How IoT Works	▪ What is the IoT?
▪ IoT Architecture	▪ How the IoT Works
▪ IoT Application Areas and Devices	▪ IoT Architecture
▪ IoT Technologies and Protocols	▪ IoT Application Areas and Devices
▪ IoT Communication Models	▪ IoT Technologies and Protocols
▪ Challenges of IoT	▪ IoT Communication Models
▪ Threat vs Opportunity	▪ Challenges of IoT
IoT Attacks	▪ Threat vs Opportunity
▪ IoT Security Problems	**IoT Attacks**
▪ OWASP Top 10 IoT Vulnerabilities and Obstacles	▪ IoT Security Problems
▪ IoT Attack Surface Areas	▪ OWASP Top 10 IoT Threats
▪ IoT Threats	▪ OWASP IoT Attack Surface Areas
▪ Hacking IoT Devices: General Scenario	▪ IoT Vulnerabilities
▪ IoT Attacks	▪ IoT Threats
○ DDoS Attack	▪ Hacking IoT Devices: General Scenario
○ Exploit HVAC	▪ IoT Attacks

○ Rolling Code Attack	○ DDoS Attack
○ BlueBorne Attack	○ Exploit HVAC
○ Jamming Attack	○ Rolling Code Attack
○ Hacking Smart Grid / Industrial Devices: Remote Access using Backdoor	○ BlueBorne Attack
○ Other IoT Attacks	○ Jamming Attack
▪ IoT Attacks in Different Sectors	○ Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor
▪ Case Study: Dyn Attack	○ SDR-Based Attacks on IoT
IoT Hacking Methodology	○ Identifying and Accessing Local IoT Devices
▪ What is IoT Device Hacking?	○ Fault Injection Attacks
▪ IoT Hacking Methodology	○ Other IoT Attacks
○ Information Gathering Using Shodan	▪ IoT Attacks in Different Sectors
○ Information Gathering using MultiPing	▪ Case Study: Dyn Attack
○ Vulnerability Scanning using Nmap	**IoT Hacking Methodology**
○ Vulnerability Scanning using RIoT Vulnerability Scanner	▪ What is IoT Device Hacking?
○ Sniffing using Foren6	▪ IoT Hacking Methodology
○ Rolling code Attack using RFCrack	○ Information Gathering Using Shodan
○ Hacking Zigbee Devices with Attify Zigbee Framework	○ Information Gathering using MultiPing
○ BlueBorne Attack Using HackRF One	○ Information Gathering using FCC ID Search
○ Gaining Remote Access using Telnet	○ Discovering IoT Devices with Default Credentials using IoTSeeker
○ Maintain Access by Exploiting Firmware	○ Vulnerability Scanning using Nmap
IoT Hacking Tools	○ Vulnerability Scanning using RIoT Vulnerability Scanner
▪ Information Gathering Tools	○ Sniffing using Foren6
▪ Sniffing Tools	○ Sniffing using Wireshark
▪ Vulnerability Scanning Tools	○ Analyzing Spectrum and IoT Traffic
▪ IoT Hacking Tools	○ Rolling code Attack using RFCrack
Countermeasures	○ Hacking Zigbee Devices with Attify Zigbee Framework
▪ How to Defend Against IoT Hacking	○ BlueBorne Attack Using HackRF One
▪ General Guidelines for IoT Device Manufacturing Companies	○ Replay Attack using HackRF One
▪ OWASP Top 10 IoT Vulnerabilities Solutions	○ SDR-Based Attacks using RTL-SDR and GNU Radio
▪ IoT Framework Security Considerations	○ Side Channel Attack using ChipWhisperer
▪ IoT Security Tools	○ Gaining Remote Access using Telnet
~~**IoT Pen Testing**~~	○ Maintain Access by Exploiting Firmware

~~▪ IoT Pen Testing~~	○ Firmware Analysis and Reverse Engineering
	IoT Hacking Tools
	▪ Information-Gathering Tools
	▪ Sniffing Tools
	▪ Vulnerability-Scanning Tools
	▪ Tools to Perform SDR-Based Attacks
	▪ IoT Hacking Tools
	Countermeasures
	▪ How to Defend Against IoT Hacking
	▪ General Guidelines for IoT Device Manufacturing Companies
	▪ OWASP Top 10 IoT Vulnerabilities Solutions
	▪ IoT Framework Security Considerations
	▪ IoT Device Management
	▪ IoT Security Tools
	OT Hacking
	OT Concepts
	▪ What is OT?
	▪ Essential Terminology
	▪ IT/OT Convergence (IIOT)
	▪ The Purdue Model
	▪ Challenges of OT
	▪ Introduction to ICS
	▪ Components of an ICS
	○ Distributed Control System (DCS)
	○ Supervisory Control and Data Acquisition (SCADA)
	○ Programmable Logic Controller (PLC)
	○ Basic Process Control System (BPCS)
	○ Safety Instrumented Systems (SIS)
	▪ OT Technologies and Protocols
	OT Attacks
	▪ OT Vulnerabilities
	▪ OT Threats
	▪ OT Attacks
	○ HMI-based Attacks
	○ Side-Channel Attacks
	• Timing Analysis
	• Power Analysis

