Ethical Hacking Course Curriculum

1. Introduction to Ethical Hacking

- Internet is Integral Part of Business and Personal Life – What Happens Online in 60 Seconds
- Information Security Overview
  - Case Study
    - eBay Data Breach
    - Google Play Hack
    - The Home Depot Data Breach
  - Year of the Mega Breach
  - Data Breach Statistics
  - Malware Trends in 2014
  - Essential Terminology
  - Elements of Information Security
  - The Security, Functionality, and Usability Triangle
- Information Security Threats and Attack Vectors
  - Motives, Goals, and Objectives of Information Security Attacks
  - Top Information Security Attack Vectors
  - Information Security Threat Categories
  - Types of Attacks on a System
    - Operating System Attacks
      - Examples of OS Vulnerabilities
    - Misconfiguration Attacks
    - Application-Level Attacks
      - Examples of Application-Level Attacks
    - Shrink Wrap Code Attacks

- Information Warfare
- Hacking Concepts, Types, and Phases
  - What is Hacking
  - Who is a Hacker?
  - Hacker Classes
  - Hacking Phases
    - Reconnaissance
    - Scanning
    - Gaining Access
    - Maintaining Access
    - Clearing Tracks
- Ethical Hacking Concepts and Scope
  - What is Ethical Hacking?
  - Why Ethical Hacking is Necessary
  - Scope and Limitations of Ethical Hacking
  - Skills of an Ethical Hacker
- Information Security Controls
  - Information Assurance (IA)
  - Information Security Management Program
  - Threat Modeling
  - Enterprise Information Security Architecture (EISA)
  - Network Security Zoning
  - Defense in Depth
  - Information Security Policies
    - Types of Security Policies
    - Examples of Security Policies
    - Privacy Policies at Workplace

        - Steps to Create and Implement Security Policies
        - HR/Legal Implications of Security Policy Enforcement
    - Physical Security
        - Physical Security Controls
    - Incident Management
        - Incident Management Process
        - Responsibilities of an Incident Response Team
    - What is Vulnerability Assessment?
        - Types of Vulnerability Assessment
        - Network Vulnerability Assessment Methodology
        - Vulnerability Research
        - Vulnerability Research Websites
    - Penetration Testing
        - Why Penetration Testing
        - Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
        - Blue Teaming/Red Teaming
        - Types of Penetration Testing
        - Phases of Penetration Testing
        - Security Testing Methodology
        - Penetration Testing Methodology
- Information Security Laws and Standards
    - Payment Card Industry Data Security Standard (PCI-DSS)
    - ISO/IEC 27001:2013
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Sarbanes Oxley Act (SOX)
    - The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

- Cyber Law in Different Countries

2. Footprinting and Reconnaissance

- Footprinting Concepts
  - What is Footprinting?
  - Objectives of Footprinting
- Footprinting Methodology
  - Footprinting through Search Engines
    - Finding Company's Public and Restricted Websites
    - Determining the Operating System
    - Collect Location Information
    - People Search: Social Networking Services
    - People Search Online Services
    - Gather Information from Financial Services
    - Footprinting through Job Sites
    - Monitoring Target Using Alerts
    - Information Gathering Using Groups, Forums, and Blogs
  - Footprinting using Advanced Google Hacking Techniques
    - Google Advance Search Operators
    - Finding Resources Using Google Advance Operator
    - Google Hacking Database (GHDB)
    - Information Gathering Using Google Advanced Search
  - Footprinting through Social Networking Sites
    - Collect Information through Social Engineering on Social Networking Sites
    - Information Available on Social Networking Sites

