

Course Outline Version 5

Module 1: Introduction to Ethical Hacking

- Why Security?
- Essential Terminologies
- Elements of Security
- The Security, Functionality, and Ease of Use Triangle
- What Does a Malicious Hacker Do?
 - Reconnaissance
 - Scanning
 - Gaining access
 - Maintaining access
 - Covering Tracks
- Types of Hacker Attacks
 - Operating System attacks
 - Application-level attacks
 - Shrink Wrap code attacks
 - Misconfiguration attacks
- Hacktivism
- Hacker Classes
- Hacker Classes and Ethical Hacking
- What Do Ethical Hackers Do?
- Can Hacking be Ethical?
- How to Become an Ethical Hacker?
- Skill Profile of an Ethical Hacker
- What is Vulnerability Research?
- Why Hackers Need Vulnerability Research?
- Vulnerability Research Tools
- Vulnerability Research Websites
- How to Conduct Ethical Hacking?
- Approaches to Ethical Hacking
- Ethical Hacking Testing
- Ethical Hacking Deliverables
- Computer Crimes and Implications
- Legal Perspective
 - U.S. Federal Law

- Japan's Cyber Laws
- United Kingdom's Cyber Laws
- Australia's Cyber Laws
- Germany's Cyber Laws
- Singapore's Cyber Laws

Module 2: Footprinting

- Revisiting Reconnaissance
- Defining of Footprinting
- Information Gathering Methodology
- Unearthing Initial Information
- Finding a Company's URL
- Internal URL
- Extracting Archive Of a Website
- Google Search for Company's Info.
- People Search
- Footprinting Through Job Sites
- Passive Information Gathering
- Competitive Intelligence Gathering
- Why Do You Need Competitive Intelligence?
- Companies Providing Competitive Intelligence Services
- Competitive Intelligence
 - When Did This Company Begin?
 - How Did It Develop?
 - What Are This Company's Plans?
 - What Does Expert Opinion Say About The Company?
 - Who Are The Leading Competitors?
- Public and Private Websites
- Tools
 - DNS Enumerator
 - SpiderFoot
 - Sensepost Footprint Tools
 - BiLE.pl
 - BiLE-weigh.pl
 - tld-expand.pl
 - vet-IPrange.pl

- qtrace.pl
 - vet-mx.pl
 - jarf-rev
 - jarf-dnsbrute
- Wikito Footprinting Tool
- Web Data Extractor Tool
- Whois
- Nslookup
- Necrosoft
- ARIN
- Traceroute
- Neo Trace
- GEOSpider
- Geowhere
- GoogleEarth
- VisualRoute Trace
- Kartoo Search Engine
- Touchgraph Visual Browser
- SmartWhois
- VisualRoute Mail Tracker
- eMailTrackerPro
- Read Notify
- HTTrack Web Site Copier
- Web Ripper
- robots.txt
- Website watcher
- E-mail Spider
- Power E-mail Collector Tool
- Steps to Perform Footprinting

Module 3: Scanning

- Definition of Scanning
- Types of Scanning
 - Port Scanning
 - Network Scanning

- Vulnerability Scanning
- Objectives of Scanning
- CEH Scanning Methodology
 - Check for live systems
 - ICMP Scanning
 - Angry IP
 - HPING2
 - Ping Sweep
 - Firewalk
 - Check for open ports
 - Nmap
 - TCP Communication Flags
 - Three Way Handshake
 - SYN Stealth / Half Open Scan
 - Stealth Scan
 - Xmas Scan
 - FIN Scan
 - NULL Scan
 - IDLE Scan
 - ICMP Echo Scanning/List Scan
 - TCP Connect / Full Open Scan
 - FTP Bounce Scan
 - FTP Bounce Attack
 - SYN/FIN Scanning Using IP Fragments
 - UDP Scanning
 - Reverse Ident Scanning
 - RPC Scan
 - Window Scan
 - Blaster Scan
 - PortScan Plus, Strobe
 - IPsecScan
 - NetScan Tools Pro
 - WUPS – UDP Scanner
 - SuperScan
 - IPScanner

- MegaPing
- Global Network Inventory Scanner
- Net Tools Suite Pack
- FloppyScan
- War Dialer Technique
- Why War Dialing?
- Wardialing
- PhoneSweep
- THC Scan
- SandTrap Tool
- Banner grabbing/OS Fingerprinting
 - OS Fingerprinting
 - Active Stack Fingerprinting
 - Passive Fingerprinting
 - Active Banner Grabbing Using Telnet
 - GET REQUESTS
 - p0f – Banner Grabbing Tool
 - p0f for Windows
 - Httprint Banner Grabbing Tool
 - Active Stack Fingerprinting
 - ◆ XPROBE2
 - ◆ RING V2
 - Netcraft
 - Disabling or Changing Banner
 - ◆ Apache Server
 - ◆ IIS Server
 - IIS Lockdown Tool
 - ServerMask
 - Hiding File Extensions
 - PageXchanger 2.0
- Identify Service
- Scan for Vulnerability
 - Bidiblah Automated Scanner
 - Qualys Web-based Scanner
 - SAINT

- ISS Security Scanner
- Nessus
- GFI LANGuard
- SATAN (Security Administrator's Tool for Analyzing Networks)
- Retina
- NIKTO
- SAFEsuite Internet Scanner
- IdentTCPScan
- Draw network diagrams of Vulnerable hosts
 - Cheops
 - FriendlyPinger
- Prepare proxies
 - Proxy Servers
 - Use of Proxies for Attack
 - SocksChain
 - Proxy Workbench
 - ProxyManager Tool
 - Super Proxy Helper Tool
 - Happy Browser Tool (Proxy-based)
 - MultiProxy
 - TOR Proxy Chaining Software
- Anonymizers
 - Primedia Anonymizer
 - Browzar
 - Torpark Browser
 - G-Zapper - Google Cookies
- SSL Proxy Tool
- HTTP Tunneling Techniques
- HTTPort
- Spoofing IP Address - Source Routing
- Detecting IP Spoofing
- Despoof Tool
- Scanning Countermeasures
- Tool: SentryPC

