



ETHICAL HACKING AND COUNTERMEASURES

<http://www.eccouncil.org>

EC-Council

C | **EH** TM
Certified Ethical Hacker

Hackers are here. Where are you?

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The definition of an Ethical Hacker is very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

Hackers Are Here. Where Are You?

Ethical Hacking and Countermeasures Training Program

Course Description

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50

Who Should Attend

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Duration:

5 days (9:00 – 5:00)

Certification

The Certified Ethical Hacker certification exam 312-50 will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the CEH certification.

Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Course Outline v6.1

Module 1: Introduction to Ethical Hacking

- Problem Definition -Why Security?
- Essential Terminologies
- Elements of Security
- The Security, Functionality and Ease of Use Triangle
- Effect on Business
- Case Study
- What does a Malicious Hacker do?
 - Phase1-Reconnaissance
 - Reconnaissance Types
 - Phase2-Scanning
 - Phase3-Gaining Access
 - Phase4-Maintaining Access
 - Phase5-Covering Tracks
- Types of Hacker Attacks
 - Operating System attacks
 - Application-level attacks
 - Shrink Wrap code attacks
 - Misconfiguration attacks
- Hactivism
- Hacker Classes
- Security News: Suicide Hacker
- Ethical Hacker Classes
- 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
 - National Vulnerability Database (nvd.nist.gov)
 - Securitytracker (www.securitytracker.com)
 - Securiteam (www.securiteam.com)
 - Secunia (www.secunia.com)
 - Hackerstorm Vulnerability Database Tool (www.hackerstrom.com)
 - HackerWatch (www.hackerwatch.org)
 - SecurityFocus (www.securityfocus.com)
 - SecurityMagazine (www.securitymagazine.com)
 - SC Magazine (www.scmagazine.com)
 - MILWORM
- How to Conduct Ethical Hacking
- How Do They Go About It
- Approaches to Ethical Hacking
- Ethical Hacking Testing
- Ethical Hacking Deliverables
- Computer Crimes and Implications

Module 2: Hacking Laws

- U.S. Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)
- Legal Perspective (U.S. Federal Law)
 - 18 U.S.C. § 1029
 - Penalties
 - 18 U.S.C. § 1030

- Penalties
 - 18 U.S.C. § 1362
 - 18 U.S.C. § 2318
 - 18 U.S.C. § 2320
 - 18 U.S.C. § 1831
 - 47 U.S.C. § 605, unauthorized publication or use of communications
 - Washington:
 - RCW 9A.52.110
 - Florida:
 - § 815.01 to 815.07
 - Indiana:
 - IC 35-43
- United Kingdom's Cyber Laws
- United Kingdom: Police and Justice Act 2006
- European Laws
- Japan's Cyber Laws
- Australia : The Cybercrime Act 2001
- Indian Law: THE INFORMATION TECHNOLOGY ACT
- Argentina Laws
- Germany's Cyber Laws
- Singapore's Cyber Laws
- Belgium Law
- Brazilian Laws
- Canadian Laws
- France Laws
- German Laws
- Italian Laws
- MALAYSIA: THE COMPUTER CRIMES ACT 1997

- HONGKONG: TELECOMMUNICATIONS
- Korea: ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.
- Greece Laws
- Denmark Laws
- Netherlands Laws
- Norway
- ORDINANCE
- Mexico
- SWITZERLAND

Module 3: Footprinting

- Revisiting Reconnaissance
- Defining Footprinting
- Why is Footprinting Necessary
- Areas and Information which Attackers Seek
- Information Gathering Methodology
 - Unearthing Initial Information
 - Finding Company's URL
 - Internal URL
 - Extracting Archive of a Website
 - www.archive.org
 - Google Search for Company's Info
 - People Search
 - Yahoo People Search
 - Satellite Picture of a Residence
 - Best PeopleSearch
 - People-Search-America.com

- Switchboard
- Anacubis
- Google Finance
- Yahoo Finance
- Footprinting through Job Sites
- Passive Information Gathering
- Competitive Intelligence Gathering
 - Why Do You Need Competitive Intelligence?
 - Competitive Intelligence Resource
 - Companies Providing Competitive Intelligence Services
 - Carratu International
 - CI Center
 - Competitive Intelligence - When Did This Company Begin? How Did It Develop?
 - Competitive Intelligence - Who Leads This Company
 - Competitive Intelligence - What Are This Company's Plans
 - Competitive Intelligence - What Does Expert Opinion Say About The Company
 - Competitive Intelligence - Who Are The Leading Competitors?
 - Competitive Intelligence Tool: Trellian
 - Competitive Intelligence Tool: Web Investigator
- Public and Private Websites
 - Footprinting Tools
 - Sensepost Footprint Tools
 - Big Brother
 - BiLE Suite
 - Alchemy Network Tool
 - Advanced Administrative Tool
 - My IP Suite
 - Wikto Footprinting Tool

- Whois Lookup
- Whois
- SmartWhois
- ActiveWhois
- LanWhois
- CountryWhois
- WhereIsIP
- Ip2country
- CallerIP
- Web Data Extractor Tool
- Online Whois Tools
- What is MyIP
- DNS Enumerator
- SpiderFoot
- Nslookup
- Extract DNS Information
 - Types of DNS Records
 - Necrosoft Advanced DIG
- Expired Domains
- DomainKing
- Domain Name Analyzer
- DomainInspect
- MSR Strider URL Tracer
- Mozzle Domain Name Pro
- Domain Research Tool (DRT)
- Domain Status Reporter
- Reggie
- Locate the Network Range

- ARIN
- Traceroute
 - Traceroute Analysis
- 3D Traceroute
- NeoTrace
- VisualRoute Trace
- Path Analyzer Pro
- Maltego
- Layer Four Traceroute
- Prefix WhoIs widget
- Touchgraph
- VisualRoute Mail Tracker
- eMailTrackerPro
- Read Notify
- E-Mail Spiders
 - 1st E-mail Address Spider
 - Power E-mail Collector Tool
 - GEOSpider
 - Geowhere Footprinting Tool
 - Google Earth
 - Kartoo Search Engine
 - Dogpile (Meta Search Engine)
 - Tool: WebFerret
 - robots.txt
 - WTR - Web The Ripper
 - HTTrack Web Site Copier
 - Website Watcher
- How to Create Fake Website

- Real and Fake Website
- Tool: Reamweaver
- Mirrored Fake Website
- Faking Websites using Man-in-the-Middle Phishing Kit
- Benefits to Fraudster
- Steps to Perform Footprinting

Module 4: Google Hacking

- What is Google hacking
- What a hacker can do with vulnerable site
- Anonymity with Caches
- Using Google as a Proxy Server
- Directory Listings
 - Locating Directory Listings
 - Finding Specific Directories
 - Finding Specific Files
 - Server Versioning
- Going Out on a Limb: Traversal Techniques
 - Directory Traversal
 - Incremental Substitution
- Extension Walking
- Site Operator
- intitle:index.of
- error | warning
- login | logon
- username | userid | employee.ID | “your username is”
- password | passcode | “your password is”
- admin | administrator

- admin login
- –ext:html –ext:htm –ext:shtml –ext:asp –ext:php
- inurl:temp | inurl:tmp | inurl:backup | inurl:bak
- intranet | help.desk
- Locating Public Exploit Sites
 - Locating Exploits Via Common Code Strings
 - Searching for Exploit Code with Nonstandard Extensions
 - Locating Source Code with Common Strings
- Locating Vulnerable Targets
 - Locating Targets Via Demonstration Pages
 - “Powered by” Tags Are Common Query Fodder for Finding Web Applications
 - Locating Targets Via Source Code
 - Vulnerable Web Application Examples
 - Locating Targets Via CGI Scanning
 - A Single CGI Scan-Style Query
- Directory Listings
 - Finding IIS 5.0 Servers
- Web Server Software Error Messages
 - IIS HTTP/1.1 Error Page Titles
 - “Object Not Found” Error Message Used to Find IIS 5.0
 - Apache Web Server
 - Apache 2.0 Error Pages
- Application Software Error Messages
 - ASP Dumps Provide Dangerous Details
 - Many Errors Reveal Pathnames and Filenames
 - CGI Environment Listings Reveal Lots of Information
- Default Pages
 - A Typical Apache Default Web Page

- Locating Default Installations of IIS 4.0 on Windows NT 4.0/OP
- Default Pages Query for Web Server
- Outlook Web Access Default Portal
- Searching for Passwords
 - Windows Registry Entries Can Reveal Passwords
 - Usernames, Cleartext Passwords, and Hostnames!
- Google Hacking Database (GHDB)
- SiteDigger Tool
- Gooscan
- Goolink Scanner
- Goolag Scanner
- Tool: Google Hacks
- Google Hack Honeygot
- Google Protocol
- Google Cartography

Module 5: Scanning

- Scanning: Definition
- Types of Scanning
- Objectives of Scanning
- CEH Scanning Methodology
 - Checking for live systems - ICMP Scanning
 - Angry IP
 - Ping Sweep
 - Firewalk Tool
 - Firewalk Commands
 - Firewalk Output

- Three Way Handshake
- TCP Communication Flags
- Nmap
- Nmap: Scan Methods
- NMAP Scan Options
- NMAP Output Format
- HPing2
- 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
- SYN/FIN Scanning Using IP Fragments
- UDP Scanning
- Reverse Ident Scanning
- Window Scan
- Blaster Scan
- Portscan Plus, Strobe
- IPsec Scan
- Netscan Tools Pro
- WUPS – UDP Scanner
- Superscan
- IPScanner
- Global Network Inventory Scanner
- Net Tools Suite Pack