- Website Footprinting
  - Website Footprinting using Web Spiders
  - Mirroring Entire Website
    - Website Mirroring Tools
  - Extract Website Information from http://www.archive.org
  - Monitoring Web Updates Using Website Watcher
    - Web Updates Monitoring Tools
- Email Footprinting
  - Tracking Email Communications
    - Collecting Information from Email Header
    - Email Tracking Tools
- Competitive Intelligence
  - Competitive Intelligence Gathering
  - Competitive Intelligence – When Did this Company Begin? How Did it Develop?
  - Competitive Intelligence – What Are the Company's Plans?
  - Competitive Intelligence – What Expert Opinions Say About the Company
  - Monitoring Website Traffic of Target Company
  - Tracking Online Reputation of the Target
    - Tools for Tracking Online Reputation of the Target
- WHOIS Footprinting
  - WHOIS Lookup
  - WHOIS Lookup Result Analysis
  - WHOIS Lookup Tools
  - WHOIS Lookup Tools for Mobile
- DNS Footprinting
  - Extracting DNS Information

        - DNS Interrogation Tools
    - Network Footprinting
        - Locate the Network Range
        - Traceroute
        - Traceroute Analysis
        - Traceroute Tools
    - Footprinting through Social Engineering
        - Footprinting through Social Engineering
        - Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- Footprinting Tools
    - Footprinting Tool
        - Maltego
        - Recon-ng
    - Additional Footprinting Tools
- Footprinting Countermeasures
- Footprinting Penetration Testing
    - Footprinting Pen Testing
    - Footprinting Pen Testing Report Templates

3. Scanning Networks

- Overview of Network Scanning
    - TCP Communication Flags
    - TCP/IP Communication
    - Creating Custom Packet Using TCP Flags

- CEH Scanning Methodology
  - Check for Live Systems
    - Checking for Live Systems – ICMP Scanning
    - Ping Sweep
      - Ping Sweep Tools
  - Check for Open Ports
    - SSDP Scanning
    - Scanning IPv6 Network
    - Scanning Tool
      - Nmap
      - Hping2 / Hping3
      - Hping Commands
    - Scanning Techniques
      - TCP Connect / Full Open Scan
      - Stealth Scan (Half-open Scan)
      - Inverse TCP Flag Scanning
      - Xmas Scan
      - ACK Flag Probe Scanning
      - IDLE/IPID Header Scan
        - IDLE Scan: Step 1
        - IDLE Scan: Step 2 and 3
      - UDP Scanning
      - ICMP Echo Scanning/List Scan
    - Scanning Tool: NetScan Tools Pro
    - Scanning Tools
    - Scanning Tools for Mobile
    - Port Scanning Countermeasures

- Scanning Beyond IDS
  - IDS Evasion Techniques
  - SYN/FIN Scanning Using IP Fragments
- Banner Grabbing
  - Banner Grabbing Tools
  - Banner Grabbing Countermeasures
    - Disabling or Changing Banner
    - Hiding File Extensions from Web Pages
- Scan for Vulnerability
  - Vulnerability Scanning
  - Vulnerability Scanning Tool
    - Nessus
    - GAFI LanGuard
    - Qualys FreeScan
  - Network Vulnerability Scanners
  - Vulnerability Scanning Tools for Mobile
- Draw Network Diagrams
  - Drawing Network Diagrams
  - Network Discovery Tool
    - Network Topology Mapper
    - OpManager and NetworkView
  - Network Discovery and Mapping Tools
  - Network Discovery Tools for Mobile
- 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

4. Enumeration

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

        - SuperScan
        - Hyena
        - Winfingerprint
        - NetBIOS Enumerator and Nsauditor Network Security Auditor
    - Enumerating User Accounts
    - Enumerating Shared Resources Using Net View
- SNMP Enumeration
    - Working of SNMP
    - Management Information Base (MIB)
    - SNMP Enumeration Tool
        - OpUtils
        - Engineer's Toolset
    - SNMP Enumeration Tools
- LDAP Enumeration
    - LDAP Enumeration Tool: Softerra LDAP Administrator
    - LDAP Enumeration Tools
- NTP Enumeration
    - NTP Enumeration Commands
    - NTP Enumeration Tools
- SMTP Enumeration
    - SMTP Enumeration Tool: NetScanTools Pro
    - Telnet Enumeration
    - DNS Zone Transfer Enumeration Using NSLookup
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing

