Ethical Hacking and Countermeasures

Version Comparison

CEHv10 Change Summary

1. The Module 05: Vulnerability Analysis is a completely new module in CEHv10
2. The Module 18: IoT Hacking is a completely new module in CEHv10
3. The Module 16: vading IDS, Firewalls, and Honeypots from CEHv9 is moved to Module 12 in CEHv10
4. The Module 07: Malware Threats module includes static and dynamic malware analysis in CEHv10
5. All the tool screenshots are replaced with the latest version
6. All the tool listing slides are updated with the latest tools

Module Comparison

CEHv9	CEHv10
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: System Hacking	Module 05: Vulnerability Analysis
Module 06: Malware Threats	Module 06: System Hacking
Module 07: Sniffing	Module 07: Malware Threats
Module 08: Social Engineering	Module 08: Sniffing

Module 09: Denial-of-Service	Module 09: Social Engineering
Module 10: Session Hijacking	Module 10: Denial-of-Service
Module 11: Hacking Webservers	Module 11: Session Hijacking
Module 12: Hacking Web Applications	Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: SQL Injection	Module 13: Hacking Web Servers
Module 14: Hacking Wireless Networks	Module 14: Hacking Web Applications
Module 15: Hacking Mobile Platforms	Module 15: SQL Injection
Module 16: Evading IDS, Firewalls, and Honeypots	Module 16: Hacking Wireless Networks
Module 17: Cloud Computing Security	Module 17: Hacking Mobile Platforms
Module 18: Cryptography	Module 18: IoT Hacking
	Module 19: Cloud Computing
	Module 20: Cryptography

Courseware Content Comparison

The notations used:

1. **Red** points are new slides in CEHv10
2. **Blue** points are substantially modified in CEHv10
3. ~~**Striked**~~ points are removed from CEHv9

CEHv9	CEHv10
Module 01: Introduction to Ethical Hacking	**Module 01: Introduction to Ethical Hacking**
▪ Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds	▪ Information Security Overview
▪ Information Security Overview	○ Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds
○ ~~Case Study: eBay Data Breach~~	○ Essential Terminology
○ ~~Case Study: Google Play Hack~~	○ Elements of Information Security
○ ~~Case Study: The Home Depot Data Breach~~	○ The Security, Functionality, and Usability Triangle
○ ~~Case Study: JPMorgan Chase Data Breach~~	▪ Information Security Threats and Attack Vectors
○ ~~Year of the Mega Breach~~	○ Motives, Goals, and Objectives of Information Security Attacks
○ ~~Data Breach Statistics~~	○ Top Information Security Attack Vectors
○ ~~Malware Trends in 2015~~	○ Information Security Threat Categories
○ Essential Terminology	○ Types of Attacks on a System
○ Elements of Information Security	○ Information Warfare
○ The Security, Functionality, and Usability Triangle	▪ Hacking Concepts
▪ Information Security Threats and Attack Vectors	○ What is Hacking?
○ Motives, Goals, and Objectives of Information Security Attacks	○ Who is a Hacker?
○ Top Information Security Attack Vectors	○ Hacker Classes
○ Information Security Threats Categories	○ Hacking Phases
○ Types of Attacks on a System	• Reconnaissance
○ Information Warfare	• Scanning
▪ Hacking Concepts, Types, and Phases	• Gaining Access
○ What is Hacking?	• Maintaining Access
○ Who is a Hacker?	• Clearing Tracks
○ Hacker Classes	▪ Ethical Hacking Concepts
○ Hacking Phases	○ What is Ethical Hacking?
• Reconnaissance	○ Why Ethical Hacking is Necessary

• Scanning	○ Scope and Limitations of Ethical Hacking
• Gaining Access	○ Skills of an Ethical Hacker
• Maintaining Access	▪ Information Security Controls
• Clearing Tracks	○ Information Assurance (IA)
▪ Ethical Hacking Concepts and Scope	○ Information Security Management Program
○ What is Ethical Hacking?	○ Enterprise Information Security Architecture (EISA)
○ Why Ethical Hacking is Necessary	○ Network Security Zoning
○ Scope and Limitations of Ethical Hacking	○ Defense-in-Depth
○ Skills of an Ethical Hacker	○ Information Security Policies
▪ Information Security Controls	• Types of Security Policies
○ Information Assurance (IA)	• Examples of Security Policies
○ Information Security Management Program	• Privacy Policies at Workplace
○ Threat Modeling	• Steps to Create and Implement Security Policies
○ Enterprise Information Security Architecture (EISA)	• HR/Legal Implications of Security Policy Enforcement
○ Network Security Zoning	○ Physical Security
○ Defense in Depth	• Types of Physical Security Control
○ Information Security Policies	• Physical Security Controls
• Types of Security Policies	○ What is Risk?
• Examples of Security Policies	• Risk Management
• Privacy Policies at Workplace	• Key Roles and Responsibilities in Risk Management
• Steps to Create and Implement Security Policies	○ Threat Modeling
• HR/Legal Implications of Security Policy Enforcement	○ Incident Management
○ Physical Security	• Incident Management Process
• Physical Security Controls	• Responsibilities of an Incident Response Team
○ Incident Management	○ Security Incident and Event Management (SIEM)
• Incident Management Process	• SIEM Architecture
• Responsibilities of an Incident Response Team	○ User Behavior Analytics (UBA)
○ What is Vulnerability Assessment?	○ Network Security Controls
• Types of Vulnerability Assessment	• Access Control
~~• Network Vulnerability Assessment Methodology~~	• Types of Access Control

• Vulnerability Research	• User Identification, Authentication, Authorization and Accounting
• Vulnerability Research Websites	○ Identity and Access Management (IAM)
○ Penetration Testing	○ Data Leakage
• Why Penetration Testing	• Data Leakage Threats
• Comparing Security Audit, Vulnerability Assessment, and Penetration Testing	• What is Data Loss Prevention (DLP)?
• Blue Teaming/Red Teaming	○ Data Backup
• Types of Penetration Testing	○ Data Recovery
• Phases of Penetration Testing	○ Role of AI/ML in Cyber Security
• Security Testing Methodology	▪ Penetration Testing Concepts
~~• Penetration Testing Methodology~~	○ Penetration Testing
▪ Information Security Laws and Standards	○ Why Penetration Testing
○ Payment Card Industry Data Security Standard (PCI-DSS)	○ Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
○ ISO/IEC 27001:2013	○ Blue Teaming/Red Teaming
○ Health Insurance Portability and Accountability Act (HIPAA)	○ Types of Penetration Testing
○ Sarbanes Oxley Act (SOX)	○ Phases of Penetration Testing
○ The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)	○ Security Testing Methodology
○ Cyber Law in Different Countries	▪ 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	○ Objectives of Footprinting
▪ Footprinting Methodology	▪ Footprinting through Search Engines
○ Footprinting through Search Engines	○ Footprinting through Search Engines

• Finding Company's Public and Restricted Websites	○ Footprint Using Advanced Google Hacking Techniques
• Determining the Operating System	○ Information Gathering Using Google Advanced Search and Image Search
• Collect Location Information	○ Google Hacking Database
• People Search: Social Networking Services Sites/People Search Services	○ VoIP and VPN Footprinting through Google Hacking Database
• People Search Online Services	▪ Footprinting through Web Services
• Gather Information from Financial Services	○ Finding Company's Top-level Domains (TLDs) and Sub-domains
• Footprinting through Job Sites	○ Finding the Geographical Location of the Target
• Monitoring Target Using Alerts	○ People Search on Social Networking Sites and People Search Services
• Information Gathering Using Groups, Forums, and Blogs	○ Gathering Information from LinkedIn
○ Footprinting using Advanced Google Hacking Techniques	○ Gather Information from Financial Services
• Google Advance Search Operators	○ Footprinting through Job Sites
• Google Hacking Databases	○ Monitoring Target Using Alerts
• Information Gathering Using Google Advanced Search	○ Information Gathering Using Groups, Forums, and Blogs
○ Footprinting through Social Networking Sites	○ Determining the Operating System
• Collect Information through Social Engineering on Social Networking Sites	○ VoIP and VPN Footprinting through SHODAN
• Information Available on Social Networking Sites	▪ Footprinting through Social Networking Sites
○ Website Footprinting	○ Collecting Information through Social Engineering on Social Networking Sites
• Website Footprinting using Web Spiders	▪ Website Footprinting
• Mirroring Entire Website	○ Website Footprinting
➢ Website Mirroring Tools	○ Website Footprinting using Web Spiders
• Extract Website Information from http://www.archive.org	○ Mirroring Entire Website
• Monitoring Web Updates Using Website-Watcher	○ Extracting Website Information from https://archive.org
➢ Web Updates Monitoring Tools	○ Extracting Metadata of Public Documents
○ Email Footprinting	○ Monitoring Web Pages for Updates and Changes
• Tracking Email Communications	▪ Email Footprinting
➢ Collecting Information from Email Header	○ Tracking Email Communications

➢ Email Tracking Tools	○ Collecting Information from Email Header
○ Competitive Intelligence	○ Email Tracking Tools
• Competitive Intelligence Gathering	▪ Competitive Intelligence
• Competitive Intelligence - When Did this Company Begin? How Did it Develop?	○ Competitive Intelligence Gathering
• Competitive Intelligence - What Are the Company's Plans?	○ Competitive Intelligence - When Did this Company Begin? How Did it Develop?
• Competitive Intelligence - What Expert Opinions Say About the Company	○ Competitive Intelligence - What Are the Company's Plans?
• Monitoring Website Traffic of Target Company	○ Competitive Intelligence - What Expert Opinions Say About the Company
• Tracking Online Reputation of the Target	○ Monitoring Website Traffic of Target Company
➢ Tools for Tracking Online Reputation of the Target	○ Tracking Online Reputation of the Target
○ WHOIS Footprinting	▪ Whois Footprinting
• WHOIS Lookup	○ Whois Lookup
• WHOIS Lookup Result Analysis	○ Whois Lookup Result Analysis
• WHOIS Lookup Tools	○ Whois Lookup Tools
• WHOIS Lookup Tools for Mobile	○ Finding IP Geolocation Information
○ DNS Footprinting	▪ DNS Footprinting
• Extracting DNS Information	○ Extracting DNS Information
• DNS Interrogation Tools	○ DNS Interrogation Tools
○ Network Footprinting	▪ Network Footprinting
• Locate the Network Range	○ Locate the Network Range
• Traceroute	○ Traceroute
• Traceroute Analysis	○ Traceroute Analysis
• Traceroute Tools	○ Traceroute Tools
○ Footprinting through Social Engineering	▪ Footprinting through Social Engineering
• Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving	○ Footprinting through Social Engineering
▪ Footprinting Tools	○ Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
○ Footprinting Tool	▪ Footprinting Tools
• Maltego	○ Maltego
• Recon-ng	○ Recon-ng
• FOCA	○ FOCA
○ Additional Footprinting Tools	○ Recon-Dog
▪ Footprinting Countermeasures	○ OSRFramework
▪ Footprinting Penetration Testing	○ Additional Footprinting Tools

○ Footprinting Pen Testing	▪ Countermeasures
○ Footprinting Pen Testing Report Templates	○ Footprinting Countermeasures
	▪ Footprinting Pen Testing
	○ Footprinting Pen Testing
	○ Footprinting Pen Testing Report Templates
Module 03: Scanning Networks	**Module 03: Scanning Networks**
~~▪ How Tech Companies Prepare for Cyber Attacks~~	▪ 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	○ Creating Custom Packet Using TCP Flags
▪ CEH Scanning Methodology	○ Scanning in IPv6 Networks
○ Check for Live Systems	▪ Scanning Tools
• Checking for Live Systems - ICMP Scanning	○ Nmap
• Ping Sweep	○ Hping2 / Hping3
➢ Ping Sweep Tools	• Hping Commands
○ Check for Open Ports	○ Scanning Tools
• SSDP Scanning	○ Scanning Tools for Mobile
• Scanning in IPv6 Networks	▪ Scanning Techniques
• Scanning Tool	○ Scanning Techniques
➢ Nmap	• ICMP Scanning - Checking for Live Systems
➢ Hping2 / Hping3	• Ping Sweep - Checking for Live Systems
➢ Hping Commands	➢ Ping Sweep Tools
• Scanning Techniques	• ICMP Echo Scanning
➢ TCP Connect / Full Open Scan	• TCP Connect / Full Open Scan
➢ Stealth Scan (Half-open Scan)	• Stealth Scan (Half-open Scan)
➢ Inverse TCP Flag Scanning	• Inverse TCP Flag Scanning
➢ Xmas Scan	• Xmas Scan
➢ ACK Flag Probe Scanning	• ACK Flag Probe Scanning
➢ IDLE/IPID Header Scan	• IDLE/IPID Header Scan
✓ IDLE Scan: Step 1	• UDP Scanning
✓ IDLE Scan: Step 2 and 3	• SSDP and List Scanning
➢ UDP Scanning	○ Port Scanning Countermeasures
➢ ICMP Echo Scanning/List Scan	▪ Scanning Beyond IDS and Firewall
• Scanning Tool: NetScan Tools Pro	○ IDS/Firewall Evasion Techniques
• Scanning Tools	• Packet Fragmentation
• Scanning Tools for Mobile	• Source Routing

• Port Scanning Countermeasures	• IP Address Decoy
○ Scanning Beyond IDS	• IP Address Spoofing
• IDS Evasion Techniques	➢ IP Spoofing Detection Techniques: Direct TTL Probes
• SYN/FIN Scanning Using IP Fragments	➢ IP Spoofing Detection Techniques: IP Identification Number
○ Banner Grabbing	➢ IP Spoofing Detection Techniques: TCP Flow Control Method
• Banner Grabbing Tools	➢ IP Spoofing Countermeasures
• Banner Grabbing Countermeasures	• Proxy Servers
➢ Disabling or Changing Banner	➢ Proxy Chaining
➢ Hiding File Extensions from Web Pages	➢ Proxy Tools
○ Scan for Vulnerability	➢ Proxy Tools for Mobile
• Vulnerability Scanning	• Anonymizers
• Vulnerability Scanning Tool	➢ Censorship Circumvention Tools: Alkasir and Tails
➢ Nessus	➢ Anonymizers
➢ GAFI LanGuard	➢ Anonymizers for Mobile
➢ Qualys FreeScan	▪ Banner Grabbing
• Network Vulnerability Scanners	○ Banner Grabbing
• Vulnerability Scanning Tools for Mobile	○ How to Identify Target System OS
○ Draw Network Diagrams	○ Banner Grabbing Countermeasures
• Drawing Network Diagrams	▪ Draw Network Diagrams
• Network Discovery Tool	○ Drawing Network Diagrams
➢ Network Topology Mapper	○ Network Discovery and Mapping Tools
➢ OpManager and NetworkView	○ Network Discovery Tools for Mobile
• Network Discovery and Mapping Tools	▪ Scanning Pen Testing
• Network Discovery Tools for Mobile	○ Scanning Pen Testing
○ Prepare Proxies	
• Proxy Servers	
• Proxy Chaining	
• Proxy Tool	
➢ Proxy Switcher	
➢ Proxy Workbench	
➢ TOR and CyberGhost	
• Proxy Tools	
• Proxy Tools for Mobile	