- Floppy Scan
- FloppyScan Steps
- E-mail Results of FloppyScan
- Atelier Web Ports Traffic Analyzer (AWPTA)
- Atelier Web Security Port Scanner (AWSPS)
- IPEye
- ike-scan
- Infiltrator Network Security Scanner
- YAPS: Yet Another Port Scanner
- Advanced Port Scanner
- NetworkActiv Scanner
- NetGadgets
- P-Ping Tools
- MegaPing
- LanSpy
- HoverIP
- LANView
- NetBruteScanner
- SolarWinds Engineer's Toolset
- AUTAPF
- OstroSoft Internet Tools
- Advanced IP Scanner
- Active Network Monitor
- Advanced Serial Data Logger
- Advanced Serial Port Monitor
- WotWeb
- Antiy Ports
- Port Detective

- Roadkil's Detector
- Portable Storage Explorer
- War Dialer Technique
 - Why War Dialing
 - Wardialing
 - Phonesweep – War Dialing Tool
 - THC Scan
 - ToneLoc
 - ModemScan
 - War Dialing Countermeasures: Sandtrap Tool
- Banner Grabbing
 - OS Fingerprinting
 - Active Stack Fingerprinting
 - Passive Fingerprinting
 - Active Banner Grabbing Using Telnet
 - GET REQUESTS
 - Pof – Banner Grabbing Tool
 - pof for Windows
 - Httpprint Banner Grabbing Tool
 - Tool: Miart HTTP Header
 - Tools for Active Stack Fingerprinting
 - Xprobe2
 - Ringv2
 - Netcraft
 - Disabling or Changing Banner
 - IIS Lockdown Tool
 - Tool: ServerMask
 - Hiding File Extensions

- Tool: PageXchanger
- Vulnerability Scanning
 - Bidiblah Automated Scanner
 - Qualys Web Based Scanner
 - SAINT
 - ISS Security Scanner
 - Nessus
 - GFI Languard
 - Security Administrator's Tool for Analyzing Networks (SATAN)
 - Retina
 - Nagios
 - PacketTrap's pt360 Tool Suite
 - NIKTO
 - SAFESuite Internet Scanner, IdentTCPScan
- Draw Network Diagrams of Vulnerable Hosts
 - Friendly Pinger
 - LANsurveyor
 - Ipsonar
 - LANState
 - Insightix Visibility
 - IPCheck Server Monitor
 - PRTG Traffic Grapher
- Preparing Proxies
 - Proxy Servers
 - Use of Proxies for Attack
 - Free Proxy Servers
 - SocksChain
 - Proxy Workbench

- Proxymanager Tool
- Super Proxy Helper Tool
- Happy Browser Tool (Proxy Based)
- Multiproxy
- Tor Proxy Chaining Software
- Additional Proxy Tools
- Anonymizers
 - Surfing Anonymously
 - Primedia Anonymizer
 - StealthSurfer
 - Anonymous Surfing: Browzar
 - Torpark Browser
 - GetAnonymous
 - IP Privacy
 - Anonymity 4 Proxy (A4Proxy)
 - Psiphon
 - Connectivity Using Psiphon
 - Bloggers Write Text Backwards to Bypass Web Filters in China
 - Vertical Text Converter
 - How to Check If Your Website Is Blocked In China or Not
 - Mowser and Phonifier
 - AnalogX Proxy
 - NetProxy
 - Proxy+
 - ProxySwitcher Lite
 - JAP
 - Proxomitron
- Google Cookies

- G-Zapper
- SSL Proxy Tool
- How to Run SSL Proxy
- HTTP Tunneling Techniques
 - Why Do I Need HTTP Tunneling
- Httptunnel for Windows
- How to Run Httptunnel
- HTTP-Tunnel
- HTTPort
- Spoofing IP Address
 - Spoofing IP Address Using Source Routing
 - Detection of IP Spoofing
 - Despoof Tool
- Scanning Countermeasures
- Tool: SentryPC

Module 6: Enumeration

- Overview of System Hacking Cycle
- What is Enumeration?
- Techniques for Enumeration
- NetBIOS Null Sessions
 - So What's the Big Deal
 - DumpSec Tool
 - NetBIOS Enumeration Using Netview
 - Nbtstat Enumeration Tool
 - SuperScan
 - Enum Tool
 - Enumerating User Accounts

- GetAcct
 - Null Session Countermeasure
- PS Tools
 - PsExec
 - PsFile
 - PsGetSid
 - PsKill
 - PsInfo
 - PsList
 - PsLogged On
 - PsLogList
 - PsPasswd
 - PsService
 - PsShutdown
 - PsSuspend
- Simple Network Management Protocol (SNMP) Enumeration
 - Management Information Base (MIB)
 - SNMPutil Example
 - SolarWinds
 - SNScan
 - Getif SNMP MIB Browser
 - UNIX Enumeration
 - SNMP UNIX Enumeration
 - SNMP Enumeration Countermeasures
- LDAP enumeration
 - JXplorer
 - LdapMiner
 - Softerra LDAP Browser

- NTP enumeration
- SMTP enumeration
 - Smtpscan
- Web enumeration
 - Asnumber
 - Lynx
- Winfingerprint
 - Windows Active Directory Attack Tool
- How To Enumerate Web Application Directories in IIS Using DirectoryServices
- IP Tools Scanner
- Enumerate Systems Using Default Password
- Tools:
 - NBTScan
 - NetViewX
 - FREENETENUMERATOR
 - Terminal Service Agent
 - TXNDS
 - Unicornscan
 - Amap
 - Netenum
- Steps to Perform Enumeration

Module 7: System Hacking

- Part 1- Cracking Password
 - CEH hacking Cycle
 - Password Types
 - Types of Password Attack
 - Passive Online Attack: Wire Sniffing

- Passive Online Attack: Man-in-the-middle and replay attacks
- Active Online Attack: Password Guessing
- Offline Attacks
 - Brute force Attack
 - Pre-computed Hashes
 - Syllable Attack/Rule-based Attack/ Hybrid attacks
 - Distributed network Attack
 - Rainbow Attack
- Non-Technical Attacks
- Default Password Database
 - <http://www.defaultpassword.com/>
 - <http://www.cirt.net/cgi-bin/passwd.pl>
 - <http://www.virus.org/index.php?>
- PDF Password Cracker
- Abcom PDF Password Cracker
- Password Mitigation
- Permanent Account Lockout-Employee Privilege Abuse
- Administrator Password Guessing
 - Manual Password cracking Algorithm
- Automatic Password Cracking Algorithm
- Performing Automated Password Guessing
 - Tool: NAT
 - Smbbf (SMB Passive Brute Force Tool)
 - SmbCrack Tool: Legion
 - Hacking Tool: LOphcrack
- Microsoft Authentication
 - LM, NTLMv1, and NTLMv2
- NTLM And LM Authentication On The Wire

- Kerberos Authentication
- What is LAN Manager Hash?
 - LM “Hash” Generation
 - LM Hash
- Salting
- PWdump2 and Pwdump3
- Tool: Rainbowcrack
- Hacking Tool: KerbCrack
- Hacking Tool: John the Ripper
- Password Sniffing
- How to Sniff SMB Credentials?
- SMB Signing
- Tool: LCP
- Tool: SID&User
- Tool: Ophcrack 2
- Tool: Crack
- Tool: Access PassView
- Tool: Asterisk Logger
- Tool: CHAOS Generator
- Tool: Asterisk Key
- Password Recovery Tool: MS Access Database Password Decoder
- Password Cracking Countermeasures
- Do Not Store LAN Manager Hash in SAM Database
- LM Hash Backward Compatibility
- How to Disable LM HASH
- Password Brute-Force Estimate Tool
- Syskey Utility
- AccountAudit

- Part2-Escalating Privileges
 - CEH Hacking Cycle
 - Privilege Escalation
 - Cracking NT/2000 passwords
 - Active@ Password Changer
 - Change Recovery Console Password - Method 1
 - Change Recovery Console Password - Method 2
 - Privilege Escalation Tool: x.exe
 - Login Hack: Example
- Part3-Executing applications
 - CEH Hacking Cycle
 - Tool: psexec
 - Tool: remoexec
 - Ras N Map
 - Tool: Alchemy Remote Executor
 - Emsa FlexInfo Pro
 - Keystroke Loggers
 - E-mail Keylogger
 - Revealer Keylogger Pro
 - Handy Keylogger
 - Ardamax Keylogger
 - Powered Keylogger
 - Quick Keylogger
 - Spy-Keylogger
 - Perfect Keylogger
 - Invisible Keylogger
 - Actual Spy
 - SpyToctor FTP Keylogger

- IKS Software Keylogger
- Ghost Keylogger
- Hacking Tool: Hardware Key Logger
- What is Spyware?
- Spyware: Spector
- Remote Spy
- Spy Tech Spy Agent
- 007 Spy Software
- Spy Buddy
- Ace Spy
- Keystroke Spy
- Activity Monitor
- Hacking Tool: eBlaster
- Stealth Voice Recorder
- Stealth Keylogger
- Stealth Website Logger
- Digi Watcher Video Surveillance
- Desktop Spy Screen Capture Program
- Telephone Spy
- Print Monitor Spy Tool
- Stealth E-Mail Redirector
- Spy Software: Wiretap Professional
- Spy Software: FlexiSpy
- PC PhoneHome
- Keylogger Countermeasures
- Anti Keylogger
- Advanced Anti Keylogger
- Privacy Keyboard

- Spy Hunter - Spyware Remover
- Spy Sweeper
- Spyware Terminator
- WinCleaner AntiSpyware
- Part4-Hiding files
 - CEH Hacking Cycle
 - Hiding Files
 - RootKits
 - Why rootkits
 - Hacking Tool: NT/2000 Rootkit
 - Planting the NT/2000 Rootkit
 - Rootkits in Linux
 - Detecting Rootkits
 - Steps for Detecting Rootkits
 - Rootkit Detection Tools
 - Sony Rootkit Case Study
 - Rootkit: Fu
 - AFX Rootkit
 - Rootkit: Nuclear
 - Rootkit: Vanquish
 - Rootkit Countermeasures
 - Patchfinder
 - RootkitRevealer
 - Creating Alternate Data Streams
 - How to Create NTFS Streams?
 - NTFS Stream Manipulation
 - NTFS Streams Countermeasures
 - NTFS Stream Detectors (ADS Spy and ADS Tools)