Module 4: Enumeration

- Overview of System Hacking Cycle
- What is Enumeration?
- Techniques for Enumeration
- Netbios Null Sessions
- Tool
 - DumpSec
 - NetBIOS Enumeration Using Netview
 - Nbtstat
 - SuperScan4
 - Enum
 - sid2user
 - user2sid
 - GetAcct
- Null Session Countermeasures
- PSTools
 - PsExec
 - PsFile
 - PsGetSid
 - PsKill
 - PsInfo
 - PsList
 - PsLoggedOn
 - PsLogList
 - PsPasswd
 - PsService
 - PsShutdown
 - PsSuspend
 - PsUptime
- SNMP Enumeration
- Management Information Base
- Tools
 - SNMPutil
 - Solarwinds
 - SNScan V1.05
 - Getif SNMP MIB Browser

- UNIX Enumeration
- SNMP UNIX Enumeration
- SNMP Enumeration Countermeasures
- Tools
 - Winfingerprint
 - Windows Active Directory Attack Tool
 - IP Tools Scanner
 - Enumerate Systems Using Default Passwords
- Steps to Perform Enumeration

Module 5: System Hacking

- Cracking Passwords
 - Password Types
 - Types of Password Attacks
 - Passive Online – Wire Sniffing
 - Passive Online Attacks
 - Active Online – Password Guessing
 - Offline Attacks
 - Dictionary Attack
 - Hybrid Attack
 - Brute-force Attack
 - Pre-computed Hashes
 - Non-Technical Attacks
 - Password Mitigation
 - Permanent Account Lockout – Employee Privilege Abuse
 - Administrator Password Guessing
 - Manual Password Cracking Algorithm
 - Automatic Password Cracking Algorithm
 - Performing Automated Password Guessing
 - Tools
 - NAT
 - Smbbf (SMB Passive Brute Force Tool)
 - SmbCrack Tool
 - Legion
 - LOphtcrack

- Microsoft Authentication - LM, NTLMv1, and NTLMv2
- Kerberos Authentication
- What is LAN Manager Hash?
- Salting
- Tools
 - PWdump2 and Pwdump3
 - Rainbowcrack
 - KerbCrack
 - NBTDeputy
 - NetBIOS DoS Attack
 - John the Ripper
- Password Sniffing
- How to Sniff SMB Credentials?
- Sniffing Hashes Using LophtCrack
- Tools
 - ScoopLM
 - SMB Replay Attacks
 - Replay Attack Tool: SMBProxy
 - Hacking Tool: SMB Grind
 - Hacking Tool: SMBDie
- SMBRelay Weaknesses & Countermeasures
- Password Cracking Countermeasures
- LM Hash Backward Compatibility
- How to Disable LM HASH?
- Tools
 - Password Brute-Force Estimate Tool
 - Syskey Utility
- Escalating Privileges
 - Privilege Escalation
 - Cracking NT/2000 Passwords
 - Active@ Password Changer
 - Change Recovery Console Password
 - Privilege Escalation Tool: x.exe
- Executing applications
 - Tool:

- Psexec
- Remoexec
- Alchemy Remote Executor
- Keystroke Loggers
- E-mail Keylogger
- Spytector FTP Keylogger
- IKS Software Keylogger
- Ghost Keylogger
- Hardware Keylogger
- Keyboard Keylogger: KeyGhost Security Keyboard
- USB Keylogger:KeyGhost USB Keylogger
- What is Spyware?
- Tools
 - Spyware: Spector
 - Remote Spy
 - eBlaster
 - Stealth Voice Recorder
 - Stealth Keylogger
 - Stealth Website Logger
 - Digi-Watcher Video Surveillance
 - Desktop Spy Screen Capture Program
 - Telephone Spy
 - Print Monitor Spy Tool
 - Perfect Keylogger
 - Stealth Email Redirector
 - Spy Software: Wiretap Professional
 - Spy Software: FlexiSpy
 - PC PhoneHome
- Keylogger Countermeasures
- Anti-Keylogger
- PrivacyKeyboard
- Hiding Files
 - Hacking Tool: RootKit
 - Why Rootkits?
 - Rootkits in Linux

- Detecting Rootkits
- Rootkit Detection Tools
 - BlackLight from F-Secure Corp
 - RootkitRevealer from Sysinternals
 - Malicious Software Removal Tool from Microsoft Corp
- Sony Rootkit Case Study
- Planting the NT/2000 Rootkit
- Rootkits
 - Fu
 - AFX Rootkit 2005
 - Nuclear
 - Vanquish
- Rootkit Countermeasures
- Patchfinder2.0
- RootkitRevealer
- Creating Alternate Data Streams
- How to Create NTFS Streams?
- NTFS Stream Manipulation
- NTFS Streams Countermeasures
- NTFS Stream Detectors
 - ADS Spy
 - ADS Tools
- What is Steganography?
- Tools
 - Merge Streams
 - Invisible Folders
 - Invisible Secrets 4
 - Image Hide
 - Stealth Files
 - Steganography
 - Masker Steganography Tool
 - Hermetic Stego
 - DCP – Hide an Operating System
 - Camera/Shy
 - Mp3Stego

- Snow.exe
 - Video Steganography
 - Steganography Detection
 - SIDS (Stego intrusion detection system)
 - High-Level View
 - Tool : dskprobe.exe
- Covering tracks
 - Disabling Auditing
 - Clearing the Event Log
 - Tools
 - elsave.exe
 - Winzapper
 - Evidence Eliminator
 - Traceless
 - Tracks Eraser Pro
 - ZeroTracks

Module 6: Trojans and Backdoors

- Introduction
- Effect on Business
- What is a Trojan?
- Overt and Covert Channels
- Working of Trojans
- Different Types of Trojans
- What Do Trojan Creators Look For?
- Different Ways a Trojan Can Get into a System
- Indications of a Trojan Attack
- Ports Used by Trojans
- How to Determine which Ports are “Listening”?
- Classic Trojans Found in the Wild
- Trojans
 - Tini
 - iCmd
 - NetBus
 - Netcat