• Free Proxy Servers	
• Introduction to Anonymizers	
➢ Censorship Circumvention Tool: Tails	
➢ G-Zapper	
➢ Anonymizers	
➢ Anonymizers for Mobile	
• Spoofing IP Address	
• IP Spoofing Detection Techniques	
➢ Direct TTL Probes	
➢ IP Identification Number	
➢ TCP Flow Control Method	
• IP Spoofing Countermeasures	
○ Scanning Pen Testing	
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 Tool: SuperScan	○ NetBIOS Enumeration Tools
○ NetBIOS Enumeration Tool: Hyena	○ Enumerating User Accounts
○ NetBIOS Enumeration Tool: Winfingerprint	○ Enumerating Shared Resources Using Net View
○ NetBIOS Enumeration Tool: NetBIOS Enumerator and Nsauditor Network Security Auditor	▪ SNMP Enumeration
○ Enumerating User Accounts	○ SNMP (Simple Network Management Protocol) Enumeration
○ Enumerating Shared Resources Using Net View	○ Working of SNMP
▪ SNMP Enumeration	○ Management Information Base (MIB)
○ SNMP (Simple Network Management Protocol) Enumeration	○ SNMP Enumeration Tools
○ Working of SNMP	▪ LDAP Enumeration
○ Management Information Base (MIB)	○ LDAP Enumeration
○ SNMP Enumeration Tool: OpUtils	○ LDAP Enumeration Tools

○ SNMP Enumeration Tool: Engineer's Toolset	▪ NTP Enumeration
○ SNMP Enumeration Tools	○ NTP Enumeration
▪ LDAP Enumeration	○ NTP Enumeration Commands
○ LDAP Enumeration Tool: Softerra LDAP Administrator	○ NTP Enumeration Tools
○ LDAP Enumeration Tools	▪ SMTP and DNS Enumeration
▪ NTP Enumeration	○ SMTP Enumeration
○ NTP Enumeration Commands	○ SMTP Enumeration Tools
○ NTP Enumeration Tools	○ DNS Enumeration Using Zone Transfer
▪ SMTP Enumeration and DNS Enumeration	▪ Other Enumeration Techniques
○ SMTP Enumeration	○ IPsec Enumeration
○ SMTP Enumeration Tool: NetScanTools Pro	○ VoIP Enumeration
○ SMTP Enumeration Tools	○ RPC Enumeration
○ DNS Zone Transfer Enumeration Using NSLookup	○ Unix/Linux User Enumeration
▪ Enumeration Countermeasures	▪ Enumeration Countermeasures
▪ SMB Enumeration Countermeasures	○ Enumeration Countermeasures
▪ Enumeration Pen Testing	▪ Enumeration Pen Testing
	○ Enumeration Pen Testing
	Module 05: Vulnerability Analysis
	▪ Vulnerability Assessment Concepts
	○ Vulnerability Research
	○ Vulnerability Classification
	○ What is Vulnerability Assessment?
	○ Types of Vulnerability Assessment
	○ Vulnerability-Management Life Cycle
	• Pre-Assessment Phase: Creating a Baseline
	• Vulnerability Assessment Phase
	• Post Assessment Phase
	▪ Vulnerability Assessment Solutions
	○ Comparing Approaches to Vulnerability Assessment
	○ Working of Vulnerability Scanning Solutions
	○ Types of Vulnerability Assessment Tools
	○ Characteristics of a Good Vulnerability Assessment Solution
	○ Choosing a Vulnerability Assessment Tool
	○ Criteria for Choosing a Vulnerability Assessment Tool

	○ Best Practices for Selecting Vulnerability Assessment Tools
	▪ Vulnerability Scoring Systems
	○ Common Vulnerability Scoring System (CVSS)
	○ Common Vulnerabilities and Exposures (CVE)
	○ National Vulnerability Database (NVD)
	○ Resources for Vulnerability Research
	▪ Vulnerability Assessment Tools
	○ Vulnerability Assessment Tools
	• Qualys Vulnerability Management
	• Nessus Professional
	• GFI LanGuard
	• Qualys FreeScan
	• Nikto
	• OpenVAS
	• Retina CS
	• SAINT
	• Microsoft Baseline Security Analyzer (MBSA)
	• AVDS - Automated Vulnerability Detection System
	• Vulnerability Assessment Tools
	○ Vulnerability Assessment Tools for Mobile
	▪ Vulnerability Assessment Reports
	○ Vulnerability Assessment Reports
	○ Analyzing Vulnerability Scanning Report
Module 05: System Hacking	**Module 06: System Hacking**
~~▪ Security Breaches 2014~~	▪ System Hacking Concepts
~~▪ Information at Hand Before System Hacking Stage~~	○ CEH Hacking Methodology (CHM)
▪ System Hacking: Goals	○ System Hacking Goals
▪ CEH Hacking Methodology (CHM)	▪ Cracking Passwords
▪ CEH System Hacking Steps	○ Password Cracking
○ Cracking Passwords	○ Types of Password Attacks
• Password Cracking	• Non-Electronic Attacks
• Types of Password Attacks	• Active Online Attack
• Non-Electronic Attacks	➢ Dictionary, Brute Forcing and Rule-based Attack

• Active Online Attack: Dictionary, Brute Forcing and Rule-based Attack	➢ Password Guessing
• Active Online Attack: Password Guessing	➢ Default Passwords
• Default Passwords	➢ Trojan/Spyware/Keylogger
• Active Online Attack: Trojan/Spyware/Keylogger	➢ Example of Active Online Attack Using USB Drive
• Example of Active Online Attack Using USB Drive	➢ Hash Injection Attack
• Active Online Attack: Hash Injection Attack	➢ LLMNR/NBT-NS Poisoning
• Passive Online Attack: Wire Sniffing	• Passive Online Attack
• Passive Online Attacks: Man-in-the-Middle and Replay Attack	➢ Wire Sniffing
• Offline Attack: Rainbow Table Attacks	➢ Man-in-the-Middle and Replay Attack
• Tools to Create Rainbow Tables: rtgen and Winrtgen	• Offline Attack
• Offline Attack: Distributed Network Attack	➢ Rainbow Table Attack
• Elcomsoft Distributed Password Recovery	➢ Tools to Create Rainbow Tables: rtgen and Winrtgen
• Microsoft Authentication	➢ Distributed Network Attack
• How Hash Passwords Are Stored in Windows SAM?	○ Password Recovery Tools
• NTLM Authentication Process	○ Microsoft Authentication
• Kerberos Authentication	○ How Hash Passwords Are Stored in Windows SAM?
• Password Salting	○ NTLM Authentication Process
• PWdump7 and Fgdump	○ Kerberos Authentication
• Password Cracking Tools: L0phtCrack and Ophcrack	○ Password Salting
• Password Cracking Tools: Cain & Abel and RainbowCrack	○ Tools to Extract the Password Hashes
• Password Cracking Tools	○ Password Cracking Tools
~~• Password Cracking Tools for Mobile: FlexiSPY Password Grabber~~	○ How to Defend against Password Cracking
• How to Defend against Password Cracking	○ How to Defend against LLMNR/NBT-NS Poisoning
~~• Implement and Enforce Strong Security Policy~~	▪ Escalating Privileges
○ Escalating Privileges	○ Privilege Escalation
• Privilege Escalation	○ Privilege Escalation Using DLL Hijacking
• Privilege Escalation Using DLL Hijacking	○ Privilege Escalation by Exploiting Vulnerabilities

• ~~Resetting Passwords Using Command Prompt~~	○ Privilege Escalation Using Dylib Hijacking
• ~~Privilege Escalation Tool: Active@ Password Changer~~	○ Privilege Escalation using Spectre and Meltdown Vulnerabilities
• ~~Privilege Escalation Tools~~	○ Other Privilege Escalation Techniques
• How to Defend Against Privilege Escalation	○ How to Defend Against Privilege Escalation
○ Executing Applications	▪ Executing Applications
• Executing Applications	○ Executing Applications
➢ Executing Applications: RemoteExec	• Tools for Executing Applications
➢ Executing Applications: PDQ Deploy	○ Keylogger
➢ Executing Applications: DameWare Remote Support	• Types of Keystroke Loggers
• Keylogger	• Hardware Keyloggers
➢ Types of Keystroke Loggers	• Keyloggers for Windows
➢ Hardware Keyloggers	• Keyloggers for Mac
➢ Keylogger: All In One Keylogger	○ Spyware
➢ Keyloggers for Windows	• Spyware
➢ Keylogger for Mac: Amac Keylogger for Mac	• USB Spyware
➢ Keyloggers for MAC	• Audio Spyware
• Spyware	• Video Spyware
➢ Spyware: Spytech SpyAgent	• Telephone/Cellphone Spyware
➢ Spyware: Power Spy 2014	• GPS Spyware
➢ Spyware	○ How to Defend Against Keyloggers
➢ USB Spyware: USBSpy	• Anti-Keylogger
➢ Audio Spyware: Spy Voice Recorder and Sound Snooper	○ How to Defend Against Spyware
➢ Video Spyware: WebCam Recorder	• Anti-Spyware
➢ Cellphone Spyware: Mobile Spy	▪ Hiding Files
➢ Telephone/Cellphone Spyware	○ Rootkits
➢ GPS Spyware: SPYPhone	• Types of Rootkits
➢ GPS Spyware	• How Rootkit Works
• How to Defend Against Keyloggers	• Rootkits
➢ Anti-Keylogger: Zemana AntiLogger	➢ Horse Pill
➢ Anti-Keylogger	➢ GrayFish
• How to Defend Against Spyware	➢ Sirefef
➢ Anti-Spyware: SUPERAntiSpyware	➢ Necurs
➢ Anti-Spywares	• Detecting Rootkits
○ Hiding Files	• Steps for Detecting Rootkits

• Rootkits	• How to Defend against Rootkits
➢ Types of Rootkits	• Anti-Rootkits
➢ How Rootkit Works	○ NTFS Data Stream
~~➢ Rootkit: Avatar~~	• How to Create NTFS Streams
➢ Rootkit: Necurs	• NTFS Stream Manipulation
~~➢ Rootkit: Azazel~~	• How to Defend against NTFS Streams
~~➢ Rootkit: ZeroAccess~~	• NTFS Stream Detectors
• Detecting Rootkits	○ What is Steganography?
➢ Steps for Detecting Rootkits	• Classification of Steganography
➢ How to Defend against Rootkits	• Types of Steganography based on Cover Medium
➢ Anti-Rootkit: Stinger and UnHackMe	➢ Whitespace Steganography
➢ Anti-Rootkits	➢ Image Steganography
• NTFS Data Stream	✓ Image Steganography Tools
➢ How to Create NTFS Streams	➢ Document Steganography
➢ NTFS Stream Manipulation	➢ Video Steganography
➢ How to Defend against NTFS Streams	➢ Audio Steganography
➢ NTFS Stream Detector: StreamArmor	➢ Folder Steganography
➢ NTFS Stream Detectors	➢ Spam/Email Steganography
• What is Steganography?	• Steganography Tools for Mobile Phones
➢ Classification of Steganography	• Steganalysis
➢ Types of Steganography based on Cover Medium	• Steganalysis Methods/Attacks on Steganography
✓ Whitespace Steganography Tool: SNOW	• Detecting Steganography (Text, Image, Audio, and Video Files)
✓ Image Steganography	• Steganography Detection Tools
▪ Least Significant Bit Insertion	▪ Covering Tracks
▪ Masking and Filtering	○ Covering Tracks
▪ Algorithms and Transformation	○ Disabling Auditing: Auditpol
▪ Image Steganography: QuickStego	○ Clearing Logs
▪ Image Steganography Tools	○ Manually Clearing Event Logs
✓ Document Steganography: wbStego	○ Ways to Clear Online Tracks
▪ Document Steganography Tools	○ Covering BASH Shell Tracks
✓ Video Steganography	○ Covering Tracks on Network
▪ Video Steganography: OmniHide PRO and Masker	○ Covering Tracks on OS

▪ Video Steganography Tools	○ Covering Tracks Tools
✓ Audio Steganography	▪ Penetration Testing
▪ Audio Steganography: DeepSound	○ Password Cracking
▪ Audio Steganography Tools	○ Privilege Escalation
✓ Folder Steganography: Invisible Secrets 4	○ Executing Applications
▪ Folder Steganography Tools	○ Hiding Files
✓ Spam/Email Steganography: Spam Mimic	○ Covering Tracks
➢ Steganography Tools for Mobile Phones	
• Steganalysis	
➢ Steganalysis Methods/Attacks on Steganography	
➢ Detecting Text and Image Steganography	
➢ Detecting Audio and Video Steganography	
➢ Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro	
➢ Steganography Detection Tools	
○ Covering Tracks	
• Disabling Auditing: Auditpol	
• Clearing Logs	
• Manually Clearing Event Logs	
• Ways to Clear Online Tracks	
• Covering Tracks Tool	
➢ CCleaner	
➢ MRU-Blaster	
• Track Covering Tools	
○ Penetration Testing	
• Password Cracking	
• Privilege Escalation	
• Executing Applications	
• Hiding Files	
• Covering Tracks	

Module 06: Malware Threats	Module 07: Malware Threats
▪ Introduction to Malware	▪ Malware Concepts
○ Different Ways a Malware can Get into a System	○ Introduction to Malware
○ Common Techniques Attackers Use to Distribute Malware on the Web	○ Different Ways a Malware can Get into a System
▪ Trojan Concepts	○ Common Techniques Attackers Use to Distribute Malware on the Web
~~○ Financial Loss Due to Trojans~~	○ Components of Malware
○ What is a Trojan?	▪ Trojan Concepts
○ How Hackers Use Trojans	○ What is a Trojan?
○ Common Ports used by Trojans	○ How Hackers Use Trojans
○ How to Infect Systems Using a Trojan	○ Common Ports used by Trojans
○ Wrappers	○ How to Infect Systems Using a Trojan
○ Dark Horse Trojan Virus Maker	○ Trojan Horse Construction Kit
○ Trojan Horse Construction Kit	○ Wrappers
○ Crypters: AIO FUD Crypter, Hidden Sight Crypter, and Galaxy Crypter	○ Crypters
○ Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor	○ How Attackers Deploy a Trojan
○ How Attackers Deploy a Trojan	○ Exploit Kits
○ Exploit Kit	○ Evading Anti-Virus Techniques
• Exploit Kit	○ Types of Trojans
➢ Infinity	• Remote Access Trojans
➢ Phoenix Exploit Kit and Blackhole Exploit Kit	• Backdoor Trojans
➢ Bleedinglife and Crimepack	• Botnet Trojans
○ Evading Anti-Virus Techniques	• Rootkit Trojans
○ Types of Trojans	• E-banking Trojans
• Command Shell Trojans	➢ Working of E-banking Trojans
• Defacement Trojans	➢ E-banking Trojan: ZeuS
➢ Defacement Trojans: Restorator	• Proxy Server Trojans
• Botnet Trojans	• Covert Channel Trojans
~~➢ Tor-based Botnet Trojans: ChewBacca~~	• Defacement Trojans
~~➢ Botnet Trojans: Skynet and CyberGate~~	• Service Protocol Trojans
• Proxy Server Trojans	• Mobile Trojans
➢ Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)	• IoT Trojans
~~• FTP Trojans~~	• Other Trojans
• VNC Trojans	▪ Virus and Worm Concepts