- Hacking Tool: USB Dumper
- What is Steganography?
 - Steganography Techniques
 - Least Significant Bit Insertion in Image files
 - Process of Hiding Information in Image Files
 - Masking and Filtering in Image files
 - Algorithms and transformation
 - Tool: Merge Streams
 - Invisible Folders
 - Tool: Invisible Secrets
 - Tool : Image Hide
 - Tool: Stealth Files
 - Tool: Steganography
 - Masker Steganography Tool
 - Hermetic Stego
 - DCPD – Hide an Operating System
 - Tool: Camera/Shy
 - www.spammimic.com
 - Tool: Mp3Stego
 - Tool: Snow.exe
 - Steganography Tool: Fort Knox
 - Steganography Tool: Blindside
 - Steganography Tool: S- Tools
 - Steganography Tool: Steghide
 - Tool: Steganos
 - Steganography Tool: Pretty Good Envelop
 - Tool: Gifshuffle
 - Tool: JPHIDE and JPSEEK

- Tool: wbStego
- Tool: OutGuess
- Tool: Data Stash
- Tool: Hydan
- Tool: Cloak
- Tool: StegoNote
- Tool: Stegomagic
- Steganos Security Suite
- C Steganography
- Isosteg
- FoxHole
- Sams Big Playmaker
- Video Steganography
- Case Study: Al-Qaida members Distributing Propaganda to Volunteers using Steganography
- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Stegdetec
- SIDS
- High-Level View
- Tool: dskprobe.exe
- Stego Watch- Stego Detection Tool
- StegSpy
- Part5-Covering Tracks
 - CEH Hacking Cycle
 - Covering Tracks
 - Disabling Auditing
 - Clearing the Event Log

- Tool: elsave.exe
- Hacking Tool: Winzapper
- Evidence Eliminator
- Tool: Traceless
- Tool: Tracks Eraser Pro
- Armor Tools
- Tool: ZeroTracks

Module 8: Trojans and Backdoors

- What is a Trojan?
 - Overt and Covert Channels
 - Working of Trojans
 - Different Types of Trojans
 - Remote Access Trojans
 - Data-Sending Trojans
 - Destructive Trojans
 - Denial-of-Service (DoS) Attack Trojans
 - Proxy Trojans
 - FTP Trojans
 - Security Software Disablers
 - 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
 - Trojan: Tini
 - Trojan: iCmd

- Trojan: NetBus
- Trojan: Netcat
- Netcat Client/Server
- Trojan: Beast
- MoSucker Trojan
- SARS Trojan Notification
- Proxy Server Trojan
- FTP Trojan - TinyFTPD
- VNC Trojan
- Wrappers
- Wrapper Covert Program
- Wrapping Tools
- One Exe Maker / YAB / Pretator Wrappers
- Packaging Tool: WordPad
- RemoteByMail
- Tool: Icon Plus
- Defacing Application: Restorator
- Tetris
- Stealth Trojans
 - HTTP Trojans
 - Trojan Attack through Http
 - HTTP Trojan (HTTP RAT)
 - Shttpd Trojan - HTTP Server
 - Tool: BadLuck Destructive Trojan
 - Loki
 - Loki Countermeasures
 - Atelier Web Remote Commander
 - Trojan Horse Construction Kit

- ICMP Tunneling
- ICMP Backdoor Trojan
- Reverse Connecting Trojans
 - Reverse Connecting Trojans
 - Nuclear RAT Trojan (Reverse Connecting)
 - Reverse Tunnel
 - Covert Channel Tunneling Tool (cctt)
 - Windows Reverse Shell
 - perl-reverse-shell
 - php-reverse-shell
 - XSS Shell Tunnel
 - winarp_mim
- Miscellaneous Trojans
 - Backdoor.Theef (AVP)
 - T2W (TrojanToWorm)
 - Biorante RAT
 - DownTroj
 - Turkojan
 - Trojan.Satellite-RAT
 - Yakoza
 - DarkLabel B4
 - Trojan.Hav-Rat
 - Poison Ivy
 - Rapid Hacker
 - SharK
 - HackerzRat
 - TYO
 - 1337 Fun Trojan

- Criminal Rat Beta
- VicSpy
- Optix PRO
- ProAgent
- OD Client
- AceRat
- Mhacker-PS
- RubyRAT Public
- SINner
- ConsoleDevil
- ZombieRat
- Webcam Trojan
- DJI RAT
- Skiddie Rat
- Biohazard RAT
- Troya
- ProRat
- Dark Girl
- DaCryptic
- Net-Devil
- PokerStealer.A
- Hovdy.a
- How to Detect Trojans?
 - Netstat
 - fPort
 - TCPView
 - CurrPorts Tool
 - Process Viewer

- Delete Suspicious Device Drivers
- Check for Running Processes: What's on My Computer
- Super System Helper Tool
- Inzider-Tracks Processes and Ports
- Tool: What's Running
- MS Configuration Utility
- Autoruns
- Hijack This (System Checker)
- Startup List
- Anti-Trojan Software
 - TrojanHunter
 - Comodo BOClean
 - Trojan Remover: XoftspySE
 - Trojan Remover: Spyware Doctor
 - SPYWAREfighter
- Evading Anti-Virus Techniques
- Sample Code for Trojan Client/Server
- Evading Anti-Trojan/Anti-Virus using Stealth Tools
- Backdoor Countermeasures
- Tripwire
- System File Verification
- MD5 Checksum.exe
- Microsoft Windows Defender
- How to Avoid a Trojan Infection

Module 9: Viruses and Worms

- Virus History
- Characteristics of Virus

- Working of Virus
 - Infection Phase
 - Attack Phase
- Why people create Computer Viruses
- Symptoms of a Virus-like Attack
- Virus Hoaxes
- Chain Letters
- Worms
- How is a Worm Different from a Virus
- Indications of a Virus Attack
- Virus Damage
 - Mode of Virus Infection
- Stages of Virus Life
- Types of Virus
 - Virus Classification
 - How Does a Virus Infect?
 - Storage Patterns of Virus
 - System Sector virus
 - Stealth Virus
 - Bootable CD-Rom Virus
 - Self -Modification
 - Encryption with a Variable Key
 - Polymorphic Code
 - Metamorphic Virus
 - Cavity Virus
 - Sparse Infector Virus
 - Companion Virus
 - File Extension Virus

- Famous Viruses and Worms
 - Famous Virus/Worms – I Love You Virus
 - Famous Virus/Worms – Melissa
 - Famous Virus/Worms – JS/Spth
 - Klez Virus Analysis
 - Slammer Worm
 - Spread of Slammer Worm – 30 min
 - MyDoom.B
 - SCO Against MyDoom Worm
- Latest Viruses
 - Latest Viruses
 - Top 10 Viruses- 2008
 - Virus: Win32.AutoRun.ah
 - Virus:W32/Virut
 - Virus:W32/Divvi
 - Worm.SymbOS.Lasco.a
 - Disk Killer
 - Bad Boy
 - HappyBox
 - Java.StrangeBrew
 - MonteCarlo Family
 - PHP.Newworld
 - W32/WBoy.a
 - ExeBug.d
 - W32/Voterai.worm.e
 - W32/Lecivio.worm
 - W32/Lurka.a
 - W32/Vora.worm!p2p

- Writing Virus Program
 - Writing a Simple Virus Program
 - Virus Construction Kits
- Virus Detection Methods
 - Virus Detection Methods
 - Virus Incident Response
 - What is Sheep Dip?
 - Virus Analysis – IDA Pro Tool
 - Online Virus Testing: <http://www.virustotal.com/>
 - Prevention is better than Cure
- Anti-Virus Software
 - Anti-Virus Software
 - AVG Antivirus
 - Norton Antivirus
 - McAfee
 - Socketsheild
 - BitDefender
 - ESET Nod32CA Anti-Virus
 - F-Secure Anti-Virus
 - Kaspersky Anti-Virus
 - F-Prot Antivirus
 - Panda Antivirus Platinum
 - avast! Virus Cleaner
 - ClamWin
 - Norman Virus Control
- Popular Anti-Virus Packages
- Virus Databases
- Snopes.com

Module 10: Sniffers

- Definition: Sniffing
- Types of Sniffing
- Protocols Vulnerable to Sniffing
- Passive Sniffing
- Active Sniffing
- Switched Port Analyzer (SPAN)
- SPAN Port
- Lawful Intercept
- Benefits of Lawful Intercept
- Network Components Used for Lawful Intercept
- Ready to Sniff?
- Tool: Network View – Scans the Network for Devices
- The Dude Sniffer
- Look@LAN
- Wireshark
- Display Filters in Wireshark
- Following the TCP Stream in Wireshark
- Pilot
- Tcpdump
- Tcpdump Commands
- Features of Sniffing Tools
- What is Address Resolution Protocol (ARP)
- ARP Spoofing Attack
- How Does ARP Spoofing Work
- ARP Poisoning
- Threats of ARP Poisoning

- MAC Flooding
- Mac Duplicating
- Mac Duplicating Attack
- Tools for ARP Spoofing
 - Ettercap
 - ArpSpyX
 - Cain and Abel
 - Steps to Perform ARP Poisoning using Cain and Abel
 - IRS – ARP Attack Tool
 - ARPWorks Tool
 - DHCP Starvation Attack
- DNS Poisoning Techniques
 - 1. Intranet DNS Spoofing (Local Network)
 - 2. Internet DNS Spoofing (Remote Network)
 - Internet DNS Spoofing
 - 3. Proxy Server DNS Poisoning
 - 4. DNS Cache Poisoning
- Tools for MAC Flooding
 - Linux Tool: Macof
 - Windows Tool: EtherFlood
- Sniffing Tools
 - Interactive TCP Relay
 - Interactive Replay Attacks
 - Tool: Nemesis
 - HTTP Sniffer: EffeTech
 - HTTP Sniffer: EffeTech
 - Ace Password Sniffer
 - Win Sniffer