- Beast
 - MoSucker
 - Proxy Server
 - SARS Trojan Notification
- Wrappers
- Wrapper Covert Program
- Wrapping Tools
 - One file EXE Maker
 - Yet Another Binder
 - Pretator Wrapper
- Packaging Tool: WordPad
- RemoteByMail
- Tool: Icon Plus
- Defacing Application: Restorator
- HTTP Trojans
- Trojan Attack through Http
- HTTP Trojan (HTTP RAT)
- Shttpd Trojan - HTTP Server
- Reverse Connecting Trojans
- Nuclear RAT Trojan (Reverse Connecting)
- Tool: BadLuck Destructive Trojan
- ICMP Tunneling
- ScreenSaver Password Hack Tool – Dummylock
- Trojan
 - Phatbot
 - Amitis
 - Senna Spy
 - QAZ
 - Back Orifice
 - Back Orifice 2000
 - SubSeven
 - CyberSpy Telnet Trojan
 - Subroot Telnet Trojan
 - Let Me Rule! 2.0 BETA 9
 - Donald Dick
 - RECUB
- Hacking Tool: Loki

- Atelier Web Remote Commander
- Trojan Horse Construction Kit
- How to Detect Trojans?
- Tools
 - Netstat
 - fPort
 - TCPView
 - CurrPorts
 - Process Viewer
 - What's on My Computer
 - Super System Helper
- Delete Suspicious Device Drivers
- Inzider - Tracks Processes and Ports
- Tools
 - What's Running?
 - MSConfig
 - Registry-What's Running
 - Autoruns
 - Hijack This (System Checker)
 - Startup List
- Anti-Trojan Software
- Evading Anti-Virus Techniques
- Evading Anti-Trojan/Anti-Virus Using Stealth Tools v2.0
- Backdoor Countermeasures
- Tools
 - Tripwire
 - System File Verification
 - MD5sum.exe
 - Microsoft Windows Defender
- How to Avoid a Trojan Infection?

Module 7: Sniffers

- Definition of Sniffing
- Protocols Vulnerable to Sniffing
 - Tool: Network View – Scans the Network for Devices
 - The Dude Sniffer

- Ethereal
 - tcpdump
- Types of Sniffing
 - Passive Sniffing
 - Active sniffing
- ARP - What is Address Resolution Protocol?
- ARP Spoofing Attack
 - How Does ARP Spoofing Work?
 - ARP Poisoning
 - Mac Duplicating Attack
- Tools for ARP Spoofing
 - Arpspoof (Linux-based tool)
 - Ettercap (Linux and Windows)
- MAC Flooding
- Tools for MAC Flooding
 - Macof (Linux-based tool)
 - Etherflood (Linux and Windows)
- Threats of ARP Poisoning
- IRS – ARP Attack Tool
- ARPWorks Tool
- Tool: Nemesis
- Sniffer Hacking Tools (dsniff package)
 - Arpspoof
 - Dnsspoof
 - Dsniff
 - Filesnarf
 - Mailsnarf
 - Msgsnarf
 - Tcpcat
 - Tcpcat
 - Tcpcat
 - Urlnarf
 - Websploit
 - Webmitm
- DNS Poisoning Techniques
- Types of DNS Poisoning:
 - Intranet DNS Spoofing (Local network)
 - Internet DNS Spoofing (Remote network)

- Proxy Server DNS Poisoning
- DNS Cache Poisoning
- Interactive TCP Relay
- Sniffers
 - HTTP Sniffer: EffeTech
 - Ace Password Sniffer
 - MSN Sniffer
 - SmartSniff
 - Session Capture Sniffer: NetWitness
 - Session Capture Sniffer: NWreader
 - Cain and Abel
 - Packet Crafter Craft Custom TCP/IP Packets
 - SMAC
 - NetSetMan Tool
 - Raw Sniffing Tools
 - Sniffit
 - Aldebaran
 - Hunt
 - NGSSniff
 - Ntop
 - Pf
 - IPTraf
 - EtherApe
 - Netfilter
 - Network Probe
 - Maa Tec Network Analyzer
- Tools
 - Snort
 - Windump
 - Etherpeek
 - Mac Changer
 - Iris
 - NetIntercept
 - WinDNSSpoof
- How to Detect Sniffing?
- AntiSniff Tool
- ArpWatch Tool

- Countermeasures

Module 8: Denial of Service

- What are Denial of Service Attacks?
- Goal of DoS
- Impact and the Modes of Attack
- Types of Attacks
 - DoS attack
 - DDos attack
- DoS Attack Classification
 - Smurf
 - Buffer Overflow Attack
 - Ping of death
 - Teardrop
 - SYN Attack
- DoS Attack Tools
 - Jolt2
 - Bubonic.c
 - Land and LaTierra
 - Targa
 - Blast20
 - Nemesy
 - Panther2
 - Crazy Pinger
 - Some Trouble
 - UDP Flood
 - FSMax
- Botnets
- Uses of botnets
- Types of Bots
 - Agobot/Phatbot/Forbot/XtremBot
 - SDBot/RBot/UrBot/UrXBot
 - mIRC-based Bots - GT-Bots
- Tool: Nuclear Bot
- What is DDoS Attack?
- Characteristics of DDoS Attacks

- DDOS Unstoppable
- Agent Handler Model
- DDoS IRC based Model
- DDoS Attack Taxonomy
- Amplification Attack
- Reflective DNS Attacks
- Reflective DNS Attacks Tool: ihateperl.pl
- DDoS Tools
 - Trin00
 - Tribe Flood Network (TFN)
 - TFN2K
 - Stacheldraht
 - Shaft
 - Trinity
 - Knight
 - Mstream
 - Kaiten
- Worms
- Slammer Worm
- Spread of Slammer Worm – 30 min
- MyDoom.B
- SCO Against MyDoom Worm
- How to Conduct a DDoS Attack
- The Reflected DoS Attacks
- Reflection of the Exploit
- Countermeasures for Reflected DoS
- DDoS Countermeasures
- Taxonomy of DDoS Countermeasures
- Preventing Secondary Victims
- Detect and Neutralize Handlers
- Detect Potential Attacks
- Mitigate or Stop the Effects of DDoS Attacks
- Deflect Attacks
- Post-attack Forensics
- Packet Traceback