	○ Hacking Programmable Logic Controller (PLC)
	○ Hacking Industrial Systems through RF Remote Controllers
	• Replay Attack
	• Command Injection
	• Re-pairing with Malicious RF controller
	• Malicious Reprogramming Attack
	○ OT Malware
	▪ OT Malware Analysis: LockerGoga Ransomware
	OT Hacking Methodology
	▪ What is OT Hacking?
	▪ OT Hacking Methodology
	○ Identifying ICS/SCADA Systems using Shodan
	○ Gathering Default Passwords using CRITIFENCE
	○ Scanning ICS/SCADA Systems using Nmap
	○ Enumerating Slave Controllers using SCADA Shutdown Tool
	○ Vulnerability Scanning using Nessus
	○ Vulnerability Scanning using Skybox Vulnerability Control
	○ Sniffing using NetworkMiner
	○ Analyzing Modbus/TCP Traffic Using Wireshark
	○ Discovering ICS/SCADA Network Topology using GRASSMARLIN
	○ Hacking ICS Hardware
	○ Hacking Modbus Slaves using Metasploit
	○ Hacking PLC using modbus-cli
	○ Gaining Remote Access using DNP3
	OT Hacking Tools
	▪ Information-Gathering Tools
	▪ Sniffing and Vulnerability-Scanning Tools
	▪ OT Hacking Tools
	Countermeasures
	▪ How to Defend Against OT Hacking
	▪ OT Vulnerabilities and Solutions
	▪ How to Secure an IT/OT Environment
	▪ International OT Security Organizations
	▪ OT Security Solutions
	▪ OT Security Tools

Module 19: Cloud Computing	**Module 19: Cloud Computing**
Cloud Computing Concepts	**Cloud Computing Concepts**
▪ Introduction to Cloud Computing	▪ Introduction to Cloud Computing
▪ Separation of Responsibilities in Cloud	▪ Types of Cloud Computing Services
▪ Cloud Deployment Models	▪ Separation of Responsibilities in Cloud
▪ NIST Cloud Deployment Reference Architecture	▪ Cloud Deployment Models
~~▪ Cloud Computing Benefits~~	▪ NIST Cloud Deployment Reference Architecture
~~▪ Understanding Virtualization~~	▪ Cloud Storage Architecture
Cloud Computing Threats	▪ Role of AI in Cloud Computing
▪ Cloud Computing Threats	▪ Virtual Reality and Augmented Reality on Cloud
Cloud Computing Attacks	▪ Cloud Service Providers
▪ Service Hijacking using Social Engineering Attacks	**Container Technology**
▪ Service Hijacking using Network Sniffing	▪ What is a Container?
▪ Session Hijacking using XSS Attack	○ Container Technology Architecture
▪ Session Hijacking using Session Riding	▪ Containers Vs. Virtual Machines
▪ Domain Name System (DNS) Attacks	▪ What is Docker?
▪ Side Channel Attacks or Cross-guest VM Breaches	○ Docker Engine
▪ SQL Injection Attacks	○ Docker Architecture
▪ Cryptanalysis Attacks	○ Microservices Vs. Docker
▪ Wrapping Attack	○ Docker Networking
▪ Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks	▪ Container Orchestration
▪ Man-in-the-Cloud Attack	▪ What is Kubernetes?
Cloud Security	○ Kubernetes Cluster Architecture
▪ Cloud Security Control Layers	○ Kubernetes Vs. Docker
▪ Cloud Security is the Responsibility of both Cloud Provider and Consumer	▪ Container Security Challenges
▪ Cloud Computing Security Considerations	▪ Container Management Platforms
▪ Placement of Security Controls in the Cloud	▪ Kubernetes Platforms
▪ Best Practices for Securing Cloud	**Serverless Computing**
▪ NIST Recommendations for Cloud Security	▪ What is Serverless Computing?
▪ Organization/Provider Cloud Security Compliance Checklist	▪ Serverless Vs. Containers
Cloud Security Tools	▪ Serverless Computing Frameworks
▪ Cloud Security Tools	**Cloud Computing Threats**
~~**Cloud Penetration Testing**~~	▪ OWASP Top 10 Cloud Security Risks
~~▪ What is Cloud Pen Testing?~~	▪ OWASP Top 10 Serverless Security Risks
~~▪ Key Considerations for Pen Testing in the Cloud~~	▪ Cloud Computing Threats