- MSN Sniffer
- SmartSniff
- Session Capture Sniffer: NetWitness
- Packet Crafter Craft Custom TCP/IP Packets
- Engage Packet Builder
- SMAC
- NetSetMan Tool
- Ntop
- EtherApe
- EtherApe Features
- Network Probe
- Maa Tec Network Analyzer
- Tool: Snort
- Tool: Windump
- Tool: Etherpeek
- NetIntercept
- Colasoft EtherLook
- AW Ports Traffic Analyzer
- Colasoft Capsa Network Analyzer
- CommView
- Sniffem
- NetResident
- IP Sniffer
- Sniphere
- IE HTTP Analyzer
- BillSniff
- URL Snooper
- EtherDetect Packet Sniffer

- ArpWatch Tool
- PromiScan
- proDETECT
- Network Packet Analyzer CAPSA

Module 11: Social Engineering

- What is Social Engineering?
- Human Weakness
- “Rebecca” and “Jessica”
- Office Workers
- Types of Social Engineering
 - Human-Based Social Engineering
 - Technical Support Example
 - More Social Engineering Examples
 - Human-Based Social Engineering: Eavesdropping
 - Human-Based Social Engineering: Shoulder Surfing
 - Human-Based Social Engineering: Dumpster Diving
 - Dumpster Diving Example
 - Oracle Snoops Microsoft’s Trash Bins
 - Movies to Watch for Reverse Engineering
 - Computer Based Social Engineering
 - Insider Attack
 - Disgruntled Employee
 - Preventing Insider Threat
 - Common Targets of Social Engineering
- Social Engineering Threats and Defenses
 - Online Threats
 - Telephone-Based Threats

- Personal approaches
- Defenses Against Social Engineering Threats
- 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
- Impersonating Orkut, Facebook, MySpace
- Orkut
- Impersonating on Orkut
- MW.Orc worm
- Facebook
- Impersonating on Facebook
- MySpace
- Impersonating on MySpace
- How to Steal Identity
- Comparison
- Original
- Identity Theft
- <http://www.consumer.gov/idtheft/>

Module 12: Phishing

- Phishing
- Introduction
- Reasons for Successful Phishing
- Phishing Methods
- Process of Phishing
- Types of Phishing Attacks
 - Man-in-the-Middle Attacks
 - URL Obfuscation Attacks
 - Cross-site Scripting Attacks
 - Hidden Attacks
 - Client-side Vulnerabilities
 - Deceptive Phishing
 - Malware-Based Phishing
 - DNS-Based Phishing
 - Content-Injection Phishing
 - Search Engine Phishing
- Phishing Statistics: March 2008
- Anti-Phishing
- Anti-Phishing Tools
 - PhishTank SiteChecker
 - NetCraft
 - GFI MailEssentials
 - SpoofGuard
 - Phishing Sweeper Enterprise
 - TrustWatch Toolbar
 - ThreatFire
 - GralicWrap

- Spyware Doctor
- Track Zapper Spyware-Adware Remover
- AdwareInspector
- Email-Tag.com

Module 13: Hacking Email Accounts

- Introduction
 - Introduction
 - Ways for Getting Email Account Information
 - Stealing Cookies
 - Social Engineering
 - Password Phishing
 - Fraudulent e-mail Messages
- Vulnerabilities
 - Web Email
 - Reaper Exploit
- Email Hacking Tools
 - Tool: Advanced Stealth Email Redirector
 - Tool: Mail PassView
 - Tool: Email Password Recovery Master
 - Tool: Mail Password
 - Email Finder Pro
 - Email Spider Easy
 - Kernel Hotmail MSN Password Recovery
 - Retrieve Forgotten Yahoo Password
 - MegaHackerZ
 - Hack Passwords

- Securing Email Accounts
 - Creating Strong Passwords
 - Creating Strong Passwords: Change Password
 - Creating Strong Passwords: Trouble Signing In
 - Sign-in Seal
 - Alternate Email Address
 - Keep Me Signed In/ Remember Me
 - Tool: Email Protector
 - Tool: Email Security
 - Tool: EmailSanitizer
 - Tool: Email Protector
 - Tool: SuperSecret

Module 14: Denial-of-Service

- Real World Scenario of DoS Attacks
- What are Denial-of-Service Attacks
- Goal of DoS
- Impact and the Modes of Attack
- Types of Attacks
- DoS Attack Classification
 - Smurf Attack
 - Buffer Overflow Attack
 - Ping of Death Attack
 - Teardrop Attack
 - SYN Attack
 - SYN Flooding
 - DoS Attack Tools
 - DoS Tool: Jolt2

- DoS Tool: Bubonic.c
- DoS Tool: Land and LaTierra
- DoS Tool: Targa
- DoS Tool: Blast
- DoS Tool: Nemesy
- DoS Tool: Panther2
- DoS Tool: Crazy Pinger
- DoS Tool: SomeTrouble
- DoS Tool: UDP Flood
- DoS Tool: FSMax
- Bot (Derived from the Word RoBOT)
- Botnets
- Uses of Botnets
- Types of Bots
- How Do They Infect? Analysis Of Agabot
- How Do They Infect
- Tool: Nuclear Bot
- What is DDoS Attack
- Characteristics of DDoS Attacks
- Is 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
 - DDoS Tool: Tribal Flood Network

- DDoS Tool: TFN2K
- DDoS Tool: Shaft
- DDoS Tool: Trinity
- DDoS Tool: Knight and Kaiten
- DDoS Tool: Mstream
- 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
- DoSHTTP Tool
- Mitigate or Stop the Effects of DDoS Attacks
- Deflect Attacks
- Post-attack Forensics
- Packet Traceback

Module 15: Session Hijacking

- What is Session Hijacking?
- Understanding Session Hijacking
- Spoofing v Hijacking
- Steps in Session Hijacking
- Types of Session Hijacking
- Session Hijacking Levels
- Network Level Hijacking

- The 3-Way Handshake
- TCP Concepts 3-Way Handshake
- Sequence Numbers
- Sequence Number Prediction
- TCP/IP hijacking
- IP Spoofing: Source Routed Packets
- RST Hijacking
 - RST Hijacking Tool: `hijack_rst.sh`
- Blind Hijacking
- Man in the Middle Attack using Packet Sniffer
- UDP Hijacking
- Application Level Hijacking
- Programs that Performs Session Hacking
 - TTY-Watcher
 - IP watcher
 - Remote TCP Session Reset Utility (SOLARWINDS)
 - Paros HTTP Session Hijacking Tool
 - Dnshijacker Tool
 - Hjksuite Tool
- Dangers Posed by Hijacking
- Protecting against Session Hijacking
- Countermeasure: IPSec

Module 16: Hacking Web Servers

- How Web Servers Work
- How are Web Servers Compromised
- Web Server Defacement

- How are Servers Defaced
- Apache Vulnerability
- Attacks against IIS
 - IIS7 Components
- Unicode
 - Unicode Directory Traversal Vulnerability
 - IIS Directory Traversal (Unicode) Attack
- Hacking Tool
 - Hacking Tool: IISxploit.exe
 - Msw3prt IPP Vulnerability
 - RPC DCOM Vulnerability
 - ASP Trojan
 - IIS Logs
 - Network Tool: Log Analyzer
 - Hacking Tool: CleanIISLog
 - IIS Security Tool: Server Mask
 - ServerMask ip100
 - Tool: CacheRight
 - Tool: CustomError
 - Tool: HttpZip
 - Tool: LinkDeny
 - Tool: ServerDefender AI
 - Tool: ZipEnable
 - Tool: w3compiler
 - Yersinia
- Tool: Metasploit Framework
- KARMA
 - Karmetasploit

- Prerequisites for Karmetasplit
- Running Karmetasplit
- Tool: Immunity CANVAS Professional
- Tool: Core Impact
- Tool: MPack
- Tool: Neosploit
- Patch Management
 - Hotfixes and Patches
 - What is Patch Management
 - Solution: UpdateExpert
 - Patch Management Tool: qfecheck
 - Patch Management Tool: HFNetChk
 - cacls.exe utility
- Vulnerability Scanners
 - Online Vulnerability Search Engine
 - Network Tool: Whisker
 - Network Tool: N-Stealth HTTP Vulnerability Scanner
 - Hacking Tool: WebInspect
 - Network Tool: Shadow Security Scanner
 - Secure IIS
 - ServersCheck Monitoring
 - GFI Network Server Monitor
 - Servers Alive
 - Webserver Stress Tool
 - Monitoring Tool: Secunia PSI
- Countermeasures
- Increasing Web Server Security
- Web Server Protection Checklist

Module 17: Web Application Vulnerabilities

- Web Application
- Web application Hacking
- Anatomy of an Attack
- Web Application Threats
- Cross-Site Scripting/XSS Flaws
 - An Example of XSS
 - Countermeasures
- SQL Injection
- Command Injection Flaws
 - Countermeasures
- Cookie/Session Poisoning
 - Countermeasures
- Parameter/Form Tampering
- Hidden Field at
- 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
 - SiteScope Tool
 - WSDigger Tool – Web Services Testing Tool
 - CookieDigger Tool
 - SSLDigger Tool
 - SiteDigger Tool
 - WindowBomb
 - Burp: Positioning Payloads
 - Burp: Configuring Payloads and Content Enumeration
 - Burp: Password Guessing
 - Burp Proxy
 - Burpsuite
 - Hacking Tool: cURL
 - dotDefender
 - Acunetix Web Scanner
 - AppScan – Web Application Scanner
 - AccessDiver

- Tool: Falcove Web Vulnerability Scanner
- Tool: NetBrute
- Tool: Emsa Web Monitor
- Tool: KeepNI
- Tool: Parosproxy
- Tool: WebScarab
- Tool: Watchfire AppScan
- Tool: WebWatchBot
- Tool: Ratproxy
- Tool: Mapper