Module 9: Social Engineering

- What is Social Engineering?
- Human Weakness
- “Rebecca” and “Jessica”
- Office Workers
- Types of Social Engineering
 - Human-based
 - Computer-based
- Preventing Insider Threat
- Common Targets of Social Engineering
- Factors that make Companies Vulnerable to Attacks
- Why is Social Engineering Effective?
- Warning Signs of an Attack
- Tool : Netcraft Anti-Phishing Toolbar
- Phases in a Social Engineering Attack
- Behaviors Vulnerable to Attacks
- Impact on the Organization
- Countermeasures
- Policies and Procedures
- Security Policies - Checklist
- Phishing Attacks and Identity Theft
- What is Phishing?
- Phishing Report
- Attacks
- Hidden Frames
- URL Obfuscation
- URL Encoding Techniques
- IP Address to Base 10 Formula
- Karen’s URL Discombobulator
- HTML Image Mapping Techniques
- Fake Browser Address Bars
- Fake Toolbars
- Fake Status Bar
- DNS Cache Poisoning Attack

Module 10: Session Hijacking

- What is Session Hijacking?
- Spoofing vs. Hijacking
- Steps in Session Hijacking
- Types of Session Hijacking
 - Active
 - Passive
- The 3-Way Handshake
- TCP Concepts 3-Way Handshake
- Sequence Number Prediction
- TCP/IP Hijacking
- RST Hijacking
- RST Hijacking Tool: `hijack_rst.sh`
- Programs that Perform Session Hijacking
- Hacking Tools
 - Juggernaut
 - Hunt
 - TTY Watcher
 - IP Watcher
 - T-Sight
 - Paros HTTP Session
- Remote TCP Session Reset Utility
- Dangers Posed by Hijacking
- Protecting against Session Hijacking
- Countermeasure: IP Security
- IP-SEC

Module 11: Hacking Web Servers

- How Web Servers Work
- How are Web Servers Compromised?
- How are Web Servers Defaced?
- Apache Vulnerability
- Attacks Against IIS
 - IIS Components
 - IIS Directory Traversal (Unicode) Attack
- Unicode
 - Unicode Directory Traversal Vulnerability

- Hacking Tool: IISexploit.exe
- Msw3prt IPP Vulnerability
- WebDAV / ntdll.dll Vulnerability
- RPC DCOM Vulnerability
- ASN Exploits
- ASP Trojan (cmd.asp)
- IIS Logs
- Network Tool: Log Analyzer
- Hacking Tool: CleanIISLog
- Unspecified Executable Path Vulnerability
- Metasploit Framework
- Immunity CANVAS Professional
- Core Impact
- Hotfixes and Patches
- What is Patch Management?
- Solution: UpdateExpert
- Patch Management Tool
 - Qfecheck
 - HFNetChk
- cacls.exe Utility
- Vulnerability Scanners
- Online Vulnerability Search Engine
- Network Tools
 - Whisker
 - N-Stealth HTTP Vulnerability Scanner
- Hacking Tool: WebInspect
- Network Tool: Shadow Security Scanner
- SecureIIS
- Countermeasures
- File System Traversal Countermeasures
- Increasing Web Server Security
- Web Server Protection Checklist

Module 12: Web Application Vulnerabilities

- Web Application Setup
- Web Application Hacking

- Anatomy of an Attack
- Web Application Threats
- Cross-Site Scripting/XSS Flaws
 - Countermeasures
- SQL Injection
- Command Injection Flaws
 - Countermeasures
- Cookie/Session Poisoning
 - Countermeasures
- Parameter/Form Tampering
- Buffer Overflow
 - Countermeasures
- Directory Traversal/Forceful Browsing
 - Countermeasures
- Cryptographic Interception
- Cookie Snooping
- Authentication Hijacking
 - Countermeasures
- Log Tampering
- Error Message Interception
- Attack Obfuscation
- Platform Exploits
- DMZ Protocol Attacks
 - Countermeasures
- Security Management Exploits
- Web Services Attacks
- Zero-Day Attacks
- Network Access Attacks
- TCP Fragmentation
- Hacking Tools
 - Instant Source
 - Wget
 - WebSleuth
 - BlackWidow
 - WindowBomb
 - Burp
 - cURL

- dotDefender
- Google Hacking
- Acunetix Web Scanner
- AppScan – Web Application Scanner
- AccessDiver

Module 13: Web-based Password Cracking Techniques

- Definition of Authentication
- Authentication Mechanisms
 - HTTP Authentication
 - Basic Authentication
 - Digest Authentication
 - Integrated Windows (NTLM) Authentication
 - Negotiate Authentication
 - Certificate-based Authentication
 - Forms-based Authentication
 - RSA Secure Token
 - Biometrics
 - Face recognition
 - Iris scanning
 - Retina scanning
 - Fingerprinting
 - Hand geometry
 - Voice recognition
- How to Select a Good Password?
- Things to Avoid in Passwords
- Changing Your Password
- Protecting Your Password
- How Hackers get hold of Passwords?
- Windows XP: Remove Saved Passwords
- Microsoft Password Checker
- What is a Password Cracker?
- Modus Operandi of an Attacker Using Password Cracker
- How does a Password Cracker Work?
- Classification of Attacks

- Password Guessing
- Query String
- Cookies
- Dictionary Maker
- Available Password Crackers
 - LOphtcrack
 - John The Ripper
 - Brutus
- Hacking Tools
 - Obiwan
 - Authforce
 - Hydra
 - Cain And Abel
 - RAR
 - Gammalog
 - WebCracker
 - Munga Bunga
 - PassList
 - SnadBoy
 - WinSSLMiM
 - ReadCookies.html
 - Wireless WEP Key Password Spy
 - RockXP
 - WinSSLMiM
 - Password Spectator
- Countermeasures

Module 14: SQL Injection

- Introducing SQL injection
- Exploiting Web Applications
- SQL Injection Steps
 - What Should You Look For?
 - What If It Doesn't Take Input?
 - OLE DB Errors
 - Input Validation Attack
- SQL Injection Techniques