5. System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
  - Cracking Passwords
    - Password Cracking
    - Types of Password Attacks
    - Non-Electronic Attacks
    - Active Online Attack
      - Dictionary, Brute Forcing and Rule-based Attack
      - Password Guessing
    - Default Passwords
    - Active Online Attack:
      - Trojan/Spyware/Keylogger
      - Example of Active Online Attack Using USB Drive
      - Hash Injection Attack
    - Passive Online Attack
      - Wire Sniffing
      - Man-in-the-Middle and Replay Attack
    - Offline Attack
      - Rainbow Attacks
        - Tools to Create Rainbow Tables: rtgen and Winrtgen
      - Distributed Network Attack
    - Elcomsoft Distributed Password Recovery
    - Microsoft Authentication

- How Hash Passwords Are Stored in Windows SAM?
  - NTLM Authentication Process
  - Kerberos Authentication
- Password Salting
- pwdump7 and fgdump
- Password Cracking Tools
  - L0phtCrack and Ophcrack
  - Cain & Abel and RainbowCrack
- Password Cracking Tools
- Password Cracking Tool for Mobile: FlexiSPY Password Grabber
- How to Defend against Password Cracking
- Implement and Enforce Strong Security Policy
- CEH System Hacking Steps

- Escalating Privileges
  - Privilege Escalation
  - Privilege Escalation Using DLL Hijacking
  - Privilege Escalation Tool: Active@ Password Changer
  - Privilege Escalation Tools
  - How to Defend Against Privilege Escalation
- Executing Applications
  - RemoteExec
  - PDQ Deploy
  - DameWare Remote Support
  - Keylogger
    - Types of Keystroke Loggers
    - Hardware Keyloggers
    - Keylogger: All In One Keylogger

        - Keyloggers for Windows
        - Keylogger for Mac: Amac Keylogger for Mac
        - Keyloggers for MAC
    - Spyware
        - Spyware: Spytech SpyAgent
        - Spyware: Power Spy 2014
        - What Does the Spyware Do?
        - Spyware
        - USB Spyware: USBSpy
        - Audio Spyware: Spy Voice Recorder and Sound Snooper
        - Video Spyware: WebCam Recorder
        - Cellphone Spyware: Mobile Spy
        - Telephone/Cellphone Spyware
        - GPS Spyware: SPYPhone
        - GPS Spyware
    - How to Defend Against Keyloggers
        - Anti-Keylogger: Zemana AntiLogger
        - Anti-Keylogger
    - How to Defend Against Spyware
        - Anti-Spyware: SUPERAntiSpyware
        - Anti-Spyware
- Hiding Files
    - Rootkits
        - Types of Rootkits
        - How Rootkit Works
        - Rootkit
            - Avatar

        - Necurs
        - Azazel
        - ZeroAccess
- Detecting Rootkits
    - Steps for Detecting Rootkits
    - How to Defend against Rootkits
    - Anti-Rootkit: Stinger and UnHackMe
    - Anti-Rootkits
- NTFS Data Stream
    - How to Create NTFS Streams
    - NTFS Stream Manipulation
    - How to Defend against NTFS Streams
    - NTFS Stream Detector: StreamArmor
    - NTFS Stream Detectors
- What Is Steganography?
    - Classification of Steganography
    - Types of Steganography based on Cover Medium
        - Whitespace Steganography Tool: SNOW
        - Image Steganography
        - Least Significant Bit Insertion
        - Masking and Filtering
        - Algorithms and Transformation
        - Image Steganography: QuickStego
        - Image Steganography Tools
        - Document Steganography: wbStego
        - Document Steganography Tools
        - Video Steganography

        - Video Steganography: OmniHide PRO and Masker
        - Video Steganography Tools
        - Audio Steganography
        - Audio Steganography: DeepSound
        - Audio Steganography Tools
        - Folder Steganography: Invisible Secrets 4
        - Folder Steganography Tools
        - Spam/Email Steganography: Spam Mimic
    - 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
    - Covering Tracks
    - Disabling Auditing: Auditpol
    - Clearing Logs
    - Manually Clearing Event Logs
    - Ways to Clear Online Tracks
    - Covering Tracks Tool: CCleaner
    - Covering Tracks Tool: MRU-Blaster
    - Track Covering Tools
- Penetration Testing
    - Password Cracking
    - Privilege Escalation