➢ VNC Trojans: Hesperbot	○ Introduction to Viruses
• HTTP/HTTPS Trojans	○ Stages of Virus Life
➢ HTTP Trojan: HTTP RAT	○ Working of Viruses
➢ Shttpd Trojan - HTTPS (SSL)	○ Indications of Virus Attack
➢ ICMP Tunneling	○ How does a Computer Get Infected by Viruses
• Remote Access Trojans	○ Virus Hoaxes
➢ Optix Pro and MoSucker	○ Fake Antiviruses
➢ BlackHole RAT and SSH - R.A.T	○ Ransomware
➢ njRAT and Xtreme RAT	○ Types of Viruses
➢ SpyGate – RAT and Punisher RAT	• System and File Viruses
➢ DarkComet RAT, Pandora RAT, and HellSpy RAT	• Multipartite and Macro Viruses
➢ ProRat and Theef	• Cluster and Stealth Viruses
➢ Hell Raiser	• Encryption and Sparse Infector Viruses
➢ Remote Access Tool: Atelier Web Remote Commander	• Polymorphic Viruses
• Covert Channel Trojan: CCTT	• Metamorphic Viruses
• E-banking Trojans	• Overwriting File or Cavity Viruses
➢ Working of E-banking Trojans	• Companion/Camouflage and Shell Viruses
➢ E-banking Trojan: ZeuS and SpyEye	• File Extension Viruses
➢ E-banking Trojan: Citadel Builder and Ice IX	• FAT and Logic Bomb Viruses
• Destructive Trojans: M4sT3r Trojan	• Web Scripting and E-mail Viruses
~~• Notification Trojans~~	• Other Viruses
~~• Data Hiding Trojans (Encrypted Trojans)~~	○ Creating Virus
▪ Virus and Worms Concepts	○ Computer Worms
○ Introduction to Viruses	○ Worm Makers
○ Stages of Virus Life	▪ Malware Analysis
○ Working of Viruses	○ What is Sheep Dip Computer?
• Infection Phase	○ Anti-Virus Sensor Systems
• Attack Phase	○ Introduction to Malware Analysis
~~○ Why Do People Create Computer Viruses~~	○ Malware Analysis Procedure: Preparing Testbed
○ Indications of Virus Attack	○ Static Malware Analysis
○ How does a Computer Get Infected by Viruses	• File Fingerprinting
○ Virus Hoaxes and Fake Antiviruses	• Local and Online Malware Scanning
○ Ransomware	• Performing Strings Search
○ Types of Viruses	• Identifying Packing/ Obfuscation Methods
• System or Boot Sector Viruses	• Finding the Portable Executables (PE)

	Information
• File and Multipartite Viruses	• Identifying File Dependencies
• Macro Viruses	• Malware Disassembly
• Cluster Viruses	○ Dynamic Malware Analysis
• Stealth/Tunneling Viruses	• Port Monitoring
• Encryption Viruses	• Process Monitoring
• Polymorphic Code	• Registry Monitoring
• Metamorphic Viruses	• Windows Services Monitoring
• File Overwriting or Cavity Viruses	• Startup Programs Monitoring
• Sparse Infector Viruses	• Event Logs Monitoring/Analysis
• Companion/Camouflage Viruses	• Installation Monitoring
• Shell Viruses	• Files and Folder Monitoring
• File Extension Viruses	• Device Drivers Monitoring
• Add-on and Intrusive Viruses	• Network Traffic Monitoring/Analysis
• Transient and Terminate and Stay Resident Viruses	• DNS Monitoring/ Resolution
○ Writing a Simple Virus Program	• API Calls Monitoring
• Sam's Virus Generator and JPS Virus Maker	○ Virus Detection Methods
• Andreinick05's Batch Virus Maker and DeadLine's Virus Maker	○ Trojan Analysis: ZeuS/Zbot
• Sonic Bat - Batch File Virus Creator and Poison Virus Maker	○ Virus Analysis: WannaCry
○ Computer Worms	▪ Countermeasures
• How Is a Worm Different from a Virus?	○ Trojan Countermeasures
• Computer Worms: Ghost Eye Worm	○ Backdoor Countermeasures
• Worm Maker: Internet Worm Maker Thing	○ Virus and Worms Countermeasures
▪ Malware Reverse Engineering	▪ Anti-Malware Software
○ What is Sheep Dip Computer?	○ Anti-Trojan Software
○ Anti-Virus Sensor Systems	○ Antivirus Software
○ Malware Analysis Procedure: Preparing Testbed	▪ Malware Penetration Testing
○ Malware Analysis Procedure	○ Malware Penetration Testing
○ Malware Analysis Tool: IDA Pro	
○ Online Malware Testing: VirusTotal	
○ Online Malware Analysis Services	
~~○ Trojan Analysis: Neverquest~~	
~~○ Virus Analysis: Ransom Cryptolocker~~	
~~○ Worm Analysis: Darlloz (Internet of Things~~	

~~(IoT) Worm)~~	
▪ Malware Detection	
○ How to Detect Trojans	
• Scanning for Suspicious Ports	
➢ Port Monitoring Tools: TCPView and CurrPorts	
• Scanning for Suspicious Processes	
➢ Process Monitoring Tool: What's Running	
➢ Process Monitoring Tools	
• Scanning for Suspicious Registry Entries	
➢ Registry Entry Monitoring Tool: RegScanner	
➢ Registry Entry Monitoring Tools	
• Scanning for Suspicious Device Drivers	
➢ Device Drivers Monitoring Tool: DriverView	
➢ Device Drivers Monitoring Tools	
• Scanning for Suspicious Windows Services	
➢ Windows Services Monitoring Tool: Windows Service Manager (SrvMan)	
➢ Windows Services Monitoring Tools	
• Scanning for Suspicious Startup Programs	
➢ Windows 8 Startup Registry Entries	
➢ Startup Programs Monitoring Tool: Security AutoRun	
➢ Startup Programs Monitoring Tools	
• Scanning for Suspicious Files and Folders	
➢ Files and Folder Integrity Checker: FastSum and WinMD5	
➢ Files and Folder Integrity Checker	
• Scanning for Suspicious Network Activities	
• Detecting Trojans and Worms with Capsa Network Analyzer	
○ Virus Detection Methods	
▪ Countermeasures	
○ Trojan Countermeasures	
○ Backdoor Countermeasures	
○ Virus and Worms Countermeasures	
▪ Anti-Malware Software	

○ Anti-Trojan Software	
• TrojanHunter	
• Emsisoft Anti-Malware	
• Anti-Trojan Software	
○ Companion Antivirus: Immunet	
○ Antivirus Tools	
▪ Penetration Testing	
○ Pen Testing for Trojans and Backdoors	
○ Penetration Testing for Virus	
Module 07: Sniffing	**Module 08: Sniffing**
▪ Sniffing Concepts	▪ Sniffing Concepts
○ Network Sniffing and Threats	○ Network Sniffing
○ How a Sniffer Works	○ Types of Sniffing
○ Types of Sniffing	○ How an Attacker Hacks the Network Using Sniffers
• Passive Sniffing	○ Protocols Vulnerable to Sniffing
• Active Sniffing	○ Sniffing in the Data Link Layer of the OSI Model
○ How an Attacker Hacks the Network Using Sniffers	○ Hardware Protocol Analyzers
○ Protocols Vulnerable to Sniffing	○ SPAN Port
○ Sniffing in the Data Link Layer of the OSI Model	○ Wiretapping
○ Hardware Protocol Analyzer	○ Lawful Interception
• Hardware Protocol Analyzers	▪ Sniffing Technique: MAC Attacks
○ SPAN Port	○ MAC Address/CAM Table
○ Wiretapping	○ How CAM Works
○ Lawful Interception	○ What Happens When CAM Table Is Full?
~~○ Wiretapping Case Study: PRISM~~	○ MAC Flooding
▪ MAC Attacks	○ Switch Port Stealing
○ MAC Address/CAM Table	○ How to Defend against MAC Attacks
○ How CAM Works	▪ Sniffing Technique: DHCP Attacks
○ What Happens When CAM Table Is Full?	○ How DHCP Works
○ MAC Flooding	○ DHCP Request/Reply Messages
○ Mac Flooding Switches with macof	○ DHCP Starvation Attack
○ Switch Port Stealing	○ Rogue DHCP Server Attack
○ How to Defend against MAC Attacks	○ How to Defend Against DHCP Starvation and Rogue Server Attack

▪ DHCP Attacks	▪ Sniffing Technique: ARP Poisoning
○ How DHCP Works	○ What Is Address Resolution Protocol (ARP)?
○ DHCP Request/Reply Messages	○ ARP Spoofing Attack
○ IPv4 DHCP Packet Format	○ Threats of ARP Poisoning
○ DHCP Starvation Attack	○ ARP Poisoning Tools
○ DHCP Starvation Attack Tools	○ How to Defend Against ARP Poisoning
○ Rogue DHCP Server Attack	○ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
○ How to Defend Against DHCP Starvation and Rogue Server Attack	○ ARP Spoofing Detection Tools
▪ ARP Poisoning	▪ Sniffing Technique: Spoofing Attacks
○ What Is Address Resolution Protocol (ARP)?	○ MAC Spoofing/Duplicating
○ ARP Spoofing Attack	○ MAC Spoofing Technique: Windows
○ How Does ARP Spoofing Work	○ MAC Spoofing Tools
○ Threats of ARP Poisoning	○ IRDP Spoofing
○ ARP Poisoning Tool	○ How to Defend Against MAC Spoofing
• Cain & Abel and WinArpAttacker	▪ Sniffing Technique: DNS Poisoning
• Ufasoft Snif	○ DNS Poisoning Techniques
○ How to Defend Against ARP Poisoning	• Intranet DNS Spoofing
○ Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches	• Internet DNS Spoofing
○ ARP Spoofing Detection: XArp	• Proxy Server DNS Poisoning
▪ Spoofing Attack	• DNS Cache Poisoning
○ MAC Spoofing/Duplicating	○ How to Defend Against DNS Spoofing
○ MAC Spoofing Technique: Windows	▪ Sniffing Tools
○ MAC Spoofing Tool: SMAC	○ Sniffing Tool: Wireshark
○ IRDP Spoofing	• Follow TCP Stream in Wireshark
○ How to Defend Against MAC Spoofing	• Display Filters in Wireshark
▪ DNS Poisoning	• Additional Wireshark Filters
○ DNS Poisoning Techniques	○ Sniffing Tools
• Intranet DNS Spoofing	○ Packet Sniffing Tools for Mobile
• Internet DNS Spoofing	▪ Countermeasures
• Proxy Server DNS Poisoning	○ How to Defend Against Sniffing
• DNS Cache Poisoning	▪ Sniffing Detection Techniques
○ How to Defend Against DNS Spoofing	○ How to Detect Sniffing
▪ Sniffing Tools	○ Sniffer Detection Techniques
○ Sniffing Tool: Wireshark	• Ping Method
• Follow TCP Stream in Wireshark	• DNS Method
• Display Filters in Wireshark	• ARP Method

• Additional Wireshark Filters	○ Promiscuous Detection Tools
○ Sniffing Tool	▪ Sniffing Pen Testing
• SteelCentral Packet Analyzer	○ Sniffing Penetration Testing
• Tcpdump/Windump	
○ Packet Sniffing Tool: Capsa Network Analyzer	
○ Network Packet Analyzer	
• OmniPeek Network Analyzer	
• Observer	
• Sniff-O-Matic	
○ TCP/IP Packet Crafter: Colasoft Packet Builder	
○ Network Packet Analyzer: RSA NetWitness Investigator	
○ Additional Sniffing Tools	
○ Packet Sniffing Tools for Mobile: Wi.cap. Network Sniffer Pro and FaceNiff	
▪ Countermeasures	
○ How to Defend Against Sniffing	
▪ Sniffing Detection Techniques	
○ How to Detect Sniffing	
○ Sniffer Detection Technique	
• Ping Method	
• ARP Method	
• DNS Method	
○ Promiscuous Detection Tool	
• PromqryUI	
• Nmap	
▪ Sniffing Pen Testing	
Module 08: Social Engineering	**Module 09: Social Engineering**
~~▪ Social Engineering Statistics~~	▪ Social Engineering Concepts
▪ Social Engineering Concepts	○ What is Social Engineering?
○ What is Social Engineering?	○ Phases of a Social Engineering Attack
○ Behaviors Vulnerable to Attacks	▪ Social Engineering Techniques
○ Factors that Make Companies Vulnerable to Attacks	○ Types of Social Engineering
○ Why is Social Engineering Effective?	○ Human-based Social Engineering

○ Phases in a Social Engineering Attack	• Impersonation
▪ Social Engineering Techniques	• Impersonation (Vishing)
○ Types of Social Engineering	• Eavesdropping
• Human-based Social Engineering	• Shoulder Surfing
➢ Impersonation	• Dumpster Diving
➢ Impersonation Scenario	• Reverse Social Engineering
✓ Over-Helpfulness of Help Desk	• Piggybacking,
✓ Third-party Authorization	• Tailgating
✓ Tech Support	○ Computer-based Social Engineering
✓ Internal Employee/Client/Vendor	• Phishing
✓ Repairman	○ Mobile-based Social Engineering
✓ Trusted Authority Figure	• Publishing Malicious Apps
➢ Eavesdropping and Shoulder Surfing	• Repackaging Legitimate Apps
➢ Dumpster Diving	• Fake Security Applications
➢ Reverse Social Engineering, Piggybacking, and Tailgating	• SMiShing (SMS Phishing)
~~➢ Watch these Movies~~	▪ Insider Threats
~~➢ Watch this Movie~~	○ Insider Threat / Insider Attack
• Computer-based Social Engineering	○ Type of Insider Threats
➢ Phishing	▪ Impersonation on Social Networking Sites
➢ Spear Phishing	○ Social Engineering Through Impersonation on Social Networking Sites
• Mobile-based Social Engineering	○ Impersonation on Facebook
➢ Publishing Malicious Apps	○ Social Networking Threats to Corporate Networks
➢ Repackaging Legitimate Apps	▪ Identity Theft
➢ Fake Security Applications	○ Identity Theft
➢ Using SMS	▪ Countermeasures
○ Insider Attack	○ Social Engineering Countermeasures
○ Disgruntled Employee	○ Insider Threats Countermeasures
○ Preventing Insider Threats	○ Identity Theft Countermeasures
○ Common Social Engineering Targets and Defense Strategies	○ How to Detect Phishing Emails?
▪ Impersonation on Social Networking Sites	○ Anti-Phishing Toolbar
○ Social Engineering Through Impersonation on Social Networking Sites	○ Common Social Engineering Targets and Defense Strategies
○ Social Engineering on Facebook	▪ Social Engineering Pen Testing
~~○ Social Engineering on LinkedIn and Twitter~~	○ Social Engineering Pen Testing
○ Risks of Social Networking to Corporate	• Using Emails