- How to Test for SQL Injection Vulnerability?
- How does it Work?
- Executing Operating System Commands
- Getting Output of SQL Query
- Getting Data from the Database Using ODBC Error Message
- How to Mine all Column Names of a Table?
- How to Retrieve any Data?
- How to Update/Insert Data into Database?
- Automated SQL Injection Tool
 - AutoMagic SQL
 - Absinthe
- SQL Injection in Oracle
- SQL Injection in MySql Database
- Attack against SQL Servers
- SQL Server Resolution Service (SSRS)
- Osql L- Probing
- SQL Injection Automated Tools
 - SQLDict
 - SqlExec
 - SQLbf
 - SQLSmack
 - SQL2.exe
- SQL Injection Countermeasures
- Preventing SQL Injection Attacks
- SQL Injection Blocking Tool: SQLBlock
- Acunetix Web Vulnerability Scanner

Module 15: Hacking Wireless Networks

- Introduction to Wireless Networking
- Wired Network vs. Wireless Network
- Effects of Wireless Attacks on Business
- Types of Wireless Networks
- Advantages and Disadvantages of a Wireless Network
- Wireless Standards
 - 802.11a
 - 802.11b – “WiFi”

- 802.11g
- 802.11i
- 802.11n
- Related Technology and Carrier Networks
- Antennas
- Cantenna
- Wireless Access Points
- SSID
- Beacon Frames
- Is the SSID a Secret?
- Setting Up a WLAN
- Detecting a Wireless Network
- How to Access a WLAN
- Terminologies
- Authentication and Association
- Authentication Modes
- Authentication and (Dis)Association Attacks
- Rogue Access Points
- Tools to Generate Rogue Access Points: Fake AP
- Tools to Detect Rogue Access Points: Netstumbler
- Tools to Detect Rogue Access Points: MiniStumbler
- Wired Equivalent Privacy (WEP)
- What is WPA?
- WPA Vulnerabilities
- WEP, WPA, and WPA2
- Steps for Hacking Wireless Networks
 - Step 1: Find networks to attack
 - Step 2: Choose the network to attack
 - Step 3: Analyze the network
 - Step 4: Crack the WEP key
 - Step 5: Sniff the network
- Cracking WEP
- Weak Keys (a.k.a. Weak IVs)
- Problems with WEP's Key Stream and Reuse
- Automated WEP Crackers
- Pad-Collection Attacks
- XOR Encryption

- Stream Cipher
- WEP Tools
 - Aircrack
 - AirSnort
 - WEPCrack
 - WepLab
- Temporal Key Integrity Protocol (TKIP)
- LEAP: The Lightweight Extensible Authentication Protocol
- LEAP Attacks
- MAC Sniffing and AP Spoofing
- Tool to Detect MAC Address Spoofing: Wellenreiter V2
- Man-in-the-Middle Attack (MITM)
- Denial-of-Service Attacks
- Dos Attack Tool: Fatajack
- Phone Jammers
- Scanning Tools
 - Redfang 2.5
 - Kismet
 - THC-WarDrive
 - PrismStumbler
 - MacStumbler
 - Mognet
 - WaveStumbler
 - StumbVerter
 - Netchaser V1.0 for Palm Tops
 - AP Scanner
 - SSID Sniff
 - Wavemon
 - Wireless Security Auditor (WSA)
 - AirTraf
 - Wifi Finder
 - AirMagnet
- Sniffing Tools
 - AiroPeek
 - NAI Wireless Sniffer
 - Ethereal
 - Aerosol v0.65

- vxSniffer
- EtherPEG
- DriftNet
- AirMagnet
- WinDump
- ssidsniff
- Multiuse Tool: THC-RUT
- PCR-PRO-1k Hardware Scanner
- Tools
 - WinPcap
 - AirPcap
- Securing Wireless Networks
- Auditing Tool: BSD-Airtools
- AirDefense Guard
- WIDZ: Wireless Intrusion Detection System
- Radius: Used as Additional Layer in Security
- Google Secure Access

Module 16: Virus and Worms

- Introduction to Virus
- Virus History
- Characteristics of a Virus
- Working of Virus
 - Infection Phase
 - Attack Phase
- Why People create computer viruses?
- Symptoms of Virus-Like Attack
- Virus Hoaxes
- Chain Letters
- How is a Worm different from a Virus?
- Indications of Virus Attack
- Hardware Threats
- Software Threats
- Virus Damage
- Modes of Virus Infection
- Stages of Virus Life

- Virus Classification
- How does a Virus Infect?
- Storage Patterns of a Virus
- System Sector Viruses
- Stealth Virus
- Bootable CD-ROM Virus
- Self-Modification
- Encryption with a Variable Key
- Polymorphic Code
- Viruses
 - Metamorphic Virus
 - Cavity Virus
 - Sparse Infector Virus
 - Companion Virus
 - File Extension Virus
 - I Love You Virus
 - Melissa Virus
- Famous Virus/Worms – JS.Spth
- Klez Virus Analysis
- Writing a Simple Virus Program
- Virus Construction Kits
- Virus Detection Methods
- Virus Incident Response
- What is Sheep Dip?
- Sheep Dip Computer
- Virus Analysis - IDA Pro Tool
- Prevention is Better than Cure
- Latest Viruses
- Top 10 Viruses- 2006
- Anti-Virus Software
 - AVG Free Edition
 - Norton Antivirus
 - McAfee
- Socketshield
- Popular Anti-Virus Packages
- Virus Databases

Module 17: Physical Security

- Security Statistics
- Physical Security Breach Incidents
- Understanding Physical Security
- What Is the Need for Physical Security?
- Who Is Accountable for Physical Security?
- Factors Affecting Physical Security
- Physical Security Checklist
 - Company surroundings
 - Premises
 - Reception
 - Server
 - Workstation area
 - Wireless access points
 - Other equipment, such as fax, and removable media
 - Access control
 - Biometric Devices
 - Smart Cards
 - Security Token
 - Computer equipment maintenance
 - Wiretapping
 - Remote access
 - Locks
- Information Security
- EPS (Electronic Physical Security)
- Wireless Security
- Laptop Theft: Security Statistics
- Laptop Theft
- Laptop Security Tools
- Laptop Tracker - XTool Computer Tracker
- Tools to Locate Stolen Laptops
- Stop's Unique, Tamper-proof Patented Plate
- Tool: TrueCrypt
- Laptop Security Countermeasures
- Mantrap
- TEMPEST

- Challenges in Ensuring Physical Security
- Spyware Technologies
- Spying Devices
- Physical Security: Lock Down USB Ports
- Tool: DeviceLock
- Blocking the Use of USB Storage Devices
- Track Stick GPS Tracking Device