~~▪ Cloud Penetration Testing~~	▪ Container Vulnerabilities
~~▪ Recommendations for Cloud Testing~~	▪ Kubernetes Vulnerabilities
	▪ Cloud Attacks
	○ Service Hijacking using Social Engineering
	○ Service Hijacking using Network Sniffing
	○ Side-Channel Attacks or Cross-guest VM Breaches
	○ Wrapping Attack
	○ Man-in-the-Cloud (MITC) Attack
	○ Cloud Hopper Attack
	○ Cloud Cryptojacking
	○ Cloudborne Attack
	○ Other Cloud Attacks
	Cloud Hacking
	▪ What is Cloud Hacking?
	▪ Hacking Cloud
	○ Container Vulnerability Scanning using Trivy
	○ Kubernetes Vulnerability Scanning using Sysdig
	○ Enumerating S3 Buckets
	• Inspecting HTML
	• Brute-Forcing URL
	• Finding Subdomains
	• Reverse IP Search
	• Advanced Google Hacking
	○ Identifying Open S3 Buckets using S3Scanner
	○ Enumerating Kubernetes etcd
	○ Enumerating AWS Account IDs
	○ Enumerating IAM Roles
	○ Enumerating Bucket Permissions using S3Inspector
	○ Exploiting Amazon Cloud Infrastructure using Nimbostratus
	○ Exploiting Misconfigured AWS S3 Buckets
	○ Compromising AWS IAM Credentials
	○ Hijacking Misconfigured IAM Roles using Pacu
	○ Cracking AWS Access Keys using DumpsterDiver
	○ Exploiting Docker Containers on AWS using Cloud Container Attack Tool (CCAT)

	○ Exploiting Docker Remote API
	○ Hacking Container Volumes
	○ CloudGoat AWS – Vulnerable by Design
	○ Gaining Access by Exploiting SSRF Vulnerability
	○ AWS IAM Privilege Escalation Techniques
	○ Escalating Privileges of Google Storage Buckets using GCPBucketBrute
	○ Backdooring Docker Images using dockerscan
	○ Maintaining Access and Covering Tracks on AWS Cloud Environment by Manipulating CloudTrial Service
	▪ AWS Hacking Tool: AWS pwn
	Cloud Security
	▪ Cloud Security Control Layers
	▪ Cloud Security is the Responsibility of both Cloud Provider and Consumer
	▪ Cloud Computing Security Considerations
	▪ Placement of Security Controls in the Cloud
	▪ Best Practices for Securing Cloud
	▪ NIST Recommendations for Cloud Security
	▪ Kubernetes Vulnerabilities and Solutions
	▪ Serverless Security Risks and Solutions
	▪ Best Practices for Container Security
	▪ Best Practices for Docker Security
	▪ Best Practices for Kubernetes Security
	▪ Best Practices for Serverless Security
	▪ Zero Trust Networks
	▪ Organization/Provider Cloud Security Compliance Checklist
	▪ International Cloud Security Organizations
	▪ Cloud Security Tools
	▪ Container Security Tools
	▪ Kubernetes Security Tools
	▪ Serverless Application Security Solutions
Module 20: Cryptography	**Module 20: Cryptography**
Cryptography Concepts	**Cryptography Concepts**
▪ Cryptography	▪ Cryptography
○ Types of Cryptography	○ Types of Cryptography
▪ Government Access to Keys (GAK)	▪ Government Access to Keys (GAK)

Encryption Algorithms	**Encryption Algorithms**
▪ Ciphers	▪ Ciphers
▪ Data Encryption Standard (DES)	▪ Data Encryption Standard (DES)
▪ Advanced Encryption Standard (AES)	▪ Advanced Encryption Standard (AES)
▪ RC4, RC5, and RC6 Algorithms	▪ RC4, RC5, and RC6 Algorithms
▪ Twofish	▪ Twofish
▪ The DSA and Related Signature Schemes	▪ Threefish
▪ Rivest Shamir Adleman (RSA)	▪ Serpent
▪ Diffie-Hellman	▪ TEA
▪ Message Digest (One-Way Hash) Functions	▪ CAST-128
○ Message Digest Function: MD5	▪ GOST Block Cipher
○ Secure Hashing Algorithm (SHA)	▪ Camellia
○ RIPEMD - 160	▪ DSA and Related Signature Schemes
○ HMAC	▪ Rivest Shamir Adleman (RSA)
Cryptography Tools	▪ Diffie-Hellman
▪ MD5 Hash Calculators	▪ YAK
▪ Hash Calculators for Mobile	▪ Message Digest (One-Way Hash) Functions
▪ Cryptography Tools	○ Message Digest Function: MD5 and MD6
○ Advanced Encryption Package 2017	○ Message Digest Function: Secure Hashing Algorithm (SHA)
○ BCTextEncoder	○ RIPEMD - 160
○ Cryptography Tools	○ HMAC
▪ Cryptography Tools for Mobile	▪ Other Encryption Techniques
▪ **Public Key Infrastructure (PKI)**	○ Elliptic Curve Cryptography
○ Public Key Infrastructure (PKI)	○ Quantum Cryptography
○ Certification Authorities	○ Homomorphic Encryption
Signed Certificate (CA) Vs. Self Signed Certificate	○ Hardware-Based Encryption
▪ **Email Encryption**	▪ Comparison of Cryptographic Algorithms
▪ Digital Signature	**Cryptography Tools**
▪ Secure Sockets Layer (SSL)	▪ MD5 and MD6 Hash Calculators
▪ Transport Layer Security (TLS)	▪ Hash Calculators for Mobile
○ Cryptography Toolkit	▪ Cryptography Tools
○ OpenSSL	▪ Cryptography Tools for Mobile
▪ Keyczar	**Public Key Infrastructure (PKI)**
Pretty Good Privacy (PGP)	▪ Public Key Infrastructure (PKI)
▪ **Disk Encryption**	○ Certification Authorities
▪ Disk Encryption	○ Signed Certificate (CA) Vs. Self Signed Certificate
○ Disk Encryption Tools	**Email Encryption**