Networks	
▪ Identity Theft	• Using Phone
~~o Identity Theft Statistics~~	• In Person
o Identify Theft	o Social Engineering Pen Testing Tools
~~o How to Steal an Identity~~	
~~• STEP 1~~	
~~• STEP 2~~	
~~• Comparison~~	
~~• STEP 3~~	
~~• Real Steven Gets Huge Credit Card Statement~~	
~~o Identity Theft - Serious Problem~~	
▪ Social Engineering Countermeasures	
o How to Detect Phishing Emails	
o Anti-Phishing Toolbar	
• Netcraft	
• PhishTank	
o Identity Theft Countermeasures	
▪ Penetration Testing	
o Social Engineering Pen Testing	
• Using Emails	
• Using Phone	
• In Person	
• Social Engineering Toolkit (SET)	
Module 09: Denial-of-Service	**Module 10: Denial-of-Service**
▪ DoS/DDoS Concepts	▪ DoS/DDoS Concepts
~~o DDoS Attack Trends~~	o What is a Denial-of-Service Attack?
o What is a Denial of Service Attack?	o What is Distributed Denial-of-Service Attack?
o What are Distributed Denial of Service Attacks?	▪ DoS/DDoS Attack Techniques
o How Distributed Denial of Service Attacks Work	o Basic Categories of DoS/DDoS Attack Vectors
▪ DoS/DDoS Attack Techniques	o UDP Flood Attack
o Basic Categories of DoS/DDoS Attack Vectors	o ICMP Flood Attack
o DoS/DDoS Attack Techniques	o Ping of Death and Smurf Attack

• ~~Bandwidth Attacks~~	○ SYN Flood Attack
• ~~Service Request Floods~~	○ Fragmentation Attack
• SYN Attack	○ HTTP GET/POST and Slowloris Attacks
• SYN Flooding	○ Multi-Vector Attack
• ICMP Flood Attack	○ Peer-to-Peer Attacks
• Peer-to-Peer Attacks	○ Permanent Denial-of-Service Attack
• Permanent Denial-of-Service Attack	○ Distributed Reflection Denial-of-Service (DRDoS)
• ~~Application Level Flood Attacks~~	▪ Botnets
• Distributed Reflection Denial of Service (DRDoS)	○ Organized Cyber Crime: Organizational Chart
▪ Botnet	○ Botnet
○ Organized Cyber Crime: Organizational Chart	○ A Typical Botnet Setup
○ Botnet	○ Botnet Ecosystem
○ A Typical Botnet Setup	○ Scanning Methods for Finding Vulnerable Machines
○ Botnet Ecosystem	○ How Malicious Code Propagates?
○ Scanning Methods for Finding Vulnerable Machines	○ Botnet Trojans
○ How Malicious Code Propagates?	▪ DDoS Case Study
○ Botnet Trojan: Blackshades NET	○ DDoS Attack
○ Botnet Trojans: Cythosia Botnet and Andromeda Bot	○ Hackers Advertise Links to Download Botnet
○ Botnet Trojan: PlugBot	○ Use of Mobile Devices as Botnets for Launching DDoS Attacks
▪ DDoS Case Study	○ DDoS Case Study: Dyn DDoS Attack
○ DDoS Attack	▪ DoS/DDoS Attack Tools
○ Hackers Advertise Links to Download Botnet	○ DoS/DDoS Attack Tools
▪ DoS Attack Tools	○ DoS and DDoS Attack Tool for Mobile
○ Pandora DDoS Bot Toolkit	▪ Countermeasures
○ Dereil and HOIC	○ Detection Techniques
○ DoS HTTP and BanglaDos	○ DoS/DDoS Countermeasure Strategies
○ DoS and DDoS Attack Tools	○ DDoS Attack Countermeasures
○ DoS and DDoS Attack Tool for Mobile	• Protect Secondary Victims
• AnDOSid	• Detect and Neutralize Handlers
• Low Orbit Ion Cannon (LOIC)	• Prevent Potential Attacks
▪ Countermeasures	• Deflect Attacks
○ Detection Techniques	• Mitigate Attacks
• Activity Profiling	• Post-Attack Forensics

• Wavelet Analysis	○ Techniques to Defend against Botnets
• Sequential Change-Point Detection	○ DoS/DDoS Countermeasures
○ DoS/DDoS Countermeasure Strategies	○ DoS/DDoS Protection at ISP Level
○ DDoS Attack Countermeasures	○ Enabling TCP Intercept on Cisco IOS Software
• DoS/DDoS Countermeasures: Protect Secondary Victims	▪ DoS/DDoS Protection Tools
• DoS/DDoS Countermeasures: Detect and Neutralize Handlers	○ Advanced DDoS Protection Appliances
• DoS/DDoS Countermeasures: Detect Potential Attacks	○ DoS/DDoS Protection Tools
• DoS/DDoS Countermeasures: Deflect Attacks	▪ DoS/DDoS Penetration Testing
• DoS/DDoS Countermeasures: Mitigate Attacks	○ Denial-of-Service (DoS) Attack Pen Testing
○ Post-Attack Forensics	
○ Techniques to Defend against Botnets	
○ DoS/DDoS Countermeasures	
○ DoS/DDoS Protection at ISP Level	
○ Enabling TCP Intercept on Cisco IOS Software	
○ Advanced DDoS Protection Appliances	
▪ DoS/DDoS Protection Tools	
○ DoS/DDoS Protection Tool: FortGuard Anti-DDoS Firewall 2014	
○ DoS/DDoS Protection Tools	
▪ Denial-of-Service (DoS) Attack Penetration Testing	
Module 10: Session Hijacking	**Module 11: Session Hijacking**
~~▪ Attack Techniques 2015~~	▪ Session Hijacking Concepts
▪ Session Hijacking Concepts	○ What is Session Hijacking?
○ What is Session Hijacking?	○ Why Session Hijacking is Successful?
○ Why Session Hijacking is Successful?	○ Session Hijacking Process
○ Session Hijacking Process	○ Packet Analysis of a Local Session Hijack
○ Packet Analysis of a Local Session Hijack	○ Types of Session Hijacking
○ Types of Session Hijacking	○ Session Hijacking in OSI Model
○ Session Hijacking in OSI Model	○ Spoofing vs. Hijacking
○ Spoofing vs. Hijacking	▪ Application Level Session Hijacking
▪ Application Level Session Hijacking	○ Application Level Session Hijacking
○ Compromising Session IDs using Sniffing	○ Compromising Session IDs using Sniffing and by Predicting Session Token

○ Compromising Session IDs by Predicting Session Token	○ How to Predict a Session Token
• How to Predict a Session Token	○ Compromising Session IDs Using Man-in-the-Middle 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 Attack	○ Compromising Session IDs Using Session Fixation
○ Compromising Session IDs Using Session Fixation	○ Session Hijacking Using Proxy Servers
• Session Fixation Attack	○ Session Hijacking Using CRIME Attack
○ Session Hijacking Using Proxy Servers	○ Session Hijacking Using Forbidden Attack
▪ Network-level Session Hijacking	▪ Network Level Session Hijacking
~~○ The 3-Way Handshake~~	○ TCP/IP Hijacking
○ TCP/IP Hijacking	○ IP Spoofing: Source Routed Packets
• TCP/IP Hijacking Process	○ RST Hijacking
○ IP Spoofing: Source Routed Packets	○ Blind Hijacking
○ RST Hijacking	○ UDP Hijacking
○ Blind Hijacking	○ MiTM Attack Using Forged ICMP and ARP Spoofing
○ MiTM Attack Using Forged ICMP and ARP Spoofing	▪ Session Hijacking Tools
○ UDP Hijacking	○ Session Hijacking Tools
▪ Session Hijacking Tools	○ Session Hijacking Tools for Mobile
○ Session Hijacking Tool	▪ Countermeasures
• Zaproxy	○ Session Hijacking Detection Methods
• Burp Suite and Hijack	○ Protecting against Session Hijacking
○ Session Hijacking Tools	○ Methods to Prevent Session Hijacking: To be Followed by Web Developers
○ Session Hijacking Tools for Mobile:	○ Methods to Prevent Session Hijacking: To be

DroidSheep and DroidSniff	Followed by Web Users
▪ Countermeasures	○ Session Hijacking Detection Tools
○ Session Hijacking Detection Methods	○ Approaches Vulnerable to Session Hijacking and their Preventative Solutions
○ Protecting against Session Hijacking	○ Approaches to Prevent Session Hijacking
○ Methods to Prevent Session Hijacking	○ IPSec
• To be Followed by Web Developers	• Components of IPsec
• To be Followed by Web Users	• Benefits of IPsec
○ Approaches Vulnerable to Session Hijacking and their Preventative Solutions	• Modes of IPsec
○ IPSec	• IPsec Architecture
• Modes of IPsec	• IPsec Authentication and Confidentiality
• IPsec Architecture	○ Session Hijacking Prevention Tools
• IPsec Authentication and Confidentiality	▪ Penetration Testing
• Components of IPsec	○ Session Hijacking Pen Testing
▪ Session Hijacking Pen Testing	
Module 16: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
~~▪ Survey: The State of Network Security 2014~~	▪ IDS, Firewall and Honeypot Concepts
~~▪ Cybersecurity Market Report~~	○ Intrusion Detection System (IDS)
▪ IDS, Firewall and Honeypot Concepts	• How IDS Detects an Intrusion
○ Intrusion Detection Systems (IDS) and their Placement	• General Indications of Intrusions
• How IDS Works	• Types of Intrusion Detection Systems
• Ways to Detect an Intrusion	• Types of IDS Alerts
• General Indications of Intrusions	○ Firewall
• General Indications of System Intrusions	• Firewall Architecture
• Types of Intrusion Detection Systems	• DeMilitarized Zone (DMZ)
~~• System Integrity Verifiers (SIV)~~	• Types of Firewalls
○ Firewall	• Firewall Technologies
• Firewall Architecture	➢ Packet Filtering Firewall
• DeMilitarized Zone (DMZ)	➢ Circuit-Level Gateway Firewall
• Types of Firewall	➢ Application-Level Firewall
➢ Packet Filtering Firewall	➢ Stateful Multilayer Inspection Firewall
➢ Circuit-Level Gateway Firewall	➢ Application Proxy
➢ Application-Level Firewall	➢ Network Address Translation (NAT)
➢ Stateful Multilayer Inspection Firewall	➢ Virtual Private Network
○ Honeypot	• Firewall Limitations

• Types of Honeypots	○ Honeypot
▪ IDS, Firewall and Honeypot System	• Types of Honeypots
○ Intrusion Detection Tool	▪ IDS, Firewall and Honeypot Solutions
• Snort	○ Intrusion Detection Tool
• Snort Rules	• Snort
➢ Rule Actions and IP Protocols	➢ Snort Rules
➢ The Direction Operator and IP Addresses	➢ Snort Rules: Rule Actions and IP Protocols
➢ Port Numbers	➢ Snort Rules: The Direction Operator and IP Addresses
• Intrusion Detection Systems: Tipping Point	➢ Snort Rules: Port Numbers
• Intrusion Detection Tools	• Intrusion Detection Tools: TippingPoint and AlienVault® OSSIM™
• Intrusion Detection Tools for Mobile	• Intrusion Detection Tools
○ Firewall	• Intrusion Detection Tools for Mobile
• ZoneAlarm PRO Firewall 2015	○ Firewalls
• Comodo Firewall	• ZoneAlarm Free Firewall 2018 and Firewall Analyzer
• Firewalls	• Firewalls
• Firewalls for Mobile: Android Firewall and Firewall iP	• Firewalls for Mobile
• Firewalls for Mobile	○ Honeypot Tools
○ Honeypot Tool	• KFSensor and SPECTER
• KFSensor and SPECTER	• Honeypot Tools
• Honeypot Tools	• Honeypot Tools for Mobile
• Honeypot Tool for Mobile: HosTaGe	▪ Evading IDS
▪ Evading IDS	○ IDS Evasion Techniques
○ Insertion Attack	• Insertion Attack
○ Evasion	• Evasion
○ Denial-of-Service Attack (DoS)	• Denial-of-Service Attack (DoS)
○ Obfuscating	• Obfuscating
○ False Positive Generation	• False Positive Generation
○ Session Splicing	• Session Splicing
○ Unicode Evasion Technique	• Unicode Evasion
○ Fragmentation Attack	• Fragmentation Attack
○ Overlapping Fragments	• Overlapping Fragments
○ Time-To-Live Attacks	• Time-To-Live Attacks
○ Invalid RST Packets	• Invalid RST Packets
○ Urgency Flag	• Urgency Flag

○ Polymorphic Shellcode	• Polymorphic Shellcode
○ ASCII Shellcode	• ASCII Shellcode
○ Application-Layer Attacks	• Application-Layer Attacks
○ Desynchronization - Pre Connection SYN	• Desynchronization
○ Desynchronization - Post Connection SYN	• Other Types of Evasion
○ Other Types of Evasion	▪ Evading Firewalls
▪ Evading Firewalls	○ Firewall Evasion Techniques
○ Firewall Identification	• Firewall Identification
• Port Scanning	• IP Address Spoofing
• Firewalking	• Source Routing
• Banner Grabbing	• Tiny Fragments
○ IP Address Spoofing	• Bypass Blocked Sites Using IP Address in Place of URL
○ Source Routing	• Bypass Blocked Sites Using Anonymous Website Surfing Sites
○ Tiny Fragments	• Bypass a Firewall Using Proxy Server
○ Bypass Blocked Sites Using IP Address in Place of URL	• Bypassing Firewall through ICMP Tunneling Method
○ Bypass Blocked Sites Using Anonymous Website Surfing Sites	• Bypassing Firewall through ACK Tunneling Method
○ Bypass a Firewall Using Proxy Server	• Bypassing Firewall through HTTP Tunneling Method
○ Bypassing Firewall through ICMP Tunneling Method	➢ Why do I Need HTTP Tunneling
○ Bypassing Firewall through ACK Tunneling Method	➢ HTTP Tunneling Tools
○ Bypassing Firewall through HTTP Tunneling Method	• Bypassing Firewall through SSH Tunneling Method
• Why do I Need HTTP Tunneling	➢ SSH Tunneling Tool: Bitvise and Secure Pipes
• HTTP Tunneling Tools	• Bypassing Firewall through External Systems
➢ HTTPort and HTTHost	• Bypassing Firewall through MITM Attack
➢ Super Network Tunnel	• Bypassing Firewall through Content
➢ HTTP-Tunnel	• Bypassing WAF using XSS Attack
○ Bypassing Firewall through SSH Tunneling Method	▪ IDS/Firewall Evading Tools
• SSH Tunneling Tool: Bitvise	○ IDS/Firewall Evasion Tools
○ Bypassing Firewall through External Systems	○ Packet Fragment Generator Tools
○ Bypassing Firewall through MITM Attack	▪ Detecting Honeypots
○ Bypassing Firewall through Content	○ Detecting Honeypots