Module 18: Linux Hacking

- Why Linux?
- Linux Distributions
- Linux – Basics
- Linux Live CD-ROMs
- Basic Commands of Linux
- Linux File Structure
- Linux Networking Commands
- Directories in Linux
- Compiling the Linux Kernel
- How to Install a Kernel Patch?
- Compiling Programs in Linux
- GCC Commands
- Make Install Command
- Linux Vulnerabilities
- Chrooting
- Why is Linux Hacked?
- Linux Vulnerabilities in 2005
- How to Apply Patches to Vulnerable Programs?
- Scanning Networks
- Tools
 - Nmap in Linux
 - Scanning Tool: Nessus
 - Tool: Cheops
 - Port Scan Detection Tools
- Password Cracking in Linux
- Firewall in Linux: IPTables
- Basic Linux Operating System Defense

- SARA (Security Auditor's Research Assistant)
- Linux Tool
 - Netcat
 - tcpdump
 - Snort
 - SAINT
 - Ethereal
 - Abacus Port Sentry
 - DSniff Collection
 - Hping2
 - Sniffit
 - Nemesis
 - LSOF
 - IPTraf
 - LIDS
 - Hunt
 - TCP Wrappers
- Linux Loadable Kernel Modules
- Hacking Tool: Linux Rootkits
- Rootkits
 - Knark
 - Torn
 - Tuxit
 - Adore
 - Ramen
 - Beastkit
- Rootkit Countermeasures
- Linux Tools: Application Security
- Advanced Intrusion Detection Environment (AIDE)
- Linux Tools
 - Security Testing Tools
 - Encryption
 - Log and Traffic Monitors
 - Security Auditing Tool (LSAT)
- Linux Security Countermeasures
- Steps for Hardening Linux

Module 19: Evading IDS, Firewalls, and Honeypots

- Introduction to Intrusion Detection Systems
- Terminologies
 - Intrusion Detection System (IDS)
 - IDS Placement
 - Ways to Detect an Intrusion
 - Types of Intrusion Detection Systems
 - System Integrity Verifiers (SIV)
 - Tripwire
 - Cisco Security Agent (CSA)
 - Signature Analysis
 - General Indications of Intrusion System Indications
 - General Indications of Intrusion File System Indications
 - General Indications of Intrusion Network Indications
 - Intrusion Detection Tools
 - ◆ Snort 2.x
 - Steps to Perform After an IDS Detects an Attack
 - Evading IDS Systems
 - Ways to Evade IDS
 - Tools to Evade IDS
 - IDS Evading Tool: ADMutate
 - Packet Generators
 - Firewall
 - What is a Firewall?
 - What does a Firewall do?
 - Packet Filtering
 - What can't a Firewall do?
 - How does a Firewall Work?
 - Firewall Operations
 - Hardware Firewall
 - Software Firewall
 - Types of Firewalls
 - ◆ Packet Filtering Firewall
 - ◆ IP Packet Filtering Firewall
 - ◆ Circuit-Level Gateway

- ◆ TCP Packet Filtering Firewall
 - ◆ Application-Level Firewall
 - ◆ Application Packet Filtering Firewall
 - ◆ Stateful Multilayer Inspection Firewall
- Firewall Identification
- Firewalking
- Banner Grabbing
- Breaching Firewalls
- Bypassing a Firewall Using HTTP Tunnel
- Placing Backdoors Through Firewalls
- Hiding behind a Covert Channel: LOKI
- ACK Tunneling
- Tools to Breach Firewalls
- Common Tool for Testing Firewall & IDS
 - ◆ IDS Informer
 - ◆ Evasion Gateway
 - ◆ Firewall Informer
- Honeypot
 - What is a Honeypot?
 - The HoneyNet Project
 - Types of Honeypots
 - Advantages and Disadvantages of a Honeypot
 - Where to Place a Honeypot ?
 - Honeypots
 - ◆ SPECTER
 - ◆ honeyd
 - ◆ KFSensor
 - ◆ Sebek
 - Physical and Virtual Honeypots
 - Tools to Detect Honeypots
 - What to do When Hacked?

SELF-STUDY MODULES

Buffer Overflows

- Why are Programs/Applications Vulnerable?
- Buffer Overflows

- Reasons for Buffer Overflow Attacks
- Knowledge Required to Program Buffer Overflow Exploits
- Types of Buffer Overflows
 - Stack-based Buffer Overflow
 - Understanding Assembly Language
 - Understanding Stacks
 - Shellcode
 - Heap/BSS-based Buffer Overflow
- How to Detect Buffer Overflows in a Program
- Attacking a Real Program
- NOPS
- How to Mutate a Buffer Overflow Exploit
- Defense Against Buffer Overflows
- Tool to Defend Buffer Overflow
 - Return Address Defender (RAD)
 - StackGuard
 - Immunix System
- Vulnerability Search – ICAT
- Simple Buffer Overflow in C
- Code Analysis

Cryptography

- Public-key Cryptography
- Working of Encryption
- Digital Signature
- RSA (Rivest Shamir Adleman)
- RC4, RC5, RC6, Blowfish
- Algorithms and Security
- Brute-Force Attack
- RSA Attacks
- Message Digest Functions
- One-way Hash Functions
- MD5
- SHA (Secure Hash Algorithm)
- SSL (Secure Sockets Layer)
- RC5

- What is SSH?
- SSH (Secure Shell)
- Government Access to Keys (GAK)
- RSA Challenge
- distributed.net
- Cleversafe Grid Builder
- PGP (Pretty Good Privacy)
- Code Breaking: Methodologies
- Cryptography Attacks
- Disk Encryption
- Hacking Tool
 - PGP Crack
 - Magic Lantern
 - WEPCrack
 - Cracking S/MIME Encryption Using Idle CPU Time
 - CypherCalc
 - Command Line Scriptor
 - CryptoHeaven

Penetration Testing

- Introduction to Penetration Testing
- Categories of Security Assessments
- Vulnerability Assessment
- Limitations of Vulnerability Assessment
- Types of Penetration Testing
- Risk Management
- Do-it-Yourself Testing
- Outsourcing Penetration Testing Services
- Terms of Engagement
- Project Scope
- Pentest Service Level Agreements
- Testing Points
- Testing Locations
- Automated Testing
- Manual Testing
- Using DNS Domain Name and IP Address Information