○ VeraCrypt	▪ Digital Signature
○ Symantec Drive Encryption	▪ Secure Sockets Layer (SSL)
Disk Encryption Tools	▪ Transport Layer Security (TLS)
▪ **Cryptanalysis**	▪ Cryptography Toolkits
○ Cryptanalysis Methods	▪ Pretty Good Privacy (PGP)
○ Linear Cryptanalysis	▪ GNU Privacy Guard (CPG)
○ Differential Cryptanalysis	▪ Web of Trust (WOT)
▪ Integral Cryptanalysis	▪ Email Encryption Tools
▪ Code Breaking Methodologies	**Disk Encryption**
○ Cryptography Attacks	▪ Disk Encryption
○ Brute-Force Attack	▪ Disk Encryption Tools: VeraCrypt and Symantec Drive Encryption
• Birthday Attack	▪ Disk Encryption Tools
• Birthday Paradox: Probability	**Cryptanalysis**
○ Meet-in-the-Middle Attack on Digital Signature Schemes	▪ Cryptanalysis Methods
○ Side Channel Attack	○ Linear Cryptanalysis
○ Hash Collision Attack	○ Differential Cryptanalysis
○ DUHK Attack	○ Integral Cryptanalysis
○ Rainbow Table Attack	▪ Code Breaking Methodologies
▪ Cryptanalysis Tools	▪ Cryptography Attacks
▪ Online MD5 Decryption Tools	○ Brute-Force Attack
▪ **Countermeasures**	○ Birthday Attack
○ How to Defend Against Cryptographic Attacks	○ Birthday Paradox: Probability
	○ Meet-in-the-Middle Attack on Digital Signature Schemes
	○ Side-Channel Attack
	○ Hash Collision Attack
	○ DUHK Attack
	○ Rainbow Table Attack
	○ Related-Key Attack
	○ Padding Oracle Attack
	○ DROWN Attack
	▪ Cryptanalysis Tools
	▪ Online MD5 Decryption Tools
	Countermeasures
	▪ How to Defend Against Cryptographic Attacks
	▪ Key Stretching
	○ PBKDF2
	○ Bcrypt

Labs Comparison

The notations used:

1. **Red** points are new labs in CEHv11
2. **Blue** points are substantially modified labs in CEHv11
3. ~~**Striked**~~ labs are removed from CEHv10

CEHv10	CEHv11
Module 01: Introduction to Ethical Hacking	**Module 01: Introduction to Ethical Hacking**
Module 02: Footprinting and Reconnaissance	**Module 02: Footprinting and Reconnaissance**
1. Open Source Information Gathering using Windows Command Line Utilities	1. Perform Footprinting Through Search Engines
~~2. Finding Company's Sub-domains using Sublist3r~~	1.1 Gather Information using Advanced Google Hacking Techniques
~~3. Gathering Personal Information using Online People Search Services~~	1.2 Gather Information from Video Search Engines
~~4. Gathering Information from LinkedIn using InSpy~~	1.3 Gather Information from FTP Search Engines
~~5. Collecting Information About a Target Website using Firebug~~	1.4 Gather Information from IoT Search Engines
6. Extracting a Company's Data using Web Data Extractor	2. Perform Footprinting Through Web Services
7. Mirroring Website using HTTrack Web Site Copier	2.1 Find the Company's Domains and Sub-domains using Netcraft
8. Collecting Information About a Target by Tracing Emails	2.2 Gather Personal Information using PeekYou Online People Search Service
~~9. Gathering IP and Domain Name Information using Whois Lookup~~	2.3 Gather an Email List using theHarvester
10. Advanced Network Route Tracing Using Path Analyzer Pro	2.4 Gather Information using Deep and Dark Web Searching
11. Footprinting a Target using Maltego	2.5 Determine Target OS Through Passive Footprinting
12. Performing Automated Network Reconnaissance using Recon-ng	3. Perform Footprinting Through Social Networking Sites
13. Using the Open-source Reconnaissance Tool Recon-ng to Gather Personnel Information	3.1 Gather Employees' Information from LinkedIn using theHarvester
~~14. Collecting Information from Social Networking Sites using Recon-ng Pushpin~~	3.2 Gather Personal Information from Various Social Networking Sites using Sherlock
15. Automated Fingerprinting of an Organization using FOCA	3.3 Gather Information using Followerwonk
16. Open Source Intelligence Gathering using	4. Perform Website Footprinting