▪ IDS/Firewall Evading Tools	○ Detecting and Defeating Honeypots
○ IDS/Firewall Evasion Tool	○ Honeypot Detection Tool: Send-Safe Honeypot Hunter
• Traffic IQ Professional	▪ IDS/Firewall Evasion Countermeasures
• tcp-over-dns	○ How to Defend Against IDS Evasion
○ IDS/Firewall Evasion Tools	○ How to Defend Against Firewall Evasion
○ Packet Fragment Generator: Colasoft Packet Builder	▪ Penetration Testing
○ Packet Fragment Generators	○ Firewall/IDS Penetration Testing
▪ Detecting Honeypots	• Firewall Penetration Testing
○ Detecting Honeypots	• IDS Penetration Testing
○ Honeypot Detecting Tool: Send-Safe Honeypot Hunter	
▪ IDS/Firewall Evasion Countermeasures	
○ Countermeasures	
▪ Penetration Testing	
Module 11: Hacking Webservers	**Module 13: Hacking Web Servers**
~~▪ Webserver Market Shares~~	▪ Web Server Concepts
▪ Webserver Concepts	○ Web Server Operations
○ Web Server Security Issue	○ Open Source Web Server Architecture
○ Why Web Servers Are Compromised	○ IIS Web Server Architecture
○ Impact of Webserver Attacks	○ Web Server Security Issue
○ Open Source Webserver Architecture	○ Why Web Servers Are Compromised?
○ IIS Web Server Architecture	○ Impact of Web Server Attacks
▪ Webserver Attacks	▪ Web Server Attacks
○ DoS/DDoS Attacks	○ DoS/DDoS Attacks
○ DNS Server Hijacking	○ DNS Server Hijacking
○ DNS Amplification Attack	○ DNS Amplification Attack
○ Directory Traversal Attacks	○ Directory Traversal Attacks
○ Man-in-the-Middle/Sniffing Attack	○ Man-in-the-Middle/Sniffing Attack
○ Phishing Attacks	○ Phishing Attacks
○ Website Defacement	○ Website Defacement
○ Webserver Misconfiguration	○ Web Server Misconfiguration
• Webserver Misconfiguration Example	○ HTTP Response Splitting Attack
○ HTTP Response Splitting Attack	○ Web Cache Poisoning Attack
○ Web Cache Poisoning Attack	○ SSH Brute Force Attack
○ SSH Bruteforce Attack	○ Web Server Password Cracking

○ Webserver Password Cracking	○ Web Application Attacks
• Webserver Password Cracking Techniques	▪ Web Server Attack Methodology
○ Web Application Attacks	○ Information Gathering
▪ Attack Methodology	• Information Gathering from Robots.txt File
○ Webserver Attack Methodology	○ Web Server Footprinting/Banner Grabbing
• Information Gathering	• Web Server Footprinting Tools
➢ Information Gathering from Robots.txt File	• Enumerating Web Server Information Using Nmap
• Webserver Footprinting	○ Website Mirroring
➢ Webserver Footprinting Tools	• Finding Default Credentials of Web Server
➢ Enumerating Webserver Information Using Nmap	• Finding Default Content of Web Server
• Mirroring a Website	• Finding Directory Listings of Web Server
• Vulnerability Scanning	○ Vulnerability Scanning
• Session Hijacking	• Finding Exploitable Vulnerabilities
• Hacking Web Passwords	○ Session Hijacking
▪ Webserver Attack Tools	○ Web Server Passwords Hacking
○ Metasploit	○ Using Application Server as a Proxy
• Metasploit Architecture	▪ Web Server Attack Tools
• Metasploit Exploit Module	○ Metasploit
• Metasploit Payload Module	• Metasploit Exploit Module
• Metasploit Auxiliary Module	• Metasploit Payload and Auxiliary Module
• Metasploit NOPS Module	• Metasploit NOPS Module
○ Wfetch	○ Web Server Attack Tools
○ Web Password Cracking Tool: THC-Hydra and Brutus	▪ Countermeasures
▪ Countermeasures	○ Place Web Servers in Separate Secure Server Security Segment on Network
○ Place Web Servers in Separate Secure Server Security Segment on Network	○ Countermeasures
○ Countermeasures	• Patches and Updates
• Patches and Updates	• Protocols
• Protocols	• Accounts
• Accounts	• Files and Directories
• Files and Directories	○ Detecting Web Server Hacking Attempts
○ Detecting Web Server Hacking Attempts	○ How to Defend Against Web Server Attacks
○ How to Defend Against Web Server Attacks	○ How to Defend against HTTP Response Splitting and Web Cache Poisoning
○ How to Defend against HTTP Response Splitting and Web Cache Poisoning	○ How to Defend against DNS Hijacking

○ How to Defend against DNS Hijacking	▪ Patch Management
▪ Patch Management	○ Patches and Hotfixes
○ Patches and Hotfixes	○ What is Patch Management
○ What is Patch Management?	○ Installation of a Patch
○ Identifying Appropriate Sources for Updates and Patches	○ Patch Management Tools
○ Installation of a Patch	▪ Web Server Security Tools
○ Implementation and Verification of a Security Patch or Upgrade	○ Web Application Security Scanners
○ Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)	○ Web Server Security Scanners
○ Patch Management Tools	○ Web Server Security Tools
▪ Webserver Security Tools	▪ Web Server Pen Testing
○ Web Application Security Scanner: Syhunt Dynamic and N-Stalker Web Application Security Scanner	○ Web Server Penetration Testing
○ Web Server Security Scanner: Wikto and Acunetix Web Vulnerability Scanner	○ Web Server Pen Testing Tools
○ Web Server Malware Infection Monitoring Tool	
• HackAlert	
• QualysGuard Malware Detection	
○ Webserver Security Tools	
▪ Webserver Pen Testing	
○ Web Server Penetration Testing	
○ Web Server Pen Testing Tool	
• CORE Impact® Pro	
• Immunity CANVAS	
• Arachni	
Module 12: Hacking Web Applications	**Module 14: Hacking Web Applications**
~~▪ Web Application Attack Report~~	▪ Web App Concepts
~~▪ Variety of Hacking Actions Within Web App Attacks Pattern~~	○ Introduction to Web Applications
▪ Web App Concepts	○ Web Application Architecture
○ Introduction to Web Applications	○ Web 2.0 Applications
○ How Web Applications Work	○ Vulnerability Stack
○ Web Application Architecture	▪ Web App Threats
○ Web 2.0 Applications	○ OWASP Top 10 Application Security Risks – 2017

○ Vulnerability Stack	• A1 - Injection Flaws
▪ Web App Threats	➢ SQL Injection Attacks
○ Web Application Threats – 1	➢ Command Injection Attacks
○ Web Application Threats - 2	✓ Command Injection Example
○ Unvalidated Input	➢ File Injection Attack
○ Parameter/Form Tampering	➢ LDAP Injection Attacks
○ Directory Traversal	• A2 - Broken Authentication
○ Security Misconfiguration	• A3 - Sensitive Data Exposure
○ Injection Flaws	• A4 - XML External Entity (XXE)
○ SQL Injection Attacks	• A5 - Broken Access Control
○ Command Injection Attacks	• A6 - Security Misconfiguration
• Command Injection Example	• A7 - Cross-Site Scripting (XSS) Attacks
○ File Injection Attack	➢ Cross-Site Scripting Attack Scenario: Attack via Email
○ What is LDAP Injection?	➢ XSS Attack in Blog Posting
• How LDAP Injection Works	➢ XSS Attack in Comment Field
○ Hidden Field Manipulation Attack	➢ Websites Vulnerable to XSS Attack
○ Cross-Site Scripting (XSS) Attacks	• A8 - Insecure Deserialization
• How XSS Attacks Work	• A9 - Using Components with Known Vulnerabilities
• Cross-Site Scripting Attack Scenario: Attack via Email	• A10 - Insufficient Logging and Monitoring
• XSS Example: Attack via Email	○ Other Web Application Threats
• XSS Example: Stealing Users' Cookies	• Directory Traversal
• XSS Example: Sending an Unauthorized Request	• Unvalidated Redirects and Forwards
• XSS Attack in Blog Posting	• Watering Hole Attack
• XSS Attack in Comment Field	• Cross-Site Request Forgery (CSRF) Attack
• Websites Vulnerable to XSS Attack	• Cookie/Session Poisoning
○ Cross-Site Request Forgery (CSRF) Attack	• Web Services Architecture
• How CSRF Attacks Work	• Web Services Attack
○ Web Application Denial-of-Service (DoS) Attack	• Web Services Footprinting Attack
• Denial of Service (DoS) Examples	• Web Services XML Poisoning
○ Buffer Overflow Attacks	• Hidden Field Manipulation Attack
○ Cookie/Session Poisoning	▪ Hacking Methodology
• How Cookie Poisoning Works	○ Web App Hacking Methodology
~~○ Session Fixation Attack~~	○ Footprint Web Infrastructure
○ CAPTCHA Attacks	• Server Discovery

○ Insufficient Transport Layer Protection	• Service Discovery
○ Improper Error Handling	• Server Identification/Banner Grabbing
○ Insecure Cryptographic Storage	• Detecting Web App Firewalls and Proxies on Target Site
○ Broken Authentication and Session Management	• Hidden Content Discovery
○ Unvalidated Redirects and Forwards	• Web Spidering Using Burp Suite
○ Web Services Architecture	• Web Crawling Using Mozenda Web Agent Builder
○ Web Services Attack	○ Attack Web Servers
○ Web Services Footprinting Attack	○ Analyze Web Applications
○ Web Services XML Poisoning	• Identify Entry Points for User Input
▪ Web App Hacking Methodology	• Identify Server- Side Technologies
○ Footprint Web Infrastructure	• Identify Server- Side Functionality
• Server Discovery	• Map the Attack Surface
• Service Discovery	○ Bypass Client-Side Controls
• Server Identification/Banner Grabbing	• Attack Hidden Form Fields
➢ Detecting Web App Firewalls and Proxies on Target Site	• Attack Browser Extensions
• Hidden Content Discovery	• Perform Source Code Review
• Web Spidering Using Burp Suite	○ Attack Authentication Mechanism
• Web Crawling Using Mozenda Web Agent Builder	• User Name Enumeration
○ Attack Web Servers	• Password Attacks: Password Functionality Exploits
• Hacking Web Servers	• Password Attacks: Password Guessing and Brute-forcing
• Web Server Hacking Tool: WebInspect	• Session Attacks: Session ID Prediction/Brute-forcing
○ Analyze Web Applications	• Cookie Exploitation: Cookie Poisoning
• Identify Entry Points for User Input	○ Attack Authorization Schemes
• Identify Server-Side Technologies	• HTTP Request Tampering
• Identify Server-Side Functionality	• Cookie Parameter Tampering
• Map the Attack Surface	○ Attack Access Controls
○ Attack Authentication Mechanism	○ Attack Session Management Mechanism
• User Name Enumeration	• Attacking Session Token Generation Mechanism
• Password Attacks	• Attacking Session Tokens Handling Mechanism: Session Token Sniffing
➢ Password Functionality Exploits	○ Perform Injection/Input Validation Attacks

➢ Password Guessing	○ Attack Application Logic Flaws
➢ Brute-forcing	○ Attack Database Connectivity
• Session Attacks: Session ID Prediction/ Brute-forcing	• Connection String Injection
• Cookie Exploitation: Cookie Poisoning	• Connection String Parameter Pollution (CSPP) Attacks
○ Authorization Attack Schemes	• Connection Pool DoS
• Authorization Attack	○ Attack Web App Client
• HTTP Request Tampering	○ Attack Web Services
• Authorization Attack: Cookie Parameter Tampering	• Web Services Probing Attacks
○ Attack Session Management Mechanism	• Web Service Attacks: SOAP Injection
• Session Management Attack	• Web Service Attacks: XML Injection
• Attacking Session Token Generation Mechanism	• Web Services Parsing Attacks
• Attacking Session Tokens Handling Mechanism: Session Token Sniffing	• Web Service Attack Tools
○ Perform Injection Attacks	▪ Web App Hacking Tools
• Injection Attacks/Input Validation Attacks	○ Web Application Hacking Tools
○ Attack Data Connectivity	▪ Countermeasures
• Connection String Injection	○ Web Application Fuzz Testing
• Connection String Parameter Pollution (CSPP) Attacks	○ Source Code Review
• Connection Pool DoS	○ Encoding Schemes
○ Attack Web App Client	○ How to Defend Against Injection Attacks
○ Attack Web Services	○ Web Application Attack Countermeasures
• Web Services Probing Attacks	○ How to Defend Against Web Application Attacks
• Web Service Attacks	▪ Web App Security Testing Tools
➢ SOAP Injection	○ Web Application Security Testing Tools
➢ XML Injection	○ Web Application Firewall
• Web Services Parsing Attacks	▪ Web App Pen Testing
• Web Service Attack Tool: soapUI and XMLSpy	○ Web Application Pen Testing
▪ Web Application Hacking Tools	• Information Gathering
○ Web Application Hacking Tool	• Configuration Management Testing
• Burp Suite Professional	• Authentication Testing
• CookieDigger	• Session Management Testing
• WebScarab	• Authorization Testing
○ Web Application Hacking Tools	• Data Validation Testing

▪ Countermeasures	• Denial-of-Service Testing
○ Encoding Schemes	• Web Services Testing
○ How to Defend Against SQL Injection Attacks	• AJAX Testing
○ How to Defend Against Command Injection Flaws	○ Web Application Pen Testing Framework
○ How to Defend Against XSS Attacks	
~~○ How to Defend Against DoS Attack~~	
○ How to Defend Against Web Services Attack	
~~○ Guidelines for Secure CAPTCHA Implementation~~	
○ Web Application Attack Countermeasures	
○ How to Defend Against Web Application Attacks	
▪ Security Tools	
○ Web Application Security Tool	
• Acunetix Web Vulnerability Scanner	
• Watcher Web Security Tool	
• Netsparker	
• N-Stalker Web Application Security Scanner	
• VampireScan	
○ Web Application Security Tools	
○ Web Application Firewall	
• dotDefender	
• ServerDefender VP	
○ Web Application Firewall	
▪ Web App Pen Testing	
○ Web Application Pen Testing	
• Information Gathering	
• Configuration Management Testing	
• Authentication Testing	
• Session Management Testing	
• Authorization Testing	
• Data Validation Testing	
• Denial-of-Service Testing	
• Web Services Testing	
• AJAX Testing	
○ Web Application Pen Testing Framework	
• Kali Linux	

• Metasploit	
• Browser Exploitation Framework (BeEF)	
• PowerSploit	
Module 13: SQL Injection	**Module 15: SQL Injection**
~~▪ SQL Injection Statistics~~	▪ SQL Injection Concepts
~~▪ SQL Most Prevalent Vulnerability 2015~~	○ What is SQL Injection?
▪ SQL Injection Concepts	○ SQL Injection and Server-side Technologies
○ What is SQL Injection?	○ Understanding HTTP POST Request
○ Why Bother about SQL Injection?	○ Understanding Normal SQL Query
~~○ How Web Applications Work~~	○ Understanding an SQL Injection Query
○ SQL Injection and Server-side Technologies	○ Understanding an SQL Injection Query – Code Analysis
○ Understanding HTTP Post Request	○ Example of a Web Application Vulnerable to SQL Injection: BadProductList.aspx
○ Example: Normal SQL Query	○ Example of a Web Application Vulnerable to SQL Injection: Attack Analysis
○ Understanding an SQL Injection Query	○ Examples of SQL Injection
• Code Analysis	▪ Types of SQL Injection
○ Example of a Web App Vulnerable to SQL Injection	○ Types of SQL injection
• BadProductList.aspx	• In-Band SQL Injection
• Attack Analysis	➢ Error Based SQL Injection
○ Example of SQL Injection	➢ Union SQL Injection
• Updating Table	• Blind/Inferential SQL Injection
• Adding New Records	➢ No Error Messages Returned
• Identifying the Table Name	➢ Blind SQL Injection: WAITFOR DELAY (YES or NO Response)
• Deleting a Table	➢ Blind SQL Injection: Boolean Exploitation and Heavy Query
▪ Types of SQL Injection	• Out-of-Band SQL injection
○ Error Based SQL Injection	▪ SQL Injection Methodology
○ Union SQL Injection	○ SQL Injection Methodology
○ Blind SQL Injection	• Information Gathering and SQL Injection Vulnerability Detection
• No Error Messages Returned	➢ Information Gathering
• Blind SQL Injection: WAITFOR DELAY (YES or NO Response)	➢ Identifying Data Entry Paths
○ Boolean Exploitation Technique	➢ Extracting Information through Error Messages