Module 18: Web-Based Password Cracking Techniques

- Authentication
 - Authentication - Definition
 - Authentication Mechanisms
 - HTTP Authentication
 - Basic Authentication
 - Digest Authentication
 - Integrated Windows (NTLM) Authentication
 - Negotiate Authentication
 - Certificate-based Authentication
 - Forms-based Authentication
 - RSA SecurID Token
 - Biometrics Authentication
 - Types of Biometrics Authentication
 - Fingerprint-based Identification
 - Hand Geometry- based Identification
 - Retina Scanning

- Afghan Woman Recognized After 17 Years
 - Face Recognition
 - Face Code: WebCam Based Biometrics Authentication System
- Bill Gates at the RSA Conference 2006
- Password Cracking
 - How to Select a Good Password
 - Things to Avoid in Passwords
 - Changing Your Password
 - Protecting Your Password
 - Examples of Bad Passwords
 - The “Mary Had A Little Lamb” Formula
 - How Hackers Get Hold of Passwords
 - Windows XP: Remove Saved Passwords
 - What is a Password Cracker
 - Modus Operandi of an Attacker Using a Password Cracker
 - How Does a Password Cracker Work
 - Attacks - Classification
 - Password Guessing
 - Query String
 - Cookies
 - Dictionary Maker
- Password Cracking Tools
 - Password Crackers Available
 - LophtCrack (LC4)
 - John the Ripper
 - Brutus
 - ObiWaN
 - Authforce

- Hydra
- Cain & Abel
- RAR
- Gammalog
- WebCracker
- Munga Bunga
- PassList
- SnadBoy
- MessenPass
- Wireless WEP Key Password Spy
- RockXP
- Password Spectator Pro
- Passwordstate
- Atomic Mailbox Password Cracker
- Advanced Mailbox Password Recovery (AMBPR)
- Tool: Network Password Recovery
- Tool: Mail PassView
- Tool: Messenger Key
- Tool: SniffPass
- Security Tools
 - WebPassword
 - Password Administrator
 - Password Safe
 - Easy Web Password
 - PassReminder
 - My Password Manager
- Countermeasures

Module 19: SQL Injection

- SQL Injection: Introduction
 - What is SQL Injection
 - Exploiting Web Applications
 - Steps for performing SQL injection
 - What You Should 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
 - BadLogin.aspx.cs
 - BadProductList.aspx.cs
 - 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
 - SQL Injection in Oracle
 - SQL Injection in MySql Database
 - Attacking Against SQL Servers
 - SQL Server Resolution Service (SSRS)
 - Osql -L Probing
- SQL Injection Tools
 - SQL Injection Automated Tools
 - Automated SQL Injection Tool: AutoMagic SQL

- Absinthe Automated SQL Injection Tool
 - Hacking Tool: SQLDict
 - Hacking Tool: SQLExec
 - SQL Server Password Auditing Tool: sqlbf
 - Hacking Tool: SQLSmack
 - Hacking Tool: SQL2.exe
 - sqlmap
 - sqlninja
 - SQLier
 - Automagic SQL Injector
 - Absinthe
- Blind SQL Injection
 - Blind SQL Injection: Countermeasure
- SQL Injection Countermeasures
 - Preventing SQL Injection Attacks
 - GoodLogin.aspx.cs
- SQL Injection Blocking Tool: SQL Block
- Acunetix Web Vulnerability Scanner

Module 20: Hacking Wireless Networks

- Introduction to Wireless Networking
 - Wireless Networking
 - Wired Network vs. Wireless Network
 - Effects of Wireless Attacks on Business
 - Types of Wireless Network
 - Advantages and Disadvantages of a Wireless Network
- Wireless Standards
 - Wireless Standard: 802.11a

- Wireless Standard: 802.11b – “WiFi”
- Wireless Standard: 802.11g
- Wireless Standard: 802.11i
- Wireless Standard: 802.11n
- Wireless Standard: 802.15 (Bluetooth)
- Wireless Standard: 802.16 (WiMax)
 - WiMax Featured Companies
 - WiMax Equipment Vendors
- Wireless Concepts
 - Related Technology and Carrier Networks
 - SSID
 - Is the SSID a Secret
 - Authentication and Association
 - Authentication Modes
 - The 802.1X Authentication Process
 - 802.11 Specific Vulnerabilities
 - Authentication and (Dis) Association Attacks
 - MAC Sniffing and AP Spoofing
 - Defeating MAC Address Filtering in Windows
- Wireless Devices
 - Antennas
 - Cantenna – www.cantenna.com
 - Wireless Access Points
 - Beacon Frames
 - Phone Jammers
 - Phone Jamming Devices
- WEP
 - Wired Equivalent Privacy (WEP)

- WEP Issues
- WEP - Authentication Phase
- WEP - Shared Key Authentication
- WEP - Association Phase
- WEP Flaws
- WPA
 - What is WPA
 - WPA Vulnerabilities
 - WEP, WPA, and WPA2
 - Wi-Fi Protected Access 2 (WPA2)
 - Attacking WPA Encrypted Networks
 - Evil Twin: Attack
- TKIP and LEAP
 - Temporal Key Integrity Protocol (TKIP)
 - Working of TKIP
 - Changes from WEP to TKIP
 - LEAP: The Lightweight Extensible Authentication Protocol
 - LEAP Attacks
 - LEAP Attack Tool: ASLEAP
 - Working of ASLEAP
- Hacking Methods
 - Techniques to Detect Open Wireless Networks
 - Steps for Hacking Wireless Networks
 - Step 1: Find Networks to Attack
 - Step 2: Choose the Network to Attack
 - Step 3: Analyzing the Network
 - Step 4: Cracking the WEP Key
 - Step 5: Sniffing the Network

- Bluejacking
- Super Bluetooth Hack
- Man-in-the-Middle Attack (MITM)
- Denial-of-Service Attacks
- Hijacking and Modifying a Wireless Network
- Cracking WEP
 - 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 Tool: Aircrack
 - Tool: AirPcap
 - Tool: Cain & Abel
 - Scanning Tool: Kismet
- Rogue Access Point
 - 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
 - Airsnarf: A Rogue AP Setup Utility
 - Cloaked Access Point
- Scanning Tools
 - Scanning Tool: Prismstumbler
 - Scanning Tool: MacStumbler
 - Scanning Tool: Mognet

- Scanning Tool: WaveStumbler
- Scanning Tool: Netchaser for Palm Tops
- Scanning Tool: AP Scanner
- Scanning Tool: Wavemon
- Scanning Tool: Wireless Security Auditor (WSA)
- Scanning Tool: AirTraf
- Scanning Tool: WiFi Finder
- Scanning Tool: WifiScanner
- eEye Retina WiFi
- Simple Wireless Scanner
- wlanScanner
- Sniffing Tools
 - Sniffing Tool: AiroPeek
 - Sniffing Tool: NAI Wireless Sniffer
 - MAC Sniffing Tool: WireShark
 - Sniffing Tool: vxSniffer
 - Sniffing Tool: Etherpeg
 - Sniffing Tool: Drifnet
 - Sniffing Tool: AirMagnet
 - Sniffing Tool: WinDump
 - Multiuse Tool: THC-RUT
 - Microsoft Network Monitor
- Wireless Security Tools
 - WLAN Diagnostic Tool: CommView for WiFi PPC
 - WLAN Diagnostic Tool: AirMagnet Handheld Analyzer
 - AirDefense Guard (www.AirDefense.com)
 - Google Secure Access
 - Tool: RogueScanner

Module 21: Physical Security

- Security Facts
- Understanding Physical Security
- Physical Security
- What Is the Need for Physical Security
- Who Is Accountable for Physical Security
- Factors Affecting Physical Security
- Physical Security Checklist
 - Physical Security Checklist -Company surroundings
 - Gates
 - Security Guards
 - Physical Security Checklist: Premises
 - CCTV Cameras
 - Reception
 - Server
 - Workstation Area
 - Wireless Access Point
 - Other Equipments
 - Access Control
 - Biometric Devices
 - Biometric Identification Techniques
 - Biometric Hacking: Biologger
 - Authentication Mechanisms
 - Authentication Mechanism Challenges: Biometrics
 - Faking Fingerprints
 - Smart cards
 - Security Token
 - Computer Equipment Maintenance

- Wiretapping
- Remote Access
- Lapse of Physical Security
- Locks
 - Lock Picking
 - Lock Picking Tools
- Information Security
- EPS (Electronic Physical Security)
- Wireless Security
- Laptop Theft Statistics for 2007
- Statistics for Stolen and Recovered Laptops
- Laptop Theft
- Laptop theft: Data Under Loss
- 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 22: Linux Hacking

- Why Linux
- Linux Distributions
- Linux Live CD-ROMs
- Basic Commands of Linux: Files & Directories
- Linux Basic
 - Linux File Structure
 - Linux Networking Commands
- Directories in Linux
- Installing, Configuring, and Compiling Linux Kernel
- How to Install a Kernel Patch
- Compiling Programs in Linux
- GCC Commands
- Make Files
- Make Install Command
- Linux Vulnerabilities
- Chrooting
- Why is Linux Hacked
- How to Apply Patches to Vulnerable Programs
- Scanning Networks
- Nmap in Linux
- Scanning Tool: Nessus
- Port Scan Detection Tools
- Password Cracking in Linux: John the Ripper
- Firewall in Linux: IPTables
- IPTables Command
- Basic Linux Operating System Defense
- SARA (Security Auditor's Research Assistant)

- Linux Tool: Netcat
- Linux Tool: tcpdump
- Linux Tool: Snort
- Linux Tool: SAINT
- Linux Tool: Wireshark
- Linux Tool: Abacus Port Sentry
- Linux Tool: DSniff Collection
- Linux Tool: Hping2
- Linux Tool: Sniffit
- Linux Tool: Nemesis
- Linux Tool: LSOF
- Linux Tool: IPTraf
- Linux Tool: LIDS
- Hacking Tool: Hunt
- Tool: TCP Wrappers
- Linux Loadable Kernel Modules
- Hacking Tool: Linux Rootkits
- Rootkits: Knark & Torn
- Rootkits: Tuxit, Adore, Ramen
- Rootkit: Beastkit
- Rootkit Countermeasures
- *'chkrootkit'* detects the following Rootkits
- Linux Tools: Application Security
- Advanced Intrusion Detection Environment (AIDE)
- Linux Tools: Security Testing Tools
- Linux Tools: Encryption
- Linux Tools: Log and Traffic Monitors
- Linux Security Auditing Tool (LSAT)