- Executing Applications
- Hiding Files
- Covering Tracks

6. Malware Threats

- Introduction to Malware
  - Different Ways a Malware can Get into a System
  - Common Techniques Attackers Use to Distribute Malware on the Web
- Trojan Concepts
  - Financial Loss Due to Trojans
  - What is a Trojan?
  - How Hackers Use Trojans
  - Common Ports used by Trojans
  - How to Infect Systems Using a Trojan
  - Wrappers
  - Dark Horse Trojan Virus Maker
  - Trojan Horse Construction Kit
  - Crypters: AIO FUD Crypter, Hidden Sight Crypter, and Galaxy Crypter
  - Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor
  - How Attackers Deploy a Trojan
    - Exploit Kit
    - Exploit Kit: Infinity
    - Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit
    - Exploit Kits: Bleedinglife and Crimepack
  - Evading Anti-Virus Techniques

- Types of Trojans
  - Command Shell Trojans
  - Defacement Trojans
  - Defacement Trojans: Restorator
  - Botnet Trojans
    - Tor-based Botnet Trojans: ChewBacca
    - Botnet Trojans: Skynet and CyberGate
  - Proxy Server Trojans
    - Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
  - FTP Trojans
  - VNC Trojans
    - VNC Trojans: WinVNC and VNC Stealer
  - HTTP/HTTPS Trojans
    - HTTP Trojan: HTTP RAT
  - Shttpd Trojan – HTTPS (SSL)
  - ICMP Tunneling
  - Remote Access Trojans
    - Optix Pro and MoSucker
    - BlackHole RAT and SSH – R.A.T
    - njRAT and Xtreme RAT
    - SpyGate – RAT and Punisher RAT
    - DarkComet RAT, Pandora RAT, and HellSpy RAT
    - ProRat and Theef
    - Hell Raiser
    - Atelier Web Remote Commander
  - Covert Channel Trojan: CCTT
  - E-banking Trojans

        - Working of E-banking Trojans
        - E-banking Trojan
            - ZeuS and SpyEye
            - Citadel Builder and Ice IX
    - Destructive Trojans: M4sT3r Trojan
    - Notification Trojans
    - Data Hiding Trojans (Encrypted Trojans)
- Virus and Worms Concepts
    - Introduction to Viruses
    - Stages of Virus Life
    - Working of Viruses:
        - Infection Phase
        - Attack Phase
    - Why Do People Create Computer Viruses
    - Indications of Virus Attack
    - Virus Hoaxes and Fake Antiviruses
    - Ransomware
    - Types of Viruses
        - System or Boot Sector Viruses
        - File and Multipartite Viruses
        - Macro Viruses
        - Cluster Viruses
        - Stealth/Tunneling Viruses
        - Encryption Viruses
        - Polymorphic Code
        - Metamorphic Viruses
        - File Overwriting or Cavity Viruses

        - Sparse Infector Viruses
        - Companion/Camouflage Viruses
        - Shell Viruses
        - File Extension Viruses
        - Add-on and Intrusive Viruses
        - Transient and Terminate and Stay Resident Viruses
    - Writing a Simple Virus Program
        - Sam’s Virus Generator and JPS Virus Maker
        - Andreinick05’s Batch Virus Maker and DeadLine’s Virus Maker
        - Sonic Bat – Batch File Virus Creator and Poison Virus Maker
    - Computer Worms
        - How Is a Worm Different from a Virus?
        - Computer Worms: Ghost Eye Worm
        - Worm Maker: Internet Worm Maker Thing
- Malware Reverse Engineering
    - What is Sheep Dip Computer?
    - Anti-Virus Sensor Systems
    - Malware Analysis Procedure: Preparing Testbed
    - Malware Analysis Procedure
    - 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
    - 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
    - Anti-virus Tools
- Penetration Testing
    - Pen Testing for Trojans and Backdoors
    - Penetration Testing for Virus