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

• Features of Different DBMSs	➢ Password Grabbing
• Creating Database Accounts	➢ Grabbing SQL Server Hashes
• Password Grabbing	➢ Extracting SQL Hashes (In a Single Statement
• 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
▪ SQL Injection Tools	➢ Creating Server Backdoors using SQL Injection
○ BSQLHacker	▪ SQL Injection Tools
○ Marathon Tool	○ SQL Injection Tools
○ SQL Power Injector	• SQL Power Injector and sqlmap
○ Havij	• The Mole and jSQL Injection
○ SQL Injection Tools	○ SQL Injection Tools
○ SQL Injection Tool for Mobile	○ SQL Injection Tools for Mobile
• DroidSQLi	▪ Evasion Techniques
• sqlmapchik	○ Evading IDS
▪ Evasion Techniques	○ Types of Signature Evasion Techniques
○ Evading IDS	• In-line Comment
○ Types of Signature Evasion Techniques	• Char Encoding
○ Evasion Technique	• String Concatenation
• Sophisticated Matches	• Obfuscated Codes
• Hex Encoding	• Manipulating White Spaces
• Manipulating White Spaces	• Hex Encoding
• In-line Comment	• Sophisticated Matches
• Char Encoding	• URL Encoding
• String Concatenation	• Null Byte
• Obfuscated Codes	• Case Variation
▪ Countermeasures	• Declare Variable
○ How to Defend Against SQL Injection Attacks	• IP Fragmentation
• Use Type-Safe SQL Parameters	▪ Countermeasures

○ SQL Injection Detection Tool	○ How to Defend Against SQL Injection Attacks
• dotDefender	• Use Type-Safe SQL Parameters
• IBM Security AppScan	○ SQL Injection Detection Tools
• WebCruiser	• IBM Security AppScan and Acunetix Web Vulnerability Scanner
○ Snort Rule to Detect SQL Injection Attacks	• Snort Rule to Detect SQL Injection Attacks
○ SQL Injection Detection Tools	○ SQL Injection Detection Tools
Module 14: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
~~▪ Are You Protected from Hackers on Public Wi-Fi?~~	▪ Wireless Concepts
~~▪ Wi-Fi Statistics~~	○ Wireless Terminologies
▪ Wireless Concepts	○ Wireless Networks
○ Wireless Terminologies	○ Wireless Standards
○ Wireless Networks	○ Service Set Identifier (SSID)
○ Wi-Fi Networks at Home and Public Places	○ Wi-Fi Authentication Modes
~~○ Wireless Technology Statistics~~	○ Wi-Fi Authentication Process Using a Centralized Authentication Server
○ Types of Wireless Networks	○ Types of Wireless Antennas
○ Wireless Standards	▪ Wireless Encryption
○ Service Set Identifier (SSID)	○ Types of Wireless Encryption
○ Wi-Fi Authentication Modes	• WEP (Wired Equivalent Privacy) Encryption
○ Wi-Fi Authentication Process Using a Centralized Authentication Server	• WPA (Wi-Fi Protected Access) Encryption
○ Wi-Fi Chalking	• WPA2 (Wi-Fi Protected Access 2) Encryption
• Wi-Fi Chalking Symbols	○ WEP vs. WPA vs. WPA2
○ Types of Wireless Antenna	○ WEP Issues
• Parabolic Grid Antenna	○ Weak Initialization Vectors (IV)
▪ Wireless Encryption	▪ Wireless Threats
○ Types of Wireless Encryption	○ Wireless Threats
• WEP Encryption	• Rogue Access Point Attack
➢ How WEP Works	• Client Mis-association
• What is WPA?	• Misconfigured Access Point Attack
➢ How WPA Works	• Unauthorized Association
➢ Temporal Keys	• Ad Hoc Connection Attack
• What is WPA2?	• Honeypot Access Point Attack
➢ How WPA2 Works	• AP MAC Spoofing
○ WEP vs. WPA vs. WPA2	• Denial-of-Service Attack

○ WEP Issues	• Key Reinstallation Attack (KRACK)
○ Weak Initialization Vectors (IV)	• Jamming Signal Attack
○ How to Break WEP Encryption	➢ Wi-Fi Jamming Devices
○ How to Break WPA Encryption	▪ Wireless Hacking Methodology
○ How to Defend Against WPA Cracking	○ Wireless Hacking Methodology
▪ Wireless Threats	• Wi-Fi Discovery
○ Access Control Attacks	➢ Footprint the Wireless Network
○ Integrity Attacks	➢ Find Wi-Fi Networks in Range to Attack
○ Confidentiality Attacks	➢ Wi-Fi Discovery Tools
○ Availability Attacks	➢ Mobile-based Wi-Fi Discovery Tools
○ Authentication Attacks	• GPS Mapping
○ Rogue Access Point Attack	➢ GPS Mapping Tools
○ Client Mis-association	➢ Wi-Fi Hotspot Finder Tools
○ Misconfigured Access Point Attack	➢ How to Discover Wi-Fi Network Using Wardriving
○ Unauthorized Association	• Wireless Traffic Analysis
○ Ad Hoc Connection Attack	➢ Choosing the Right Wi-Fi Card
○ HoneySpot Access Point Attack	➢ Wi-Fi USB Dongle: AirPcap
○ AP MAC Spoofing	➢ Wi-Fi Packet Sniffer
○ Denial-of-Service Attack	➢ Perform Spectrum Analysis
○ Jamming Signal Attack	• Launch Wireless Attacks
○ Wi-Fi Jamming Devices	➢ Aircrack-ng Suite
▪ Wireless Hacking Methodology	➢ How to Reveal Hidden SSIDs
○ Wi-Fi Discovery	➢ Fragmentation Attack
• Footprint the Wireless Network	➢ How to Launch MAC Spoofing Attack
• Find Wi-Fi Networks to Attack	➢ Denial-of-Service: Disassociation and Deauthentication Attacks
• Wi-Fi Discovery Tool	➢ Man-in-the-Middle Attack
➢ inSSIDer and NetSurveyor	➢ MITM Attack Using Aircrack-ng
➢ Vistumbler and NetStumbler	➢ Wireless ARP Poisoning Attack
• Wi-Fi Discovery Tools	➢ Rogue Access Points
• Mobile-based Wi-Fi Discovery Tool	➢ Evil Twin
○ GPS Mapping	➢ How to Set Up a Fake Hotspot (Evil Twin)
• GPS Mapping Tool	• Crack Wi-Fi Encryption
➢ WIGLE	➢ How to Break WEP Encryption
➢ Skyhook	➢ How to Crack WEP Using Aircrack-ng
• Wi-Fi Hotspot Finder	➢ How to Break WPA/WPA2 Encryption

➢ Wi-Fi Finder	➢ How to Crack WPA-PSK Using Aircrack-ng
➢ WeFi	➢ WEP Cracking and WPA Brute Forcing Using Cain & Abel
• How to Discover Wi-Fi Network Using Wardriving	▪ Wireless Hacking Tools
○ Wireless Traffic Analysis	○ WEP/WPA Cracking Tools
• Wireless Cards and Chipsets	○ WEP/WPA Cracking Tool for Mobile
• Wi-Fi USB Dongle: AirPcap	○ Wi-Fi Sniffer
• Wi-Fi Packet Sniffer	○ Wi-Fi Traffic Analyzer Tools
➢ Wireshark with AirPcap	○ Other Wireless Hacking Tools
➢ SteelCentral Packet Analyzer	▪ Bluetooth Hacking
➢ OmniPeek Network Analyzer	○ Bluetooth Stack
➢ CommView for Wi-Fi	○ Bluetooth Hacking
• What is Spectrum Analysis?	○ Bluetooth Threats
• Wi-Fi Packet Sniffers	○ How to BlueJack a Victim
○ Launch Wireless Attacks	○ Bluetooth Hacking Tools
• Aircrack-ng Suite	▪ Countermeasures
• How to Reveal Hidden SSIDs	○ Wireless Security Layers
• Fragmentation Attack	○ How to Defend Against WPA/WPA2 Cracking
• How to Launch MAC Spoofing Attack	○ How to Defend Against KRACK Attacks
• Denial of Service: Deauthentication and Disassociation Attacks	○ How to Detect and Block Rogue AP
• Man-in-the-Middle Attack	○ How to Defend Against Wireless Attacks
• MITM Attack Using Aircrack-ng	○ How to Defend Against Bluetooth Hacking
• Wireless ARP Poisoning Attack	▪ Wireless Security Tools
• Rogue Access Point	○ Wireless Intrusion Prevention Systems
• Evil Twin	○ Wireless IPS Deployment
➢ How to Set Up a Fake Hotspot (Evil Twin)	○ Wi-Fi Security Auditing Tools
○ Crack Wi-Fi Encryption	○ Wi-Fi Intrusion Prevention System
• How to Crack WEP Using Aircrack	○ Wi-Fi Predictive Planning Tools
• How to Crack WPA-PSK Using Aircrack	○ Wi-Fi Vulnerability Scanning Tools
• WPA Cracking Tool: KisMAC	○ Bluetooth Security Tools
• WEP Cracking Using Cain & Abel	○ Wi-Fi Security Tools for Mobile
• WPA Brute Forcing Using Cain & Abel	▪ Wireless Pen Testing
• WPA Cracking Tool: Elcomsoft Wireless Security Auditor	○ Wireless Penetration Testing
• WEP/WPA Cracking Tools	○ Wireless Penetration Testing Framework

• WEP/WPA Cracking Tool for Mobile: Penetrate Pro	• Pen Testing for General Wi-Fi Network Attack
▪ Wireless Hacking Tools	• Pen Testing WEP Encrypted WLAN
○ Wi-Fi Sniffer: Kismet	• Pen Testing WPA/WPA2 Encrypted WLAN
○ Wardriving Tools	• Pen Testing LEAP Encrypted WLAN
○ RF Monitoring Tools	• Pen Testing Unencrypted WLAN
○ Wi-Fi Traffic Analyzer Tools	
○ Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools	
○ Wireless Hacking Tools for Mobile: WiHack and Backtrack Simulator	
▪ Bluetooth Hacking	
○ Bluetooth Stack	
○ Bluetooth Threats	
○ How to BlueJack a Victim	
○ Bluetooth Hacking Tool	
• PhoneSnoop	
• BlueScanner	
○ Bluetooth Hacking Tools	
▪ Countermeasures	
○ How to Defend Against Bluetooth Hacking	
○ How to Detect and Block Rogue AP	
○ Wireless Security Layers	
○ How to Defend Against Wireless Attacks	
▪ Wireless Security Tools	
○ Wireless Intrusion Prevention Systems	
○ Wireless IPS Deployment	
○ Wi-Fi Security Auditing Tool	
• AirMagnet WiFi Analyzer	
• Motorola’s AirDefense Services Platform (ADSP)	
• Adaptive Wireless IPS	
• Aruba RFProtect	
○ Wi-Fi Intrusion Prevention System	
○ Wi-Fi Predictive Planning Tools	
○ Wi-Fi Vulnerability Scanning Tools	
○ Bluetooth Security Tool: Bluetooth Firewall	
○ Wi-Fi Security Tools for Mobile: Wifi Protector, WiFiGuard, and Wifi Inspector	

▪ Wi-Fi Pen Testing	
○ Wireless Penetration Testing	
○ Wireless Penetration Testing Framework	
○ Wi-Fi Pen Testing Framework	
○ Pen Testing LEAP Encrypted WLAN	
○ Pen Testing WPA/WPA2 Encrypted WLAN	
○ Pen Testing WEP Encrypted WLAN	
○ Pen Testing Unencrypted WLAN	
Module 15: Hacking Mobile Platforms	**Module 17: Hacking Mobile Platforms**
~~▪ The Future of Mobile~~	▪ 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 Mobile Top 10 Risks	○ 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 when Successfully Compromised	○ Mobile Attack Vectors and Mobile Platform Vulnerabilities
○ Mobile Attack Vectors	○ Security Issues Arising from App Stores
○ Mobile Platform Vulnerabilities and Risks	○ App Sandboxing Issues
○ Security Issues Arising from App Stores	○ Mobile Spam
○ App Sandboxing Issues	○ SMS Phishing Attack (SMiShing) (Targeted Attack Scan)
○ Mobile Spam	• SMS Phishing Attack Examples
○ SMS Phishing Attack (SMiShing) (Targeted Attack Scan)	○ Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
• Why SMS Phishing is Effective?	▪ Hacking Android OS
• SMS Phishing Attack Examples	○ Android OS
○ Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections	• Android Device Administration API
▪ Hacking Android OS	○ Android Rooting
○ Android OS	• Rooting Android Using KingoRoot
○ Android OS Architecture	• Android Rooting Tools
○ Android Device Administration API	○ Blocking Wi-Fi Access using NetCut
○ Android Rooting	○ Hacking with zANTI
~~• Rooting Android Phones using SuperOneClick~~	○ Hacking Networks Using Network Spoofer
~~• Rooting Android Phones Using Superboot~~	○ Launching DoS Attack using Low Orbit Ion

	Cannon (LOIC)
• Android Rooting Tools	○ Performing Session Hijacking Using DroidSheep
○ Hacking Networks Using Network Spoofer	○ Hacking with Orbot Proxy
○ Session Hijacking Using DroidSheep	○ Android-based Sniffers
○ Android-based Sniffer	○ Android Trojans
• FaceNiff	○ Securing Android Devices
• Packet Sniffer, tPacketCapture, and Android PCAP	○ Android Security Tool: Find My Device
○ Android Trojan	○ Android Security Tools
• ZitMo (ZeuS-in-the-Mobile)	○ Android Vulnerability Scanner
• FakeToken and TRAMP.A	○ Android Device Tracking Tools
• Fakedefender and Obad	▪ Hacking iOS
• FakeInst and OpFake	○ Apple iOS
• AndroRAT and Dendroid	○ Jailbreaking iOS
○ Securing Android Devices	• Jailbreaking Techniques
• Google Apps Device Policy	• Jailbreaking of iOS 11.2.1 Using Cydia
• Remote Wipe Service: Remote Wipe	• Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang
• Android Security Tool	• Jailbreaking Tools
➢ DroidSheep Guard	○ iOS Trojans
➢ TrustGo Mobile Security and Sophos Mobile Security	○ Guidelines for Securing iOS Devices
➢ 360 Security, AVL, and Avira Antivirus Security	○ iOS Device Tracking Tools
➢ Android Vulnerability Scanner: X-Ray	○ iOS Device Security Tools
➢ Android Device Tracking Tools	▪ Mobile Spyware
▪ Hacking iOS	○ Mobile Spyware
○ Apple iOS	○ Mobile Spyware: mSpy
○ Jailbreaking iOS	○ Mobile Spywares
• Types of Jailbreaking	▪ Mobile Device Management
• Jailbreaking Techniques	○ Mobile Device Management (MDM)
• App Platform for Jailbroaken Devices: Cydia	○ Mobile Device Management Solutions
• Jailbreaking Tool: Pangu	○ Bring Your Own Device (BYOD)
➢ Untethered Jailbreaking of iOS 7.1.1/7.1.2 Using Pangu for Mac	• BYOD Risks
• Jailbreaking Tools	• BYOD Policy Implementation
➢ Redsn0w and Absinthe	• BYOD Security Guidelines
➢ evasi0n7 and GeekSn0w	▪ Mobile Security Guidelines and Tools