- Linux Security Countermeasures
- Steps for Hardening Linux

Module 23: Evading IDS, Firewalls and Detecting Honey Pots

- Introduction to Intrusion Detection System
 - Terminologies
 - Intrusion Detection System (IDS)
 - IDS Placement
 - Ways to Detect an Intrusion
 - Types of Instruction Detection Systems
 - System Integrity Verifiers (SIVS)
 - Tripwire
 - Cisco Security Agent (CSA)
 - True/False, Positive/Negative
 - Signature Analysis
 - General Indications of System Intrusions
 - General Indications of File System Intrusions
 - General Indication of Network Intrusions
 - Intrusion Detection Tools
 - Snort
 - Running Snort on Windows 2003
 - Snort Console
 - Testing Snort
 - Configuring Snort (snort.conf)
 - Snort Rules
 - Set up Snort to Log to the Event Logs and to Run as a Service
 - Using EventTriggers.exe for Eventlog Notifications

- SnortSam
- 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
- Intrusion Prevention System
 - Intrusion Prevention Strategies
 - IPS Deployment Risks
 - Types of IPS
 - Host Based IPS (HIPS)
 - Network Based IPS (NIPS)
 - Content Based IPS (CIPS)
 - Rate Based IPS (RIPS)
 - Information Flow in IDS and IPS
 - IDS vs. IPS
 - IPS Vendors and Products
- 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 Firewall
 - 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
- Packet Filtering Firewall
- Firewall Identification
- Firewalking
- Banner Grabbing
- Breaching Firewalls
- Bypassing a Firewall using HTTP Tunnel
- Placing Backdoors through Firewalls
- Hiding Behind a Covert Channel: LOKI
- Tool: NCovert
- ACK Tunneling
- Tools to breach firewalls
- Common Tool for Testing Firewall and IDS
 - IDS Testing Tool: Traffic IQ Professional
 - IDS Tool: Next-Generation Intrusion Detection Expert System (NIDES)
 - IDS Tool: SecureHost
 - IDS Tool: Snare
 - IDS Testing Tool: TCPOpera
 - IDS testing tool: Firewall Informer
 - Atelier Web Firewall Tester
- What is Honeygot?
 - The Honeygot Project
 - Types of Honeygot

- Low-interaction honeypot
- Medium-interaction honeypot
- High-interaction honeypot
- Advantages and Disadvantages of a Honeypot
- Where to place Honeypots
- Honeypots
 - Honeypot-SPECTER
 - Honeypot - honeyd
 - Honeypot – KFSensor
 - Sebek
- Physical and Virtual Honeypots
- Tools to Detect Honeypots
- What to do when hacked

Module 24: Buffer Overflows

- Buffer Overflow Concepts
 - Why are Programs/Applications Vulnerable
 - Buffer Overflows
 - Reasons for Buffer Overflow Attacks
 - Knowledge Required to Program Buffer Overflow Exploits
 - Understanding Stacks
 - Understanding Heaps
 - Types of Buffer Overflows: Stack-based Buffer Overflow
 - Types of Buffer Overflows: Heap-Based Buffer Overflow
 - Understanding Assembly Language
 - Shellcode
- Attacking a Real Program
- NOPs

- How to Mutate a Buffer Overflow Exploit
- Once the Stack is Smashed
- Examples of Buffer Overflow
 - Simple Uncontrolled Overflow of the Stack
 - Heap Memory Buffer Overflow Bug
 - Simple Buffer Overflow in C
 - Code Analysis
- **Tools**
 - Tool to Defend Buffer Overflow: Return Address Defender (RAD)
 - Tool to Defend Buffer Overflow: StackGuard
 - Insure++
 - Comodo Memory Firewall
 - DefencePlus
 - BufferShield
 - Hardware Level Prevention Of Buffer Overflow
- How to Detect Buffer Overflows in a Program
- Defense Against Buffer Overflows

Module 25: Cryptography

- Public-key Cryptography
- Working of Encryption
- Digital Signature
- RSA (Rivest Shamir Adleman)
 - Example of RSA Algorithm
- 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
- Government Access to Keys (GAK)
- RSA Challenge
- distributed.net
- Code Breaking: Methodologies
- Cryptography Attacks
- Disk Encryption
- Magic Lantern
- WEPCrack
- Cracking S/MIME Encryption Using Idle CPU Time
- Cryptography Tools
 - Cleversafe Grid Builder
 - PGP (Pretty Good Privacy)
 - CypherCalc
 - Command Line Scriptor
 - CryptoHeaven
 - Microsoft Cryptography Tools

Module 26: Penetration Testing

- Introduction to Penetration Testing (PT)
- Categories of security assessments
- Vulnerability Assessment

- Limitations of Vulnerability Assessment
- Testing
 - Penetration Testing
 - 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
- Penetration Testing Tools
 - Pentest using Appscan
 - HackerShield
 - Pen-Test Using Cerberus Internet Scanner
 - Pen-Test Using Cybercop Scanner
 - Pen-Test Using FoundScan Hardware Appliances
 - Pen-Test Using Nessus
 - Pen-Test Using NetRecon
 - Pen-Test Using SAINT

- Pen-Test Using SecureNet Pro
- Pen-Test Using SecureScan
- Pen-Test Using SATAN, SARA and Security Analyzer
- Pen-Test Using STAT Analyzer
- Pentest Using VigilENT
- Pentest Using WebInspect
- Pentest Using CredDigger
- Pentest Using Nsauditor
- Evaluating Different Types of Pen-Test Tools
- Asset Audit
- Fault Tree and Attack Trees
- GAP Analysis
- Threat
 - Business Impact of Threat
 - Internal Metrics Threat
 - External Metrics Threat
 - Calculating Relative Criticality
 - Test Dependencies
- Other Tools Useful in Pen-Test
 - Defect Tracking Tools: Bug Tracker Server
 - Disk Replication Tools
 - DNS Zone Transfer Testing Tools
 - Network Auditing Tools
 - Trace Route Tools and Services
 - Network Sniffing Tools
 - Denial of Service Emulation Tools
 - Traditional Load Testing Tools
 - System Software Assessment Tools

- Operating System Protection Tools
- Fingerprinting Tools
- Port Scanning Tools
- Directory and File Access Control Tools
- File Share Scanning Tools
- Password Directories
- Password Guessing Tools
- Link Checking Tools
- Web-Testing Based Scripting tools
- Buffer Overflow protection Tools
- File Encryption Tools
- Database Assessment Tools
- Keyboard Logging and Screen Reordering Tools
- System Event Logging and Reviewing Tools
- Tripwire and Checksum Tools
- Mobile-code Scanning Tools
- Centralized Security Monitoring Tools
- Web Log Analysis Tools
- Forensic Data and Collection Tools
- Security Assessment Tools
- Multiple OS Management Tools
- Phases of Penetration Testing
- Pre-attack Phase
- Best Practices
- Results that can be Expected
- Passive Reconnaissance
- Active Reconnaissance
- Attack Phase

- Activity: Perimeter Testing
- Activity: Web Application Testing
- Activity: Wireless Testing
- Activity: Acquiring Target
- Activity: Escalating Privileges
- Activity: Execute, Implant and Retract
- Post Attack Phase and Activities
- Penetration Testing Deliverables Templates

Module 27: 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
- Standard Direct Connection
- Reverse Shell (Reverse Telnet)
- Direct Attack Example
- In-Direct Attack Example
- Reverse Connecting Agents
- Covert Channel Attack Tools
 - Netcat
 - DNS Tunneling
 - Covert Channel Using DNS Tunneling

- DNS Tunnel Client
- DNS Tunneling Countermeasures
- 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
 - Ncovert - How it works
- Covert Channel Hacking via Spam E-mail Messages
- Hydan

Module 28: 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
 - Virus Infection: Step I
 - Directory Traversal Method
 - Example Directory Traversal Function
 - “dot dot” Method
 - Example Code for a “dot dot” Method
 - Virus Infection: Step II

- Virus Infection: Step III
 - Marking a File for Infection
- Virus Infection: Step IV
- Virus Infection: Step V
- Components of Viruses
 - Functioning of Replicator part
 - Writing Replicator
 - Writing Concealer
 - Dispatcher
 - Writing Bomb/Payload
 - Trigger Mechanism
 - Bombs/Payloads
 - Brute Force Logic Bombs
- Testing Virus Codes
- Tips for Better Virus Writing

Module 29: Assembly Language Tutorial

- Base 10 System
- Base 2 System
- Decimal 0 to 15 in Binary
- Binary Addition (C stands for Canary)
- 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

Module 30: 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

Module 31: 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

Module 32: 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

Module 33: 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

Module 34: Macintosh Hacking

- Introduction to MAC OS
- Vulnerabilities in MAC
 - Buffer Overflow Vulnerability
 - Local Privilege Escalation Vulnerabilities

- DiskManagement BOM Local Privilege Escalation Vulnerability
- HFS+ do_hfs_truncate() Denial of Service Vulnerability
- ATPsndrsp() Heap Buffer Overflow Vulnerability
- UFS ufs_lookup() Denial of Service Vulnerability
- Other Vulnerabilities in MAC
- How a Malformed Installer Package Can Crack Mac OS X
- Worm and Viruses in MAC
 - OSX/Leap-A
 - Inqtana.A
 - Macro Viruses
- MAC OS X Trojans
 - Termite
 - Sub7ME
 - WinJack
 - Xover
 - Hell Raiser 2.5b
- Anti-Viruses in MAC
 - VirusBarrier
 - McAfee Virex for Macintosh
 - Sophos Endpoint Security and Control
 - Norton Internet Security
- Mac Security Tools
 - MacScan
 - ClamXav
 - IPNetsentryx
 - FileGuard
- Countermeasures