OSRFramework	
17. Information Gathering using Metasploit	4.1 Gather Information About a Target Website using Ping Command Line Utility
18. Information Gathering using theHarvester	4.2 Gather Information About a Target Website using Website Informer
	4.3 Extract a Company's Data using Web Data Extractor
	4.4 Mirror a Target Website using HTTrack Web Site Copier
	4.5 Gather a Wordlist from the Target Website using CeWL
	5. Perform Email Footprinting
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro
	6. Perform Whois Footprinting
	6.1 Perform Whois Lookup using DomainTools
	7. Perform DNS Footprinting
	7.1 Gather DNS Information using nslookup Command Line Utility and Online Tool
	7.2 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon
	8. Perform Network Footprinting
	8.1 Locate the Network Range
	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
	9.1 Footprinting a Target using Recon-ng
	9.2 Footprinting a Target using Maltego
	9.3 Footprinting a Target using OSRFramework
	9.4 Footprinting a Target using FOCA
	9.5 Footprinting a Target using BillCipher
	9.6 Footprinting a Target using OSINT Framework
Module 03: Scanning Networks	**Module 03: Scanning Networks**
1. Scanning the Network using the Colasoft Packet Builder	1. Perform Host Discovery
2. UDP and TCP Packet Crafting Techniques using HPING3	1.1 Perform Host Discovery using Nmap

3. Basic Network Troubleshooting using MegaPing	1.2 Perform Host Discovery using Angry IP Scanner
4. Understanding Network Scanning using Nmap	2. Perform Port and Service Discovery
5. Scanning a Network using NetScan Tools Pro	2.1 Perform Port and Service Discovery using MegaPing
~~6. Scanning for Network Traffic Going through a Computer's Adapter using IP-Tools~~	2.2 Perform Port and Service Discovery using NetScanTools Pro
7. Checking for Live Systems using Angry IP Scanner	2.3 Explore Various Network Scanning Techniques using Nmap
8. Exploring Various Network Scanning Techniques	2.4 Explore Various Network Scanning Techniques using Hping3
9. Perform ICMP Probing using Ping/Traceroute for Network Troubleshooting	3. Perform OS Discovery
10. Avoiding Scanning Detection using Multiple Decoy IP Addresses	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark
~~11. Daisy Chaining using Proxy Workbench~~	3.2 Perform OS Discovery using Nmap Script Engine (NSE)
12. Anonymous Browsing using Proxy Switcher	3.3 Perform OS Discovery using Unicornscan
13. Anonymous Browsing using CyberGhost	4. Scan beyond IDS and Firewall
14. Identify Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark	4.1 Scan beyond IDS/Firewall using various Evasion Techniques
15. Drawing Network Diagrams using Network Topology Mapper	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall
	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall
	4.4 Create Custom Packets using Nmap to Scan beyond IDS/Firewall
	4.5 Browse Anonymously using Proxy Switcher
	4.6 Browse Anonymously using CyberGhost VPN
	5. Draw Network Diagrams
	5.1 Draw Network Diagrams using Network Topology Mapper
	6. Perform Network Scanning using Various Scanning Tools
	6.1 Scan a Target Network using Metasploit
Module 04: Enumeration	**Module 04: Enumeration**
1. NetBIOS Enumeration using Global Network Inventory	1. Perform NetBIOS Enumeration
2. Enumerating Network Resources using Advanced IP canner	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities

~~3. Performing Network Enumeration using SuperScan~~	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator
~~4. Enumerating Resources in a Local Machine using Hyena~~	1.3 Perform NetBIOS Enumeration using an NSE Script
5. Performing Network Enumeration using NetBIOS Enumerator	2. Perform SNMP Enumeration
6. Enumerating a Network using SoftPerfect Network Scanner	2.1 Perform SNMP Enumeration using snmp-check
7. Enumerating a Target Network using Nmap and Net Use	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner
~~8. Enumerating Services on a Target Machine~~	3. Perform LDAP Enumeration
~~9. SNMP Enumeration using snmp_enum~~	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)
10. LDAP Enumeration using Active Directory Explorer (ADExplorer)	4. Perform NFS Enumeration
11. Enumerating Information from Windows and Samba Host using Enum4linux	4.1 Perform NFS Enumeration using RPCScan and SuperEnum
	5. Perform DNS Enumeration
	5.1 Perform DNS Enumeration using Zone Transfer
	5.2 Perform DNS Enumeration using DNSSEC Zone Walking
	6. Perform RPC, SMB, and FTP Enumeration
	6.1 Perform RPC and SMB Enumeration using NetScanTools Pro
	6.2 Perform RPC, SMB, and FTP Enumeration using Nmap
	7. Perform Enumeration using Various Enumeration Tools
	7.1 Enumerate Information using Global Network Inventory
	7.2 Enumerate Network Resources using Advanced IP Scanner
	7.3 Enumerate Information from Windows and Samba Hosts using Enum4linux
Module 05: Vulnerability Analysis	**Module 05: Vulnerability Analysis**
1. Vulnerability Analysis using Nessus	1. Perform Vulnerability Research with Vulnerability Scoring Systems and Databases
2. Scanning for Network Vulnerabilities using the GFI LanGuard	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)
3. CGI Scanning with Nikto	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)
	2. Perform Vulnerability Assessment using Various Vulnerability Assessment Tools
	2.1 Perform Vulnerability Analysis using OpenVAS
	2.2 Perform Vulnerability Scanning using Nessus
	2.3 Perform Vulnerability Scanning using GFI LanGuard
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto
Module 06: System Hacking	**Module 06: System Hacking**
1. Active Online Attack using Responder	1. Gain Access to the System
~~2. Dumping and Cracking SAM Hashes to Extract Plaintext Passwords~~	1.1 Perform Active Online Attack to Crack the System's Password using Responder
~~3. Creating and using the Rainbow Tables~~	1.2 Audit System Passwords using L0phtCrack
4. Auditing System Passwords using L0phtCrack	1.3 Find Vulnerabilities on Exploit Sites
5. Exploiting Client Side Vulnerabilities and Establishing a VNC Session	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session
6. Escalating Privileges by Exploiting Client Side Vulnerabilities	1.5 Gain Access to a Remote System using Armitage
7. Hacking Windows Server 2012 with a Malicious Office Document using TheFatRat	1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat
8. Hacking Windows 10 using Metasploit and Post-Exploitation using Meterpreter	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System
9. User System Monitoring and Surveillance using Spytech SpyAgent	2. Perform Privilege Escalation to Gain Higher Privileges
10. Web Activity Monitoring and Recording using Power Spy	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities
11. Hiding Files using NTFS Streams	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter
12. Hiding Data using White Space Steganography	3. Maintain Remote Access and Hide Malicious Activities
13. Image Steganography using OpenStego	3.1 User System Monitoring and Surveillance using Power Spy
~~14. Image Steganography using Quick Stego~~	3.2 User System Monitoring and Surveillance using Spytech SpyAgent
15. Covert channels using Covert_TCP	3.3 Hide Files using NTFS Streams
16. Viewing, Enabling and Clearing Audit Policies	3.4 Hide Data using White Space