- Enumerating Information about Hosts on Publicly-Available Networks
- Testing Network-Filtering Devices
- Enumerating Devices
- Denial of Service Emulation
- Tools
 - Appscan
 - HackerShield
 - Cerberus Internet Scanner
 - Cybercop Scanner
 - FoundScan Hardware Appliances
 - Nessus
 - NetRecon
 - SAINT
 - SecureNET Pro
 - SecureScan
 - SATAN
 - SARA
 - Security Analyzer
 - STAT Analyzer
 - VigilENT
 - WebInspect
- Evaluating Different Types of Pentest Tools
- Asset Audit
- Fault Trees and Attack Trees
- GAP Analysis
- Threat
- Business Impact of Threat
- Internal Metrics Threat
- External Metrics Threat
- Calculating Relative Criticality
- Test Dependencies
- Defect Tracking Tools
 - Web-based Bug/Defect Tracking Software
 - SWB Tracker
 - Advanced Defect Tracking Web Edition
- Disk Replication Tools
 - Snapback DUP

- Daffodil Replicator
- Image MASter 4002i
- DNS Zone Transfer Testing Tools
 - DNS analyzer
 - Spam blacklist
- Network Auditing Tools
 - eTrust Audit (AUDIT LOG REPOSITORY)
 - iInventory
 - Centennial Discovery
- Trace Route Tools and Services
 - Ip Tracer 1.3
 - Trellian Trace Route
- Network Sniffing Tools
 - Sniff'em
 - PromiScan
- Denial-of-Service Emulation Tools
 - FlameThrower®
 - Mercury LoadRunner™
 - ClearSight Analyzer
- Traditional Load Testing Tools
 - WebMux
 - SilkPerformer
 - PORTENT Supreme
- System Software Assessment Tools
 - Database Scanner
 - System Scanner
 - Internet Scanner
- Operating System Protection Tools
 - Bastille Linux
 - Engarde Secure Linux
- Fingerprinting Tools
 - Foundstone
 - @Stake LC 5
- Port Scanning Tools
 - Superscan
 - Advanced Port Scanner
 - AW Security Port Scanner

- Directory and File Access Control Tools
 - Abyss Web Server for windows
 - GFI LANguard Portable Storage Control
 - Windows Security Officer - wso
- File Share Scanning Tools
 - Infiltrator Network Security Scanner
 - Encrypted FTP 3
- Password Directories
 - Passphrase Keeper 2.60
 - IISProtect
- Password Guessing Tools
 - Webmaster Password Generator
 - Internet Explorer Password Recovery Master
 - Password Recovery Toolbox
- Link Checking Tools
 - Alert Link Runner
 - Link Utility
 - LinxExplorer
- Web Testing-based Scripting Tools
 - Svoi.NET PHP Edit
 - OptiPerl
 - Blueprint Software Web Scripting Editor
- Buffer Overflow Protection Tools
 - StackGuard
 - FormatGuard
 - RaceGuard
- File Encryption Tools
 - Maxcrypt
 - Secure IT
 - Steganos
- Database Assessment Tools
 - EMS MySQL Manager
 - SQL Server Compare
 - SQL Stripes
- Keyboard Logging and Screen Reordering Tools
 - Spector Professional 5.0
 - Handy Keylogger

- Snapshot Spy
- System Event Logging and Reviewing Tools
 - LT Auditor Version 8.0
 - ZVisual RACF
 - Network Intelligence Engine LS Series
- Tripwire and Checksum Tools
 - SecurityExpressions
 - MD5
 - Tripwire for Servers
- Mobile-Code Scanning Tools
 - Vital Security
 - E Trust Secure Content Manager 1.1
 - Internet Explorer Zones
- Centralized Security Monitoring Tools
 - ASAP eSMART™ Software Usage by ASAP Software
 - WatchGuard VPN Manager
 - Harvester
- Web Log Analysis Tools
 - AWStats
 - Azure Web Log
 - Summary
- Forensic Data and Collection Tools
 - Encase tool
 - SafeBack
 - ILook Investigator
- Security Assessment Tools
 - Nessus Windows Technology
 - NetIQ Security Manager
 - STAT Scanner
- Multiple OS Management Tools
 - Multiple Boot Manager
 - Acronis OS Selector
 - Eon
- Phases of Penetration Testing
 - Pre-Attack Phase
 - Attack Phase
 - Post-Attack Phase

- Penetration Testing Deliverables Templates

Covert Hacking

- Insider attacks
- What is covert channel?
- Security Breach
- Why Do You Want to Use Covert Channel?
- Motivation of a Firewall Bypass
- Covert Channels Scope
- Covert Channel: Attack Techniques
- Simple Covert Attacks
- Advanced Covert Attacks
- Reverse Connecting Agents
- Covert Channel Attack Tools
 - Netcat
 - DNS tunnel
 - DNS Tunneling
 - Covert Channel Using DNS Tunneling
 - DNS Tunnel Client
 - DNS Tunneling Countermeasures
 - SSH reverse tunnel
 - Covert Channel Using SSH
 - Covert Channel using SSH (Advanced)
 - HTTP/S Tunneling Attack
 - Covert Channel Hacking Tool: Active Port Forwarder
 - Covert Channel Hacking Tool: CCTT
 - Covert Channel Hacking Tool: Firepass
 - Covert Channel Hacking Tool: MsnShell
 - Covert Channel Hacking Tool: Web Shell
 - Covert Channel Hacking Tool: NCovert
 - Covert Channel Hacking via Spam E-mail Messages
 - Hydan
 - Covert Channel Hacking Tool: NCOVERT

Writing Virus Codes

- Introduction of Virus
- Types of Viruses
- Symptoms of a Virus Attack
- Prerequisites for Writing Viruses
- Required Tools and Utilities
- Virus Infection Flow Chart
 - Step – I Finding file to infect
 - Directory Traversal Method
 - “dot dot” Method
 - Step – II Check viruses infection criteria
 - Step – III Check for previous infection
 - Marking a File for Infection
 - Step – IV Infect the file
 - Step – V Covering tracks
 -
- Components of Viruses
- Functioning of Replicator part
- Diagrammatical representation
- Writing Replicator
- Writing Concealer
- Dispatcher
- Writing Bomb/Payload
- Trigger Mechanism
- Brute Force Logic Bombs
- Testing Virus Codes
- Tips for Better Virus Writing