Module 35: Hacking Routers, cable Modems and Firewalls

- Network Devices
- Identifying a Router
 - SING: Tool for Identifying the Router
- HTTP Configuration Arbitrary Administrative Access Vulnerability
- ADMSnmp
- Solarwinds MIB Browser
- Brute-Forcing Login Services
- Hydra
- Analyzing the Router Config
- Cracking the Enable Password
- Tool: Cain and Abel
- Implications of a Router Attack
- Types of Router Attacks
- Router Attack Topology
- Denial of Service (DoS) Attacks
- Packet “Mistreating” Attacks
- Routing Table Poisoning
- Hit-and-run Attacks vs. Persistent Attacks
- Cisco Router
 - Finding a Cisco Router
 - How to Get into Cisco Router
 - Breaking the Password
 - Is Anyone Here
 - Covering Tracks
 - Looking Around
- Eigrp-tool

- Tool: Zebra
- Tool: Yersinia for HSRP, CDP, and other layer 2 attacks
- Tool: Cisco Torch
- Monitoring SMTP(port25) Using SLcheck
- Monitoring HTTP(port 80)
- Cable Modem Hacking
 - OneStep: ZUP
- www.bypassfirewalls.net
- Waldo Beta 0.7 (b)

Module 36: Hacking Mobile Phones, PDA and Handheld Devices

- Different OS in Mobile Phone
- Different OS Structure in Mobile Phone
- Evolution of Mobile Threat
- Threats
- What Can A Hacker Do
- Vulnerabilities in Different Mobile Phones
- Malware
 - Spyware: SymbOS/Htool-SMSSender.A.intd
 - Spyware: SymbOS/MultiDropper.CG
 - Best Practices against Malware
- Blackberry
 - Blackberry Attacks
 - Blackberry Attacks: Blackjacking
 - BlackBerry Wireless Security
 - BlackBerry Signing Authority Tool

- Countermeasures
- PDA
 - PDA Security Issues
 - ActiveSync attacks
 - HotSync Attack
 - PDA Virus: Brador
 - PDA Security Tools: TigerSuite PDA
 - Security Policies for PDAs
- iPod
 - Misuse of iPod
 - Jailbreaking
 - Tool for Jailbreaking: iDemocracy
 - Tool for Jailbreaking: iActivator
 - Tool for Jailbreaking: iNdependence
 - Tools for jailbreaking: iFuntastic
 - Prerequisite for iPhone Hacking
 - Step by Step iPhone Hacking using iFuntastic
 - Step by step iPhone Hacking
 - AppSnapp
 - Steps for AppSnapp
 - Tool to Unlock iPhone: iPhoneSimFree
 - Tool to Unlock iPhone: anySIM
 - Steps for Unlocking your iPhone using AnySIM
 - Activate the Voicemail Button on your Unlocked iPhone
 - Podloso Virus
 - Security tool: Icon Lock-iT XP
- Mobile: Is It a Breach to Enterprise Security?
 - Threats to Organizations Due to Mobile Devices

- Security Actions by Organizations
- Viruses
 - Skulls
 - Duts
 - Doomboot.A: Trojan
- Antivirus
 - Kaspersky Antivirus Mobile
 - Airscanner
 - BitDefender Mobile Security
 - SMobile VirusGuard
 - Symantec AntiVirus
 - F-Secure Antivirus for Palm OS
 - BullGuard Mobile Antivirus
- Security Tools
 - Sprite Terminator
 - Mobile Security Tools: Virus Scan Mobile
- Defending Cell Phones and PDAs Against Attack
- Mobile Phone Security Tips

Module 37: Bluetooth Hacking

- Bluetooth Introduction
- Security Issues in Bluetooth
- Security Attacks in Bluetooth Devices
 - Bluejacking
 - Tools for Bluejacking
 - BlueSpam
 - Blue snarfing

- BlueBug Attack
- Short Pairing Code Attacks
- Man-In-Middle Attacks
- OnLine PIN Cracking Attack
- BTKeylogging attack
- BTVoiceBugging attack
- Blueprinting
- Bluesmacking - The Ping of Death
- Denial-of-Service Attack
- BlueDump Attack
- Bluetooth hacking tools
 - BTScanner
 - Bluesnarfer
 - Bluediving
 - Transient Bluetooth Environment Auditor
 - BTcrack
 - Blooover
 - Hidattack
- Bluetooth Viruses and Worms
 - Cabir
 - Mabir
 - Lasco
- Bluetooth Security tools
 - BlueWatch
 - BlueSweep
 - Bluekey
 - BlueFire Mobile Security Enterprise Edition
 - BlueAuditor

- Bluetooth Network Scanner
- Countermeasures

Module 38: VoIP Hacking

- What is VoIP
- VoIP Hacking Steps
- Footprinting
 - Information Sources
 - Unearthing Information
 - Organizational Structure and Corporate Locations
 - Help Desk
 - Job Listings
 - Phone Numbers and Extensions
 - VoIP Vendors
 - Resumes
 - WHOIS and DNS Analysis
 - Steps to Perform Footprinting
- Scanning
 - Host/Device Discovery
 - ICMP Ping Sweeps
 - ARP Pings
 - TCP Ping Scans
 - SNMP Sweeps
 - Port Scanning and Service Discovery
 - TCP SYN Scan
 - UDP Scan
 - Host/Device Identification
- Enumeration

- Steps to Perform Enumeration
- Banner Grabbing with Netcat
- SIP User/Extension Enumeration
 - REGISTER Username Enumeration
 - INVITE Username Enumeration
 - OPTIONS Username Enumeration
 - Automated OPTIONS Scanning with sipsak
 - Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN against SIP server
 - Automated OPTIONS Scanning Using SIPSCAN against SIP Phones
- Enumerating TFTP Servers
- SNMP Enumeration
- Enumerating VxWorks VoIP Devices
- Steps to Exploit the Network
 - Denial-of-Service (DoS)
 - Distributed Denial-of-Service (DDoS) Attack
 - Internal Denial-of-Service Attack
 - DoS Attack Scenarios
 - Eavesdropping
 - Packet Spoofing and Masquerading
 - Replay Attack
 - Call Redirection and Hijacking
 - ARP Spoofing
 - ARP Spoofing Attack
 - Service Interception
 - H.323-Specific Attacks
 - SIP Security Vulnerabilities
 - SIP Attacks

- Flooding Attacks
- DNS Cache Poisoning
- Sniffing TFTP Configuration File Transfers
- Performing Number Harvesting and Call Pattern Tracking
- Call Eavesdropping
- Interception through VoIP Signaling Manipulation
- Man-In-The-Middle (MITM) Attack
- Application-Level Interception Techniques
 - How to Insert Rogue Application
 - SIP Rogue Application
 - Listening to/Recording Calls
 - Replacing/Mixing Audio
 - Dropping Calls with a Rogue SIP Proxy
 - Randomly Redirect Calls with a Rogue SIP Proxy
 - Additional Attacks with a Rogue SIP Proxy
- What is Fuzzing
 - Why Fuzzing
 - Commercial VoIP Fuzzing tools
- Signaling and Media Manipulation
 - Registration Removal with erase_registrations Tool
 - Registration Addition with add_registrations Tool
- VoIP Phishing
- Covering Tracks

Module 39: RFID Hacking

- RFID- Definition
- Components of RFID Systems
- RFID Collisions

- RFID Risks
 - Business Process Risk
 - Business Intelligence Risk
 - Privacy Risk
 - Externality Risk
 - Hazards of Electromagnetic Radiation
 - Computer Network Attacks
- RFID and Privacy Issues
- Countermeasures
- RFID Security and Privacy Threats
 - Sniffing
 - Tracking
 - Spoofing
 - Replay attacks
 - Denial-of-service
- Protection Against RFID Attacks
- RFID Guardian
- RFID Malware
 - How to Write an RFID Virus
 - How to Write an RFID Worm
 - Defending Against RFID Malware
- RFID Exploits
- Vulnerabilities in RFID-enabled Credit Cards
 - Skimming Attack
 - Replay Attack
 - Eavesdropping Attack
- RFID Hacking Tool: RFDump
- RFID Security Controls

- Management Controls
- Operational Controls
- Technical Controls
- RFID Security

Module 40: Spamming

- Introduction
- Techniques used by Spammers
- How Spamming is performed
- Ways of Spamming
- Spammer: Statistics
- Worsen ISP: Statistics
- Top Spam Effected Countries: Statistics
- Types of Spam Attacks
- Spamming Tools
 - Farelogic Worldcast
 - 123 Hidden Sender
 - YL Mail Man
 - Sendblaster
 - Direct Sender
 - Hotmailer
 - PackPal Bulk Email Server
 - IEmailer
- Anti-Spam Techniques
- Anti- Spamming Tools
 - AEVITA Stop SPAM Email
 - SpamExperts Desktop
 - SpamEater Pro

- SpamWeasel
- Spytech SpamAgent
- AntispamSniper
- Spam Reader Spam Assassin Proxy (SA) Proxy
- MailWasher Free
- Spam Bully
- Countermeasures

Module 41: Hacking USB Devices

- Introduction to USB Devices
- Electrical Attack
- Software Attack
- USB Attack on Windows
- Viruses and Worms
 - W32/Madang-Fam
 - W32/Hasnot-A
 - W32/Fujacks-AK
 - W32/Fujacks-E
 - W32/Dzan-C
 - W32/SillyFD-AA
 - W32/SillyFDC-BK
 - W32/LiarVB-A
 - W32/Hairy-A
 - W32/QRRob-ADN
 - W32/VBAut-B
 - HTTP W32.Drom
- Hacking Tools
 - USB Dumper

- USB Switchblade
- USB Hacksaw
- USB Security Tools
 - MyUSBonly
 - USBDeview
 - USB-Blocker
 - USB CopyNotify
 - Remora USB File Guard
 - Advanced USB Pro Monitor
 - Folder Password Expert USB
 - USBlyzer
 - USB PC Lock Pro
 - Torpark
 - Virus Chaser USB
- Countermeasures