using Auditpol	Steganography
	3.5 Image Steganography using OpenStego
	3.6 Covert Channels using Covert_TCP
	4. Clear Logs to Hide the Evidence of Compromise
	4.1 View, Enable, and Clear Audit Policies using Auditpol
	4.2 Clear Windows Machine Logs using Various Utilities
	4.3 Clear Linux Machine Logs using the BASH Shell
	4.4 Clear Windows Machine Logs using CCleaner
Module 07: Malware Threats	**Module 07: Malware Threats**
1. Gaining Control over a Victim Machine using njRAT	1. Gain Access to the Target System using Trojans
2. Obfuscating a Trojan using SwayzCryptor and Making it Undetectable to Various Anti-Virus Programs	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan
~~3. Creating a Trojan Server using the GUI Trojan MoSucker~~	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs
4. Creating a Server using the ProRat Tool	1.3 Create a Server using the ProRat Tool
5. Creating a Trojan Server using Theef	1.4 Create a Trojan Server using Theef RAT Trojan
~~6. Creating a HTTP Trojan and Remote Controlling a Target Machine using HTTP RAT~~	2. Infect the Target System using a Virus
7. Creating a Virus using the JPS Virus Maker Tool	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System
~~8. Creating a Worm using the Internet Worm Maker Thing~~	3. Perform Static Malware Analysis
9. Virus Analysis using VirusTotal	3.1 Perform Online Malware Scanning using VirusTotal
10. Virus Analysis using IDA Pro	3.2 Perform a Strings Search using BinText
11. Virus Analysis using OllyDbg	3.3 Identify Packaging and Obfuscation Methods using PEid
12. Monitoring TCP/IP Connections using the CurrPorts	3.4 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer
13. Performing Registry Entry Monitoring	3.5 Identify File Dependencies using Dependency Walker
14. Startup Program Monitoring Tool	3.6 Perform Malware Disassembly using IDA and OllyDbg

15. Perform Device Driver Monitoring	4. Perform Dynamic Malware Analysis
16. Detecting Trojans	4.1 Perform Port Monitoring using TCPView and CurrPorts
~~17. Removing Malware using ClamWin~~	4.2 Perform Process Monitoring using Process Monitor
	4.3 Perform Registry Monitoring using Regshot and jv16 PowerTools
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol
	4.6 Perform Installation Monitoring using Mirekusoft Install Monitor
	4.7 Perform Files and Folder Monitoring using PA File Sight
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Booster
	4.9 Perform DNS Monitoring using DNSQuerySniffer
Module 08: Sniffing	**Module 08: Sniffing**
1. Performing Man-in-the-Middle Attack using Cain & Abel	1. Perform Active Sniffing
2. Spoofing MAC Address using SMAC	1.1 Perform MAC Flooding using macof
3. Sniffing Passwords using Wireshark	1.2 Perform a DHCP Starvation Attack using Yersinia
4. Analyzing a Network using the Capsa Network Analyzer	1.3 Perform ARP Poisoning using arpspoof
5. Sniffing the Network using the Omnipeek Network Analyzer	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel
6. Detecting ARP Poisoning in a Switch Based Network	1.5 Spoof a MAC Address using TMAC and SMAC
7. Detecting ARP Attacks with XArp Tool	2. Perform Network Sniffing using Various Sniffing Tools
	2.1 Perform Password Sniffing using Wireshark
	2.2 Analyze a Network using the Capsa Network Analyzer
	2.3 Analyze a Network using the Omnipeek Network Protocol Analyzer
	2.4 Analyze a Network using the SteelCentral Packet Analyzer
	3. Detect Network Sniffing
	3.1 Detect ARP Poisoning in a Switch-Based