Assembly Language Tutorial

- Number System
- Base 10 System
- Base 2 System
- Decimal 0 to 15 in Binary
- Binary Addition (C stands for Carry)
- Hexadecimal Number
- Hex Example

- Hex Conversion
- nibble
- Computer memory
- Characters Coding
- ASCII and UNICODE
- CPU
- Machine Language
- Compilers
- Clock Cycle
- Original Registers
- Instruction Pointer
- Pentium Processor
- Interrupts
- Interrupt handler
- External interrupts and Internal interrupts
- Handlers
- Machine Language
- Assembly Language
- Assembler
- Assembly Language Vs High-level Language
- Assembly Language Compilers
- Instruction operands
- MOV instruction
- ADD instruction
- SUB instruction
- INC and DEC instructions
- Directive
- preprocessor
- equ directive
- %define directive
- Data directives
- Labels
- Input and output
- C Interface
- Call
- Creating a Program
- Why should anyone learn assembly at all?

- First.asm
 - Assembling the code
 - Compiling the C code
 - Linking the object files
 - Understanding an assembly listing file
 - Big and Little Endian Representation
 - Skeleton File
 - Working with Integers
 - Signed integers
 - Signed Magnitude
 - Two's Complement
 - If statements
 - Do while loops
 - Indirect addressing
 - Subprogram
 - The Stack
 - The SS segment
 - ESP
 - The Stack Usage
 - The CALL and RET Instructions
 - General subprogram form
 - Local variables on the stack
 - General subprogram form with local variables
 - Multi-module program
 - Saving registers
 - Labels of functions
 - Calculating addresses of local variables

Exploit Writing

- Exploits Overview
- Prerequisites for Writing Exploits and Shellcodes
- Purpose of Exploit Writing
- Types of Exploits
 - Stack Overflow
 - Heap Corruption
 - Format String

- Integer Bug Exploits
 - Race Condition
 - TCP/IP Attack
- The Proof-of-Concept and Commercial Grade Exploit
- Converting a Proof of Concept Exploit to Commercial Grade Exploit
- Attack Methodologies
- Socket Binding Exploits
- Tools for Exploit Writing
 - LibExploit
 - Metasploit
 - CANVAS
- Steps for Writing an Exploit
- Differences Between Windows and Linux Exploits
- Shellcodes
 - NULL Byte
 - Types of Shellcodes
- Tools Used for Shellcode Development
 - NASM
 - GDB
 - objdump
 - ktrace
 - strace
 - readelf
- Steps for Writing a Shellcode
- Issues Involved With Shellcode Writing
 - Addressing problem
 - Null byte problem
 - System call implementation

Smashing the Stack for Fun and Profit

- What is a Buffer?
- Static Vs Dynamic Variables
- Stack Buffers
- Data Region
- Memory Process Regions
- What Is A Stack?

- Why Do We Use A Stack?
- The Stack Region
- Stack frame
- Stack pointer
- Procedure Call (Procedure Prolog)
- Compiling the code to assembly
- Call Statement
- Return Address (RET)
- Word Size
- Stack
- Buffer Overflows
- Error
- Why do we get a segmentation violation?
- Segmentation Error
- Instruction Jump
- Guess Key Parameters
- Calculation
- Shell Code
 - The code to spawn a shell in C
- Lets try to understand what is going on here. We'll start by studying main:
- `execve()`
 - `execve()` system call
- `exit.c`
 - List of steps with exit call
- The code in Assembly
- JMP
- Code using indexed addressing
- Offset calculation
- `shellcodeasm.c`
- `testsc.c`
- Compile the code
- NULL byte
- `shellcodeasm2.c`
- `testsc2.c`
- Writing an Exploit
- `overflow1.c`
- Compiling the code

- sp.c
- vulnerable.c
- NOPs
 - Using NOPs
 - Estimating the Location

Windows Based Buffer Overflow Exploit Writing

- Buffer Overflow
- Stack overflow
- Writing Windows Based Exploits
- Exploiting stack based buffer overflow
- OpenDataSource Buffer Overflow Vulnerability Details
- Simple Proof of Concept
- Windbg.exe
- Analysis
- EIP Register
 - Location of EIP
 - EIP
- Execution Flow
- But where can we jump to?
- Offset Address
- The Query
- Finding jmp esp
- Debug.exe
- listdlls.exe
- Msvcrt.dll
- Out.sql
- The payload
- ESP
- Limited Space
- Getting Windows API/function absolute address
- Memory Address
- Other Addresses
- Compile the program
- Final Code

Reverse Engineering

- Positive Applications of Reverse Engineering
- Ethical Reverse Engineering
- World War Case Study
- DMCA Act
- What is Disassembler?
- Why do you need to decompile?
- Professional Disassembler Tools
- Tool: IDA Pro
- Convert Machine Code to Assembly Code
- Decompilers
- Program Obfuscation
- Convert Assembly Code to C++ code
- Machine Decompilers
- Tool: dcc
- Machine Code of compute.exe Program
- Assembly Code of compute.exe Program
- Code Produced by the dcc Decompiler in C
- Tool: Boomerang
- What Boomerang Can Do?
- Andromeda Decompiler
- Tool: REC Decompiler
- Tool: EXE To C Decompiler
- Delphi Decompilers
- Tools for Decompiling .NET Applications
- Salamander .NET Decompiler
- Tool: LSW DotNet-Reflection-Browser
- Tool: Reflector
- Tool: Spices NET.Decompiler
- Tool: Decompilers.NET
- .NET Obfuscator and .NET Obfuscation
- Java Bytecode Decompilers
- Tool: JODE Java Decompiler
- Tool: JREVERSEPRO
- Tool: SourceAgain
- Tool: ClassCracker
- Python Decompilers

- Reverse Engineering Tutorial
- OllyDbg Debugger
- How Does OllyDbg Work?
- Debugging a Simple Console Application