➢ Sn0wbreeze and PwnageTool	○ General Guidelines for Mobile Platform Security
➢ LimeRa1n and Blackra1n	○ Mobile Device Security Guidelines for Administrator
○ Guidelines for Securing iOS Devices	○ SMS Phishing Countermeasures
• iOS Device Tracking Tools	○ Mobile Protection Tools
~~▪ Hacking Windows Phone OS~~	○ Mobile Anti-Spyware
~~○ Windows Phone 8~~	▪ Mobile Pen Testing
~~○ Windows Phone 8 Architecture~~	○ Android Phone Pen Testing
~~○ Secure Boot Process~~	○ iPhone Pen Testing
~~○ Guidelines for Securing Windows OS Devices~~	○ Mobile Pen Testing Toolkit: Hackode
~~• Windows OS Device Tracking Tool: FollowMee GPS Tracker~~	
~~▪ Hacking BlackBerry~~	
~~○ BlackBerry Operating System~~	
~~○ BlackBerry Enterprise Solution Architecture~~	
~~○ Blackberry Attack Vectors~~	
~~• Malicious Code Signing~~	
~~• JAD File Exploits and Memory/ Processes Manipulations~~	
~~• Short Message Service (SMS) Exploits~~	
~~• Email Exploits~~	
~~• PIM Data Attacks and TCP/IP Connections Vulnerabilities~~	
~~○ Guidelines for Securing BlackBerry Devices~~	
~~• BlackBerry Device Tracking Tools: MobileTracker and Position Logic Blackberry Tracker~~	
• Mobile Spyware: mSpy and StealthGenie	
• Mobile Spyware	
▪ Mobile Device Management	
○ Mobile Device Management (MDM)	
• MDM Solution: MaaS360 Mobile Device Management (MDM)	
• MDM Solutions	
○ Bring Your Own Device (BYOD)	
• BYOD Risks	
• BYOD Policy Implementation	
• BYOD Security Guidelines for Administrator	

• BYOD Security Guidelines for Employee	
▪ Mobile Security Guidelines and Tools	
○ General Guidelines for Mobile Platform Security	
○ Mobile Device Security Guidelines for Administrator	
○ SMS Phishing Countermeasures	
○ Mobile Protection Tool	
• BullGuard Mobile Security	
• Lookout	
• WISeID	
• zIPS	
○ Mobile Protection Tools	
○ Mobile Anti-Spyware	
▪ Mobile Pen Testing	
○ Android Phone Pen Testing	
○ iPhone Pen Testing	
○ Windows Phone Pen Testing	
○ BlackBerry Pen Testing	
○ Mobile Pen Testing Toolkit	
• zANTI	
• dSploit	
• Hackode (The Hacker's Toolbox)	
	Module 18: IoT Hacking
	▪ IoT Concepts
	○ What is IoT
	○ How IoT Works
	○ IoT Architecture
	○ IoT Application Areas and Devices
	○ IoT Technologies and Protocols
	○ IoT Communication Models
	○ Challenges of IoT
	○ Threat vs Opportunity
	▪ IoT Attacks
	○ IoT Security Problems
	○ OWASP Top 10 IoT Vulnerabilities and Obstacles
	○ IoT Attack Surface Areas

	○ IoT Threats
	○ Hacking IoT Devices: General Scenario
	○ IoT Attacks
	• DDoS Attack
	• Exploit HVAC
	• Rolling Code Attack
	• BlueBorne Attack
	• Jamming Attack
	• Hacking Smart Grid / Industrial Devices: Remote Access using Backdoor
	• Othr IoT Attacks
	○ IoT Attacks in Different Sectors
	○ Case Study: Dyn Attack
	▪ IoT Hacking Methodology
	○ What is IoT Device Hacking?
	○ IoT Hacking Methodology
	• Information Gathering Using Shodan
	• Information Gathering using MultiPing
	• Vulnerability Scanning using Nmap
	• Vulnerability Scanning using RIoT Vulnerability Scanner
	• Sniffing using Foren6
	• Rolling code Attack using RFCrack
	• Hacking Zigbee Devices with Attify Zigbee Framework
	• BlueBorne Attack Using HackRF One
	• Gaining Remote Access using Telnet
	• Maintain Access by Exploiting Firmware
	▪ IoT Hacking Tools
	○ Information Gathering Tools
	○ Sniffing Tools
	○ Vulnerability Scanning Tools
	○ 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 Security Tools
	▪ IoT Pen Testing
	○ IoT Pen Testing
Module 17: Cloud Computing	**Module 19: Cloud Computing**
~~▪ Statistics: Cloud Predictions~~	▪ Cloud Computing Concepts
▪ Introduction to Cloud Computing	○ Introduction to Cloud Computing
○ Types of Cloud Computing Services	○ Separation of Responsibilities in Cloud
○ Separation of Responsibilities in Cloud	○ Cloud Deployment Models
○ Cloud Deployment Models	○ NIST Cloud Deployment Reference Architecture
○ NIST Cloud Computing Reference Architecture	○ Cloud Computing Benefits
○ Cloud Computing Benefits	○ Understanding Virtualization
○ Understanding Virtualization	▪ Cloud Computing Threats
○ Benefits of Virtualization in Cloud	○ Cloud Computing Threats
▪ Cloud Computing Threats	▪ Cloud Computing Attacks
▪ Cloud Computing Attacks	○ Service Hijacking using Social Engineering Attacks
○ Service Hijacking using Social Engineering Attacks	○ Service Hijacking using Network Sniffing
○ Service Hijacking using Network Sniffing	○ Session Hijacking using XSS Attack
○ Session Hijacking using XSS Attack	○ Session Hijacking using Session Riding
○ Session Hijacking using Session Riding	○ Domain Name System (DNS) Attacks
○ Domain Name System (DNS) Attacks	○ Side Channel Attacks or Cross-guest VM Breaches
○ Side Channel Attacks or Cross-guest VM Breaches	○ SQL Injection Attacks
• Side Channel Attack Countermeasures	○ Cryptanalysis Attacks
○ SQL Injection Attacks	○ Wrapping Attack
○ Cryptanalysis Attacks	○ Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
• Cryptanalysis Attack Countermeasures	○ Man-in-the-Cloud Attack
○ Wrapping Attack	▪ Cloud Security
○ Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks	○ Cloud Security Control Layers
▪ Cloud Security	○ Cloud Security is the Responsibility of both Cloud Provider and Consumer
○ Cloud Security Control Layers	○ Cloud Computing Security Considerations
○ Cloud Security is the Responsibility of both Cloud Provider and Consumer	○ Placement of Security Controls in the Cloud
○ Cloud Computing Security Considerations	○ Best Practices for Securing Cloud

○ Placement of Security Controls in the Cloud	○ NIST Recommendations for Cloud Security
○ Best Practices for Securing Cloud	○ Organization/Provider Cloud Security Compliance Checklist
○ NIST Recommendations for Cloud Security	▪ Cloud Security Tools
○ Organization/Provider Cloud Security Compliance Checklist	○ Cloud Security Tools
▪ Cloud Security Tools	▪ Cloud Penetration Testing
○ Core CloudInspect	○ What is Cloud Pen Testing?
○ CloudPassage Halo	○ Key Considerations for Pen Testing in the Cloud
○ Cloud Security Tools	○ Cloud Penetration Testing
▪ Cloud Penetration Testing	○ Recommendations for Cloud Testing
○ What is Cloud Pen Testing?	
○ Key Considerations for Pen Testing in the Cloud	
○ Scope of Cloud Pen Testing	
○ Cloud Penetration Testing	
○ Recommendations for Cloud Testing	
Module 18: Cryptography	**Module 20: Cryptography**
~~▪ Market Survey 2014: The Year of Encryption~~	▪ Cryptography Concepts
~~▪ Case Study: Heartbleed~~	○ Cryptography
~~▪ Case Study: Poodlebleed~~	• Types of Cryptography
▪ Cryptography Concepts	○ Government Access to Keys (GAK)
○ Cryptography	▪ Encryption Algorithms
○ Types of Cryptography	○ Ciphers
○ Government Access to Keys (GAK)	○ Data Encryption Standard (DES)
▪ Encryption Algorithms	○ Advanced Encryption Standard (AES)
○ Ciphers	○ RC4, RC5, and RC6 Algorithms
○ Data Encryption Standard (DES)	○ Twofish
○ Advanced Encryption Standard (AES)	○ The DSA and Related Signature Schemes
○ RC4, RC5, RC6 Algorithms	○ Rivest Shamir Adleman (RSA)
○ The DSA and Related Signature Schemes	○ Diffie-Hellman
○ RSA (Rivest Shamir Adleman)	○ Message Digest (One-Way Hash) Functions
• The RSA Signature Scheme	• Message Digest Function: MD5
• Example of RSA Algorithm	• Secure Hashing Algorithm (SHA)
○ Message Digest (One-way Hash) Functions	• RIPEMD - 160
• Message Digest Function: MD5	• HMAC
○ Secure Hashing Algorithm (SHA)	▪ Cryptography Tools

~~○ What is SSH (Secure Shell)?~~	○ MD5 Hash Calculators
▪ Cryptography Tools	○ Hash Calculators for Mobile
○ MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles	○ Cryptography Tools
○ Hash Calculators for Mobile: MD5 Hash Calculator, Hash Droid, and Hash Calculator	• Advanced Encryption Package 2017
○ Cryptography Tool	• BCTextEncoder
• Advanced Encryption Package 2014	• Cryptography Tools
• BCTextEncoder	○ Cryptography Tools for Mobile
○ Cryptography Tools	▪ Public Key Infrastructure (PKI)
○ Cryptography Tools for Mobile: Secret Space Encryptor, CryptoSymm, and Cipher Sender	○ Public Key Infrastructure (PKI)
▪ Public Key Infrastructure (PKI)	• Certification Authorities
○ Certification Authorities	• Signed Certificate (CA) Vs. Self Signed Certificate
○ Signed Certificate (CA) Vs. Self Signed Certificate	▪ Email Encryption
▪ Email Encryption	○ Digital Signature
○ Digital Signature	○ Secure Sockets Layer (SSL)
○ SSL (Secure Sockets Layer)	○ Transport Layer Security (TLS)
○ Transport Layer Security (TLS)	○ Cryptography Toolkit
○ Cryptography Toolkit	• OpenSSL
• OpenSSL	• Keyczar
• Keyczar	○ Pretty Good Privacy (PGP)
○ Pretty Good Privacy (PGP)	▪ Disk Encryption
▪ Disk Encryption	○ Disk Encryption
○ Disk Encryption Tools: Symantec Drive Encryption and GiliSoft Full Disk Encryption	○ Disk Encryption Tools
○ Disk Encryption Tools	• VeraCrypt
▪ Cryptography Attacks	• Symantec Drive Encryption
○ Code Breaking Methodologies	• Disk Encryption Tools
○ Brute-Force Attack	▪ Cryptanalysis
○ Meet-in-the-Middle Attack on Digital Signature Schemes	○ Cryptanalysis Methods
○ Side Channel Attack	• Linear Cryptanalysis
• Side Channel Attack - Scenario	• Differential Cryptanalysis
▪ Cryptanalysis Tools	• Integral Cryptanalysis
○ Cryptanalysis Tool: CrypTool	○ Code Breaking Methodologies
○ Cryptanalysis Tools	○ Cryptography Attacks
○ Online MD5 Decryption Tools	• Brute-Force Attack

	• Birthday Attack
	➢ Birthday Paradox: Probability
	• Meet-in-the-Middle Attack on Digital Signature Schemes
	• Side Channel Attack
	• Hash Collision Attack
	• DUHK Attack
	• Rainbow Table Attack
	○ Cryptanalysis Tools
	○ Online MD5 Decryption Tools
	▪ Countermeasures
	○ How to Defend Against Cryptographic Attacks

Labs Comparison

The notations used:

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

CEHv9	CEHv10
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. Open Source Information Gathering using Windows Command Line Utilities
2. Gathering personal information using Online People Search Services	2. Finding Company's Sub-domains using Sublist3r
3. Collecting Information about a Target Website Using Firebug	3. Gathering Personal Information using Online People Search Services
4. Extracting a Company's Data Using Web Data Extractor	4. Gathering Information from LinkedIn using InSpy
5. Mirroring Website Using HTTrack Web Site Copier	5. Collecting Information About a Target Website using Firebug
6. Collecting Information about a Target by Tracing Emails	6. Extracting a Company's Data using Web Data Extractor
7. Gathering IP and Domain Name Information Using Whois Lookup	7. Mirroring Website using HTTrack Web Site Copier
8. Advanced network Route Tracing using Path Analyzer Pro	8. Collecting Information About a Target by Tracing Emails
9. Footprinting a target Using Maltego	9. Gathering IP and Domain Name Information using Whois Lookup
10. Performing Automated Network Reconnaissance Using Recon-ng	10. Advanced Network Route Tracing Using Path Analyzer Pro
11. Using Open-source Reconnaissance Tool Recon-ng to Gather Personnel Information	11. Footprinting a Target using Maltego
12. Collecting Information from Social Networking Sites Using Recon-ng Pushpin	12. Performing Automated Network Reconnaissance using Recon-ng
13. Automated Fingerprinting of an Organization Using FOCA	13. Using the Open-source Reconnaissance Tool Recon-ng to Gather Personnel Information
~~14. Identifying Vulnerabilities and Information Disclosures in Search Engines Using SearchDiggity~~	14. Collecting Information from Social Networking Sites using Recon-ng Pushpin
	15. Automated Fingerprinting of an Organization using FOCA
	16. Open Source Intelligence Gathering using OSRFramework