	Network
	3.2 Detect ARP Attacks using Xarp
	3.3 Detect Promiscuous Mode using Nmap and NetScanTools Pro
Module 09: Social Engineering	**Module 09: Social Engineering**
1. Detecting Phishing using Netcraft	1. Perform Social Engineering using Various Techniques
2. Detecting Phishing using PhishTank	1.1 Sniff Users' Credentials using the Social-Engineer Toolkit (SET)
3. Sniffing Facebook Credentials using Social Engineering Toolkit (SET)	1.2 Perform Phishing using ShellPhish
~~4. Phishing User Credentials using SpeedPhish Framework (SPF)~~	2. Detect a Phishing Attack
	2.1 Detect Phishing using Netcraft
	2.2 Detect Phishing using PhishTank
	3. Audit Organization's Security for Phishing Attacks
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish
Module 10: Denial-of-Service	**Module 10: Denial-of-Service**
1. SYN Flooding a Target Host using Metasploit	1. Perform DoS and DDoS Attacks using Various Techniques
2. SYN Flooding a Target Host using hping3	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit
3. Performing Distributed Denial of Service Attack using HOIC	1.2 Perform a DoS Attack on a Target Host using hping3
~~4. Detecting and Analyzing DoS Attack Traffic using KFSensor and Wireshark~~	1.3 Perform a DDoS Attack using HOIC
	1.4 Perform a DDoS Attack using LOIC
	2. Detect and Protect Against DoS and DDoS Attacks
	2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian
Module 11: Session Hijacking	**Module 11: Session Hijacking**
1. Session Hijacking using the Zed Attack Proxy (ZAP)	1. Perform Session Hijacking
2. Perform sslstrip and Intercept HTTP Traffic through BetterCAP	1.1 Hijack a Session using Zed Attack Proxy (ZAP)
	1.2 Intercept HTTP Traffic using bettercap

	2. Detect Session Hijacking
	2.1 Detect Session Hijacking using Wireshark
Module 12: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
1. Detecting Intrusions using Snort	1. Perform Intrusion Detection using Various Tools
2. Detecting Malicious Network Traffic using HoneyBOT	1.1 Detect Intrusions using Snort
3. ~~Detecting Intruders and Worms using KFSensor Honeypot IDS~~	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019
4. Bypassing Windows Firewall using Nmap Evasion Techniques	1.3 Detect Malicious Network Traffic using HoneyBOT
5. Bypassing Firewall Rules using HTTP/FTP Tunneling	2. Evade Firewalls using Various Evasion Techniques
6. ~~Bypassing Windows Firewall using Metasploit~~	2.1 Bypass Windows Firewall using Nmap Evasion Techniques
	2.2 Bypass Firewall Rules using HTTP/FTP Tunneling
Module 13: Hacking Web Servers	**Module 13: Hacking Web Servers**
1. Performing Web Server Reconnaissance using Skipfish	1. Footprint the Web Server
2. Footprinting a Web Server using the httprecon Tool	1.1 Information Gathering using Ghost Eye
3. Footprinting a Web Server using ID Serve	1.2 Perform Web Server Reconnaissance using Skipfish
4. Uniscan Web Server Fingerprinting in Kali Linux	1.3 Footprint a Web Server using the httprecon Tool
5. Cracking FTP Credentials using Dictionary Attack	1.4 Footprint a Web Server using ID Serve
	1.5 Footprint a Web Server using Netcat and Telnet
	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)
	1.7 Uniscan Web Server Fingerprinting in Parrot Security
	2. Perform a Web Server Attack
	2.1 Crack FTP Credentials using a Dictionary Attack
Module 14: Hacking Web Applications	**Module 14: Hacking Web Applications**
1. Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications	1. Footprint the Web Infrastructure

2. Performing Cross-Site Request Forgery (CSRF) Attack	1.1 Perform Web Application Reconnaissance
3. Enumerating and Hacking a Web Application using WPScan and Metasploit	1.2 Perform Web Application Reconnaissance using WhatWeb
4. Exploiting Remote Command Execution Vulnerability to Compromise a Target Web Server	1.3 Perform Web Spidering using OWASP ZAP
5. Exploiting File Upload Vulnerability at Different Security Levels	1.4 Detect Load Balancers using Various Tools
~~6. Website Vulnerability Scanning using Acunetix WVS~~	1.5 Identify Web Server Directories
7. Auditing Web Application Framework using Vega	1.6 Perform Web Application Vulnerability Scanning using Vega
	1.7 Identify Clickjacking Vulnerability using iframe
	2. Perform Web Application Attacks
	2.1 Perform a Brute-force Attack using Burp Suite
	2.2 Perform Parameter Tampering using Burp Suite
	2.3 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications
	2.4 Perform Cross-Site Request Forgery (CSRF) Attack
	2.5 Enumerate and Hack a Web Application using WPScan and Metasploit
	2.6 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server
	2.7 Exploit a File Upload Vulnerability at Different Security Levels
	2.8 Gain Backdoor Access via a Web Shell using Weevely
	3. Detect Web Application Vulnerabilities using Various Web Application Security Tools
	3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner
Module 15: SQL Injection	**Module 15: SQL Injection**
1. SQL Injection Attacks on MSSQL Database	1. Perform SQL Injection Attacks
2. Performing SQL Injection Attack against MSSQL to Extract Databases and WebShell using SQLMAP	1.1 Perform an SQL Injection Attack on an MSSQL Database