7. Sniffing

- Sniffing Concepts
    - Network Sniffing and Threats
    - How a Sniffer Works
    - Types of Sniffing
        - Passive Sniffing
        - Active Sniffing
    - How an Attacker Hacks the Network Using Sniffers
    - Protocols Vulnerable to Sniffing
    - Sniffing in the Data Link Layer of the OSI Model
    - Hardware Protocol Analyzer
    - Hardware Protocol Analyzers
    - SPAN Port
    - Wiretapping

- Lawful Interception
- Wiretapping Case Study: PRISM

- MAC Attacks
  - MAC Address/CAM Table
  - How CAM Works
  - What Happens When CAM Table Is Full?
  - MAC Flooding
  - Mac Flooding Switches with macof
  - Switch Port Stealing
  - How to Defend against MAC Attacks
- DHCP Attacks
  - How DHCP Works
  - DHCP Request/Reply Messages
  - IPv4 DHCP Packet Format
  - DHCP Starvation Attack
  - DHCP Starvation Attack Tools
  - Rogue DHCP Server Attack
  - How to Defend Against DHCP Starvation and Rogue Server Attack
- ARP Poisoning
  - What Is Address Resolution Protocol (ARP)?
  - ARP Spoofing Attack
  - How Does ARP Spoofing Work
  - Threats of ARP Poisoning
  - ARP Poisoning Tool
    - Cain & Abel and WinArpAttacker
    - Ufasoft Snif
  - How to Defend Against ARP Poisoning

    - Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
    - ARP Spoofing Detection: XArp
- Spoofing Attack
    - MAC Spoofing/Duplicating
    - MAC Spoofing Technique: Windows
    - MAC Spoofing Tool: SMAC
    - IRDP Spoofing
    - How to Defend Against MAC Spoofing
- DNS Poisoning
    - DNS Poisoning Techniques
    - Intranet DNS Spoofing
    - Internet DNS Spoofing
    - Proxy Server DNS Poisoning
    - DNS Cache Poisoning
    - How to Defend Against DNS Spoofing
- Sniffing Tools
- Sniffing Tool: Wireshark
- Follow TCP Stream in Wireshark
- Display Filters in Wireshark
- Additional Wireshark Filters
- Sniffing Tool
        - SteelCentral Packet Analyzer
        - 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
- Counter measures
    - 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

8. Social Engineering

- Social Engineering Concepts
    - What is Social Engineering?
    - Behaviors Vulnerable to Attacks
    - Factors that Make Companies Vulnerable to Attacks
    - Why Is Social Engineering Effective?
    - Warning Signs of an Attack
    - Phases in a Social Engineering Attack

- Social Engineering Techniques
  - Types of Social Engineering
    - Human-based Social Engineering
    - Impersonation
      - Impersonation Scenario
        - Over-Helpfulness of Help Desk
        - Third-party Authorization
        - Tech Support
        - Internal Employee/Client/Vendor
        - Repairman
        - Trusted Authority Figure
    - Eavesdropping and Shoulder Surfing
    - Dumpster Diving
    - Reverse Social Engineering, Piggybacking, and Tailgating
  - Watch these Movies
  - Watch this Movie
  - Computer-based Social Engineering
    - Phishing
    - Spear Phishing
  - Mobile-based Social Engineering
    - Publishing Malicious Apps
    - Repackaging Legitimate Apps
    - Fake Security Applications
    - Using SMS
  - Insider Attack
  - Disgruntled Employee
  - Preventing Insider Threats

- Common Social Engineering Targets and Defense Strategies
- Impersonation on Social Networking Sites
  - Social Engineering Through Impersonation on Social Networking Sites
  - Social Engineering on Facebook
  - Social Engineering on LinkedIn and Twitter
  - Risks of Social Networking to Corporate Networks
- Identity Theft
  - Identity Theft Statistics
  - Identify Theft
  - How to Steal an Identity
    - STEP 1
    - STEP 2
    - Comparison
    - STEP 3
  - Real Steven Gets Huge Credit Card Statement
  - Identity Theft – Serious Problem
- Social Engineering Countermeasures
  - How to Detect Phishing Emails
  - Anti-Phishing Toolbar
    - Netcraft
    - PhishTank
  - Identity Theft Countermeasures
- Penetration Testing
  - Social Engineering Pen Testing
    - Using Emails
    - Using Phone
    - In Person