	17. Information Gathering using Metasploit
	18. Information Gathering using theHarvester
Module 03: Scanning Networks	**Module 03: Scanning Networks**
1. UDP and TCP Packet Crafting Techniques using HPING3	1. Scanning the Network using the Colasoft Packet Builder
2. Scanning the Network Using the Colasoft Packet Builder	2. UDP and TCP Packet Crafting Techniques using HPING3
3. Basic Network Troubleshooting Using the MegaPing	3. Basic Network Troubleshooting using MegaPing
4. Understanding Network Scanning Using Nmap	4. Understanding Network Scanning using Nmap
5. Exploring Various Network Scanning Techniques	5. Scanning a Network using NetScan Tools Pro
6. Scanning a Network Using the NetScan Tools Pro	6. Scanning for Network Traffic Going through a Computer's Adapter using IP-Tools
7. Avoiding Scanning Detection using Multiple Decoy IP Addresses	7. Checking for Live Systems using Angry IP Scanner
8. Vulnerability Analysis Using the Nessus	8. Exploring Various Network Scanning Techniques
9. Scanning for Network Vulnerabilities Using the GFI LanGuard 2014	9. Perform ICMP Probing using Ping/Traceroute for Network Troubleshooting
10. Drawing Network Diagrams Using Network Topology Mapper	10. Avoiding Scanning Detection using Multiple Decoy IP Addresses
~~11. Scanning Devices in a Network using The Dude~~	11. Daisy Chaining using Proxy Workbench
12. Daisy Chaining using Proxy Workbench	12. Anonymous Browsing using Proxy Switcher
13. Anonymous Browsing using Proxy Switcher	13. Anonymous Browsing using CyberGhost
14. Anonymous Browsing using CyberGhost	14. Identify Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark
	15. Drawing Network Diagrams using Network Topology Mapper
Module 04: Enumeration	**Module 04: Enumeration**
1. NetBIOS Enumeration Using Global Network Inventory	1. NetBIOS Enumeration using Global Network Inventory
2. Enumerating Network Resources Using Advanced IP Scanner	2. Enumerating Network Resources using Advanced IP canner
3. Performing Network Enumeration Using SuperScan	3. Performing Network Enumeration using SuperScan
4. Enumerating Resources in a Local Machine Using Hyena	4. Enumerating Resources in a Local Machine using Hyena
5. Performing Network Enumeration Using NetBIOS Enumerator	5. Performing Network Enumeration using NetBIOS Enumerator
6. Enumerating a Network Using SoftPerfect Network Scanner	6. Enumerating a Network using SoftPerfect Network Scanner

7. Enumerating a Target Network using Nmap and Net Use	7. Enumerating a Target Network using Nmap and Net Use
8. Enumerating Services on a Target Machine	8. Enumerating Services on a Target Machine
9. SNMP Enumeration Using SNMPCHECK	9. SNMP Enumeration using snmp_enum
10. LDAP Enumeration Using Active Directory Explorer (ADExplorer)	10. LDAP Enumeration using Active Directory Explorer (ADExplorer)
~~11. Performing Network Enumeration Using Various DNS Interrogation Tools~~	11. Enumerating Information from Windows and Samba Host using Enum4linux
	Module 05: Vulnerability Analysis
	1. Vulnerability Analysis using Nessus
	2. Scanning for Network Vulnerabilities using the GFI LanGuard
	3. CGI Scanning with Nikto
Module 05: System Hacking	**Module 06: System Hacking**
1. Dumping and Cracking SAM Hashes to Extract Plaintext Passwords	1. Active Online Attack using Responder
2. Creating and Using the Rainbow Tables	2. Dumping and Cracking SAM Hashes to Extract Plaintext Passwords
3. Auditing System Passwords Using L0phtCrack	3. Creating and using the Rainbow Tables
4. Exploiting Client Side Vulnerabilities and Establishing a VNC Session	4. Auditing System Passwords using L0phtCrack
5. Escalating Privileges by Exploiting Client Side Vulnerabilities	5. Exploiting Client Side Vulnerabilities and Establishing a VNC Session
~~6. Exploiting freeSSHd Vulnerability and Gaining Access to a Target System~~	6. Escalating Privileges by Exploiting Client Side Vulnerabilities
7. Hacking Windows 8.1 using Metasploit and Post Exploitation Using Meterpreter	7. Hacking Windows Server 2012 with a Malicious Office Document using TheFatRat
~~8. System Monitoring Using RemoteExec~~	8. Hacking Windows 10 using Metasploit and Post-Exploitation using Meterpreter
9. User System Monitoring and Surveillance Using Spytech SpyAgent	9. User System Monitoring and Surveillance using Spytech SpyAgent
10. Web Activity Monitoring and Recording using Power Spy 2014	10. Web Activity Monitoring and Recording using Power Spy
11. Hiding Files Using NTFS Streams	11. Hiding Files using NTFS Streams
~~12. Find Hidden Files Using ADS Spy~~	12. Hiding Data using White Space Steganography
13. Hiding Data Using White Space Steganography	13. Image Steganography using OpenStego
14. Image Steganography Using OpenStego	14. Image Steganography using Quick Stego
15. Image Steganography Using Quick Stego	15. Covert channels using Covert_TCP
16. Viewing, Enabling and Clearing the Audit Policies Using Auditpol	16. Viewing, Enabling and Clearing Audit Policies using Auditpol

Module 06: Malware Threats	**Module 07: Malware Threats**
1. Creating a HTTP Trojan and Remotely Controlling a Target Machine Using HTTP RAT	1. Gaining Control over a Victim Machine using njRAT
2. Creating a Trojan Server Using the GUI Trojan MoSucker	2. Obfuscating a Trojan using SwayzCryptor and Making it Undetectable to Various Anti-Virus Programs
3. Gaining Control over a Victim machine Using njRAT	3. Creating a Trojan Server using the GUI Trojan MoSucker
4. Obfuscating a Trojan Using SwayzCryptor and Making it Undetectable from Various Anti-Virus Programs	4. Creating a Server using the ProRat Tool
5. Creating a Trojan Server Using the ProRat Tool	5. Creating a Trojan Server using Theef
6. Creating a Trojan Server Using the Theef	6. Creating a HTTP Trojan and Remote Controlling a Target Machine using HTTP RAT
~~7. Attaining Remote Access Using Atelier Web Remote Commander~~	7. Creating a Virus using the JPS Virus Maker Tool
~~8. Building a Botnet Infrastructure Using Umbra Loader~~	8. Creating a Worm using the Internet Worm Maker Thing
9. Creating a Virus Using the JPS Virus Maker Tool	9. Virus Analysis using VirusTotal
~~10. Creating a Worm Using Ghost Eye Worm and maintaining a Persistent Connection Using njRAT~~	10. Virus Analysis using IDA Pro
11. Creating a Worm Using the Internet Worm Maker Thing	11. Virus Analysis using OllyDbg
12. Virus analysis using IDA Pro	12. Monitoring TCP/IP Connections using the CurrPorts
13. Virus analysis using Virus Total	13. Performing Registry Entry Monitoring
14. Virus Analysis Using OllyDbg	14. Startup Program Monitoring Tool
15. Detecting Trojans	15. Perform Device Driver Monitoring
16. Monitoring TCP/IP Connections Using the CurrPorts	16. Detecting Trojans
	17. Removing Malware using ClamWin
Module 07: Sniffing	**Module 08: Sniffing**
1 Sniffing Passwords using Wireshark	1. Performing Man-in-the-Middle Attack using Cain & Abel
2 Analyzing a Network Using the Capsa Network Analyzer	2. Spoofing MAC Address using SMAC
3 Sniffing the Network Using the OmniPeek Network Analyzer	3. Sniffing Passwords using Wireshark
4 Spoofing MAC Address Using SMAC	4. Analyzing a Network using the Capsa Network Analyzer

5 Performing Man-in-the-Middle Attack using Cain & Abel	5. Sniffing the Network using the Omnipeek Network Analyzer
~~6 Detecting Systems running in Promiscuous mode in a Network using PromqryUI~~	6. Detecting ARP Poisoning in a Switch Based Network
7 Detecting ARP Poisoning in a Switch Based Network	7. Detecting ARP Attacks with XArp Tool
8 Detecting ARP attacks with XArp tool	
~~9 Performing DNS Poisoning in a Switch Based Network~~	
Module 08: Social Engineering	**Module 09: Social Engineering**
1. Detecting Phishing Using Netcraft	1. Detecting Phishing using Netcraft
2. Detecting Phishing Using PhishTank	2. Detecting Phishing using PhishTank
3. Sniffing Facebook Credentials using Social Engineering Toolkit (SET)	3. Sniffing Facebook Credentials using Social Engineering Toolkit (SET)
~~4. Creating a Malicious Payload Using SET and Exploiting a Windows Machine~~	4. Phishing User Credentials using SpeedPhish Framework (SPF)
Module 09: Denial-of-Service	**Module 10: Denial-of-Service**
1. SYN Flooding a Target Host Using Metasploit	1. SYN Flooding a Target Host using Metasploit
2. SYN Flooding a Target Host Using hping3	2. SYN Flooding a Target Host using hping3
~~3. HTTP Flooding using DoSHTTP~~	3. Performing Distributed Denial of Service Attack using HOIC
~~4. Implementing DoS Attack on a Router using Slowloris Script~~	4. Detecting and Analyzing DoS Attack Traffic using KFSensor and Wireshark
5. Performing Distributed Denial of Service Attack Using HOIC	
6. Detecting and Analyzing DoS Attack Traffic Using KFSensor and Wireshark	
Module 10: Session Hijacking	**Module 11: Session Hijacking**
1. Session Hijacking Using the Zed Attack Proxy (ZAP)	1. Session Hijacking using the Zed Attack Proxy (ZAP)
~~2. Hijacking a User Session Using Firebug~~	2. Perform sslstrip and Intercept HTTP Traffic through BetterCAP
~~3. Hijacking HTTPS Traffic in a Network Using sslstrip~~	
~~4. Performing a MiTM Attack and Hijacking an Established Session Using Websploit~~	
Module 16: Evading IDS, Firewalls, and Honeypots	**Module 12: Evading IDS, Firewalls, and Honeypots**
1. Detecting Intrusions using Snort	1. Detecting Intrusions using Snort

2. Detecting Malicious Network Traffic Using HoneyBot	2. Detecting Malicious Network Traffic using HoneyBOT
3. Detecting Intruders and Worms using KFSensor Honeypot IDS	3. Detecting Intruders and Worms using KFSensor Honeypot IDS
4. Bypassing Windows Firewall Using Nmap Evasion Techniques	4. Bypassing Windows Firewall using Nmap Evasion Techniques
5. Bypassing Firewall Rules Using HTTP/FTP Tunneling	5. Bypassing Firewall Rules using HTTP/FTP Tunneling
6. Bypassing Windows Firewall and Maintaining a Persistent Connection with a Victim	6. Bypassing Windows Firewall using Metasploit
Module 11: Hacking Webservers	**Module 13: Hacking Web Servers**
1. Performing Web Server Reconnaissance using Skipfish	1. Performing Web Server Reconnaissance using Skipfish
2. Footprinting Webserver Using the httprecon Tool	2. Footprinting a Web Server using the httprecon Tool
3. Footprinting a Webserver Using ID Serve	3. Footprinting a Web Server using ID Serve
~~4. Exploiting Java Vulnerability using Metasploit Framework~~	4. Uniscan Web Server Fingerprinting in Kali Linux
~~5. Performing ShellShock Exploitation on a Web Server and Gaining Unrestricted Access to the Server~~	5. Cracking FTP Credentials using Dictionary Attack
6. Cracking FTP Credentials Using Dictionary Attack	
Module 12: Hacking Web Applications	**Module 14: Hacking Web Applications**
1. Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications	1. Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications
~~2. Using Stored XSS Attack to Hijack an Authenticated User Session~~	2. Performing Cross-Site Request Forgery (CSRF) Attack
3. Enumerating and Hacking a Web Application Using WPScan and Metasploit	3. Enumerating and Hacking a Web Application using WPScan and Metasploit
~~4. Exploiting WordPress Plugin Vulnerabilities using Metasploit~~	4. Exploiting Remote Command Execution Vulnerability to Compromise a Target Web Server
5. Exploiting Remote Command Execution Vulnerability to Compromise a Target Web Server	5. Exploiting File Upload Vulnerability at Different Security Levels
~~6. Auditing Web Application Framework Using W3AF~~	6. Website Vulnerability Scanning using Acunetix WVS
7. Website Vulnerability Scanning Using Acunetix WVS	7. Auditing Web Application Framework using Vega

Module 13: SQL Injection	**Module 15: SQL Injection**
1. SQL Injection Attacks on MS SQL Database	1. SQL Injection Attacks on MSSQL Database
~~2. Performing Blind SQL Injection on DVWA Application~~	2. Performing SQL Injection Attack against MSSQL to Extract Databases and WebShell using SQLMAP
3. Testing for SQL Injection Using IBM Security AppScan Tool	3. Testing for SQL Injection using IBM Security AppScan Tool
~~4. Testing for SQL Injection Using WebCruiser Tool~~	4. Scanning Web Applications using N-Stalker Tool
5. Scanning Web Applications Using N-Stalker Tool	
Module 14: Hacking Wireless Networks	**Module 16: Hacking Wireless Networks**
1. WiFi Packet Sniffing Using AirPcap with Wireshark	1. WiFi Packet Sniffing using Microsoft Network Monitor and Wireshark
~~2. Sniffing the Network Using the OmniPeek Network Analyzer~~	2. Cracking a WEP Network with Aircrack-ng
3. Cracking a WEP Network with Aircrack-ng for Windows	3. Cracking a WPA Network with Aircrack-ng
Module 15: Hacking Mobile Platforms	**Module 17: Hacking Mobile Platforms**
1. Creating Binary Payloads using Kali Linux to Hack Android	1. Creating Binary Payloads using Kali Linux to Hack Android
2. Harvesting Users' Credentials Using Social Engineering Toolkit	2. Harvesting Users' Credentials using Social Engineering Toolkit
3. Using Mobile Platform to Enforce a DoS Attack on a Victim Machine	3. Using Mobile Platform to Enforce a DoS Attack on a Target Website
4. Securing Android Device from Malicious Applications	4. Hacking Android Device with a Malicious App using TheFatRat
	5. Securing Android Devices from Malicious Applications
Module 17: Cloud Computing Security	**Module 19: Cloud Computing**
1. Building a Cloud Using ownCloud and WampServer	1. Building a Cloud using ownCloud and LAMPServer
~~2. Transferring Cloud Data Over Secure Channel~~	2. Securing ownCloud from Malicious File Uploads using ClamAV
~~3. Harvesting Cloud Credentials by Exploiting Java Vulnerability~~	3. Bypassing ownCloud AV and Hacking the Host using Kali Linux
~~4. Performing Cloud Vulnerability Assessment Using Mobile Based Security Scanner zANTI~~	4. Implementing DoS Attack on Linux Cloud Server using Slowloris Script

Module 18: Cryptography	**Module 20: Cryptography**
~~1. Calculating MD5 Hashes and Verifying File Integrity Using Quick Checksum Verifier~~	1. Calculating One-way Hashes using HashCalc
2. Calculating One-way Hashes Using HashCalc	2. Calculating MD5 Hashes using MD5 Calculator
3. Calculating MD5 Hashes Using MD5 Calculator	3. Understanding File and Text Encryption using CryptoForge
4. Understanding File and Text Encryption Using CryptoForge	4. Basic Data Encryption using Advanced Encryption Package
5. Basic Data Encryption Using Advanced Encryption Package	5. Encrypting and Decrypting the Data using BCTextEncoder
6. Encrypting and Decrypting the Data Using BCTextEncoder	6. Creating and using Self-Signed Certificates
~~7. Exploiting OpenSSL Heartbleed Vulnerability on a HTTPS website~~	7. Basic Disk Encryption using VeraCrypt
8. Creating and Using Self-Signed Certificates	8. Basic Data Encrypting using Rohos Disk Encryption
9. Basic Disk Encryption Using VeraCrypt	9. Basic Data Encryption using CrypTool
10. Basic Data Encrypting Using Rohos Disk Encryption	
11. Basic Data Encryption Using CrypTool	