~~3. Testing for SQL Injection using IBM Security AppScan Tool~~	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap
4. Scanning Web Applications using N-Stalker Tool	2. Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools
	2.1 Detect SQL Injection Vulnerabilities using DSSS
	2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP
Module 16: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
1. WiFi Packet Sniffing using Microsoft Network Monitor and Wireshark	1. Footprint a Wireless Network
2. Cracking a WEP Network with Aircrack-ng	1.1 Find Wi-Fi Networks in Range using NetSurveyor
3. Cracking a WPA Network with Aircrack-ng	2. Perform Wireless Traffic Analysis
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark
	3. Perform Wireless Attacks
	3.1 Find Hidden SSIDs using Aircrack-ng
	3.2 Crack a WEP Network using Wifiphisher
	3.3 Crack a WEP Network using Aircrack-ng
	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 using MANA-Toolkit
Module 17: Hacking Mobile Platforms	**Module 17: Hacking Mobile Platforms**
1. Creating Binary Payloads using Kali Linux to Hack Android	1. Hack Android Devices
2. Harvesting Users' Credentials using Social Engineering Toolkit	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security
3. Using Mobile Platform to Enforce a DoS Attack on a Target Website	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit
~~4. Hacking Android Device with a Malicious App using TheFatRat~~	1.3 Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform
5. Securing Android Devices from Malicious Applications	1.4 Exploit the Android Platform through ADB using PhoneSploit
	2. Secure Android Devices using Various Android Security Tools
	2.1 Analyze a Malicious App using Online Android Analyzers

	2.2 Analyze a Malicious App using Quixxi Vulnerability Scanner
	2.3 Secure Android Devices from Malicious Apps using Malwarebytes Security
Module 18: IoT Hacking	**Module 18: IoT and OT Hacking**
	1. Perform Footprinting using Various Footprinting Techniques
	1.1 Gather Information using Online Footprinting Tools
	2. Capture and Analyze IoT Device Traffic
	2.1 Capture and Analyze IoT Traffic using Wireshark
Module 19: Cloud Computing	**Module 19: Cloud Computing**
~~1. Building a Cloud using ownCloud and LAMPServer~~	1. Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools
~~2. Securing ownCloud from Malicious File Uploads using ClamAV~~	1.1 Enumerate S3 Buckets using lazys3
~~3. Bypassing ownCloud AV and Hacking the Host using Kali Linux~~	1.2 Enumerate S3 Buckets using S3Scanner
~~4. Implementing DoS Attack on Linux Cloud Server using Slowloris Script~~	2. Exploit S3 Buckets
	2.1 Exploit Open S3 Buckets using AWS CLI
	3. Perform Privilege Escalation to Gain Higher Privileges
	3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy
Module 20: Cryptography	**Module 20: Cryptography**
1. Calculating One-way Hashes using HashCalc	1. Encrypt the Information using Various Cryptography Tools
2. Calculating MD5 Hashes using MD5 Calculator	1.1 Calculate One-way Hashes using HashCalc
3. Understanding File and Text Encryption using CryptoForge	1.2 Calculate MD5 Hashes using MD5 Calculator
4. Basic Data Encryption using Advanced Encryption Package	1.3 Calculate MD5 Hashes using HashMyFiles
5. Encrypting and Decrypting the Data using BCTextEncoder	1.4 Perform File and Text Message Encryption using CryptoForge
6. Creating and using Self-Signed Certificates	1.5 Perform File Encryption using Advanced Encryption Package
7. Basic Disk Encryption using VeraCrypt	1.6 Encrypt and Decrypt Data using BCTextEncoder

8. Basic Data Encrypting using Rohos Disk Encryption	2. Create a Self-Signed Certificate
9. Basic Data Encryption using CrypTool	2.1 Create and Use Self-signed Certificates
	3. Perform Email Encryption
	3.1 Perform Email Encryption using Rmail
	4. Perform Disk Encryption
	4.1 Perform Disk Encryption using VeraCrypt
	4.2 Perform Disk Encryption using BitLocker Drive Encryption
	4.3 Perform Disk Encryption using Rohos Disk Encryption
	5. Perform Cryptanalysis using Various Cryptanalysis Tools
	5.1 Perform Cryptanalysis using CrypTool
	5.2 Perform Cryptanalysis using AlphaPeeler