- Social Engineering Toolkit (SET)

9. Denial-of-Service

- DoS/DDoS Concepts
  - DDoS Attack Trends
  - What is a Denial of Service Attack?
  - What Are Distributed Denial of Service Attacks?
  - How Distributed Denial of Service Attacks Work
- DoS/DDoS Attack Techniques
  - Basic Categories of DoS/DDoS Attack Vectors
  - DoS/DDoS Attack Techniques
    - Bandwidth Attacks
    - Service Request Floods
    - SYN Attack
    - SYN Flooding
    - ICMP Flood Attack
    - Peer-to-Peer Attacks
    - Permanent Denial-of-Service Attack
    - Application Level Flood Attacks
    - Distributed Reflection Denial of Service (DRDoS)
- Botnets
  - Organized Cyber Crime: Organizational Chart
  - Botnet
  - A Typical Botnet Setup
  - Botnet Ecosystem

    - Scanning Methods for Finding Vulnerable Machines
    - How Malicious Code Propagates?
    - Botnet Trojan
        - Blackshades NET
        - Cythosia Botnet and Andromeda Bot
        - PlugBot
- DDoS Case Study
    - DDoS Attack
    - Hackers Advertise Links to Download Botnet
- DoS/DDoS Attack Tools
    - Pandora DDoS Bot Toolkit
    - Dereil and HOIC
    - DoS HTTP and BanglaDos
    - DoS and DDoS Attack Tools
    - DoS and DDoS Attack Tool for Mobile
        - AnDOSid
        - Low Orbit Ion Cannon (LOIC)
- Counter-measures
    - Detection Techniques
    - Activity Profiling
    - Wavelet Analysis
    - Sequential Change-Point Detection
    - DoS/DDoS Countermeasure Strategies
    - DDoS Attack Countermeasures
        - Protect Secondary Victims
        - Detect and Neutralize Handlers
        - Detect Potential Attacks

        - Deflect Attacks
        - Mitigate Attacks
    - 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
- DoS/DDoS Attack Penetration Testing

10. Session Hijacking

- Attack Techniques 2015
- Session Hijacking Concepts
    - What is Session Hijacking?
    - Why Session Hijacking is Successful?
    - Session Hijacking Process
    - Packet Analysis of a Local Session Hijack
    - Types of Session Hijacking
    - Session Hijacking in OSI Model
    - Spoofing vs. Hijacking
- Application Level Session Hijacking
    - Compromising Session IDs using Sniffing
    - Compromising Session IDs by Predicting Session Token

        - How to Predict a Session Token
    - Compromising Session IDs Using Man-in-the-Middle Attack
    - Compromising Session IDs Using 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: Cross-site Script 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 Fixation
        - Session Fixation Attack
    - Session Hijacking Using Proxy Servers
- Network-level Session Hijacking
    - The 3-Way Handshake
    - TCP/IP Hijacking
        - TCP/IP Hijacking Process
    - IP Spoofing: Source Routed Packets
    - RST Hijacking
    - Blind Hijacking
    - MiTM Attack Using Forged ICMP and ARP Spoofing
    - UDP Hijacking
- Session Hijacking Tools
    - Session Hijacking Tool
        - Zaproxy
        - Burp Suite and JHijack
    - Session Hijacking Tools

- Session Hijacking Tools for Mobile: DroidSheep and DroidSniff

- Countermeasures
  - Session Hijacking Detection Methods
  - Protecting against Session Hijacking
  - Methods to Prevent Session Hijacking
    - To be Followed by Web Developers
    - To be Followed by Web Users
  - Approaches Vulnerable to Session Hijacking and their Preventative Solutions
  - IPSec

Join in Ethical Hacking Training in Bangalore providing by Tek Classes to gain extreme knowledge in your favorite subject.

Contact Us: +91-7411642061