Module 42: Hacking Database Servers

- Hacking Database server: Introduction
- Hacking Oracle Database Server
 - Attacking Oracle
 - Security Issues in Oracle
 - Types of Database Attacks
 - How to Break into an Oracle Database and Gain DBA Privileges
 - Oracle Worm: Voyager Beta
 - Ten Hacker Tricks to Exploit SQL Server Systems
- Hacking SQL Server
 - How SQL Server is Hacked
 - Query Analyzer

- odbcping Utility
- Tool: ASPRunner Professional
- Tool: FlexTracer
- Security Tools
- SQL Server Security Best Practices: Administrator Checklist
- SQL Server Security Best Practices: Developer Checklist

Module 43: Cyber Warfare- Hacking, Al-Qaida and Terrorism

- Cyber Terrorism Over Internet
- Cyber-Warfare Attacks
- 45 Muslim Doctors Planned US Terror Raids
- Net Attack
- Al-Qaeda
- Why Terrorists Use Cyber Techniques
- Cyber Support to Terrorist Operations
- Planning
- Recruitment
- Research
- Propaganda
- Propaganda: Hizballah Website
- Cyber Threat to the Military
- Russia 'hired botnets' for Estonia Cyber-War
- NATO Threatens War with Russia
- Bush on Cyber War: 'a subject I can learn a lot about'
- E.U. Urged to Launch Coordinated Effort Against Cybercrime
- Budget: Eye on Cyber-Terrorism Attacks
- Cyber Terror Threat is Growing, Says Reid
- Terror Web 2.0

- Table 1: How Websites Support Objectives of terrorist/Extremist Groups
- Electronic Jihad
- Electronic Jihad' App Offers Cyber Terrorism for the Masses
- Cyber Jihad – Cyber Firesale
- <http://internet-haganah.com/haganah/>

Module 44: Internet Content Filtering Techniques

- Introduction to Internet Filter
 - Key Features of Internet Filters
 - Pros and Cons of Internet Filters
- Internet Content Filtering Tools
 - iProtectYou
 - Tool: Block Porn
 - Tool: FilterGate
 - Tool: Adblock
 - Tool: AdSubtract
 - Tool: GalaxySpy
 - Tool: AdsGone Pop Up Killer
 - Tool: AntiPopUp
 - Tool: Pop Up Police
 - Tool: Super Ad Blocker
 - Tool: Anti-AD Guard
 - Net Nanny
 - CyberSieve
 - BSafe Internet Filter
 - Tool: Stop-the-Pop-Up Lite
 - Tool: WebCleaner
 - Tool: AdCleaner

- Tool: Adult Photo Blanker
- Tool: LiveMark Family
- Tool: KDT Site Blocker
- Internet Safety Guidelines for Children

Module 45: Privacy on the Internet

- Internet privacy
- Proxy privacy
- Spyware privacy
- Email privacy
- Cookies
- Examining Information in Cookies
- How Internet Cookies Work
- How Google Stores Personal Information
- Google Privacy Policy
- Web Browsers
- Web Bugs
- Downloading Freeware
- Internet Relay Chat
- Pros and Cons of Internet Relay Chat
- Electronic Commerce
- Internet Privacy Tools: Anonymizers
 - Anonymizer Anonymous Surfing
 - Anonymizer Total Net Shield
 - Anonymizer Nyms
 - Anonymizer Anti-Spyware
 - Anonymizer Digital Shredder Lite
 - Steganos Internet Anonym

- Invisible IP Map
- NetConceal Anonymity Shield
- Anonymous Guest
- ViewShield
- IP Hider
- Mask Surf Standard
- VIP Anonymity
- SmartHide
- Anonymity Gateway
- Hide My IP
- Claros Anonymity
- Max Internet Optimizer
- Hotspot Shield
- Anonymous Browsing Toolbar
- Invisible Browsing
- Real Time Cleaner
- Anonymous Web Surfing
- Anonymous Friend
- Easy Hide IP
- Internet Privacy Tools: Firewall Tools
 - Agnitum firewall
 - Firestarter
 - Sunbelt Personal Firewall
 - Netdefender
- Internet Privacy Tools: Others
 - Privacy Eraser
 - CookieCop
 - Cookiepal

- Historykill
- Tracks eraser
- Best Practices
 - Protecting Search Privacy
 - Tips for Internet Privacy
- Counter measures

Module 46: Securing Laptop Computers

- Statistics for Stolen and Recovered Laptops
- Statistics on Security
- Percentage of Organizations Following the Security Measures
- Laptop threats
- Laptop Theft
- Fingerprint Reader
- Protecting Laptops Through Face Recognition
- Bluetooth in Laptops
- Tools
 - Laptop Security
 - Laptop Security Tools
 - Laptop Alarm
 - Flexysafe
 - Master Lock
 - eToken
 - STOP-Lock
 - True Crypt
 - PAL PC Tracker
 - Cryptex
 - Dekart Private Disk Multifactor

- Laptop Anti-Theft
- Inspice Trace
- ZTRACE GOLD
- SecureTrieve Pro
- XTool Laptop Tracker
- XTool Encrypted Disk
- XTool Asset Auditor
- XTool Remote Delete
- Securing from Physical Laptop Thefts
- Hardware Security for Laptops
- Protecting the Sensitive Data
- Preventing Laptop Communications from Wireless Threats
- Protecting the Stolen Laptops from Being Used
- Security Tips

Module 47: Spying Technologies

- Spying
- Motives of Spying
- Spying Devices
 - Spying Using Cams
 - Video Spy
 - Video Spy Devices
 - Tiny Spy Video Cams
 - Underwater Video Camera
 - Camera Spy Devices
 - Goggle Spy
 - Watch Spy
 - Pen Spy

- Binoculars Spy
- Toy Spy
- Spy Helicopter
- Wireless Spy Camera
- Spy Kit
- Spy Scope: Spy Telescope and Microscope
- Spy Eye Side Telescope
- Audio Spy Devices
- Eavesdropper Listening Device
- GPS Devices
- Spy Detectors
- Spy Detector Devices
- Vendors Hosting Spy Devices
 - Spy Gadgets
 - Spy Tools Directory
 - Amazon.com
 - Spy Associates
 - Paramountzone
 - Surveillance Protection
- Spying Tools
 - Net Spy Pro-Computer Network Monitoring and Protection
 - SpyBoss Pro
 - CyberSpy
 - Spytech SpyAgent
 - ID Computer Spy
 - e-Surveiller
 - KGB Spy Software
 - O&K Work Spy

- WebCam Spy
- Golden Eye
- Anti-Spying Tools
 - Internet Spy Filter
 - Spybot - S&D
 - SpyCop
 - Spyware Terminator
 - XoftSpySE

Module 48: Corporate Espionage- Hacking Using Insiders

- Introduction To Corporate Espionage
- Information Corporate Spies Seek
- Insider Threat
- Different Categories of Insider Threat
- Privileged Access
- Driving Force behind Insider Attack
- Common Attacks carried out by Insiders
- Techniques Used for Corporate Espionage
- Process of Hacking
- Former Forbes Employee Pleads Guilty
- Former Employees Abet Stealing Trade Secrets
- California Man Sentenced For Hacking
- Federal Employee Sentenced for Hacking
- Facts
- Key Findings from U.S Secret Service and CERT Coordination Center/SEI study on Insider Threat
- Tools
 - NetVizor

- Privatefirewall w/Pest Patrol
- Countermeasures
 - Best Practices against Insider Threat
 - Countermeasures

Module 49: Creating Security Policies

- Security policies
- Key Elements of Security Policy
- Defining the Purpose and Goals of Security Policy
- Role of Security Policy
- Classification of Security Policy
- Design of Security Policy
- Contents of Security Policy
- Configurations of Security Policy
- Implementing Security Policies
- Types of Security Policies
 - Promiscuous Policy
 - Permissive Policy
 - Prudent Policy
 - Paranoid Policy
 - Acceptable-Use Policy
 - User-Account Policy
 - Remote-Access Policy
 - Information-Protection Policy
 - Firewall-Management Policy
 - Special-Access Policy
 - Network-Connection Policy
 - Business-Partner Policy

- Other Important Policies
- Policy Statements
- Basic Document Set of Information Security Policies
- E-mail Security Policy
 - Best Practices for Creating E-mail Security Policies
 - User Identification and Passwords Policy
- Software Security Policy
- Software License Policy
- Points to Remember While Writing a Security Policy
- Sample Policies
 - Remote Access Policy
 - Wireless Security Policy
 - E-mail Security Policy
 - E-mail and Internet Usage Policies
 - Personal Computer Acceptable Use Policy
 - Firewall Management policy
 - Internet Acceptable Use Policy
 - User Identification and Password Policy
 - Software License Policy

Module 50: Software Piracy and Warez

- Software Activation: Introduction
 - Process of Software Activation
- Piracy
 - Piracy Over Internet
 - Abusive Copies
 - Pirated Copies
 - Cracked Copies

- Impacts of piracy
- Software Piracy Rate in 2006
- Piracy Blocking
- Software Copy Protection Backgrounders
 - CD Key Numbers
 - Dongles
 - Media Limited Installations
 - Protected Media
 - Hidden Serial Numbers
 - Digital Right Management (DRM)
 - Copy protection for DVD
- Warez
 - Warez
 - Types of Warez
 - Warez Distribution
 - Distribution Methods
- Tool: Crypkey
- Tool: EnTrial
- EnTrial Tool: Distribution File
- EnTrial Tool: Product & Package Initialization Dialog
- EnTrial Tool: Add Package GUI
- Tool: DF_ProtectionKit
- Tool: Crack Killer
- Tool: Logic Protect
- Tool: Software License Manager
- Tool: Quick License Manager
- Tool: WTM CD Protect

Module 51: Hacking and Cheating Online Games

- Online Games
- Basics of Game Hacking
- Online Gaming Exploits
- Types of Exploits
- Online Gaming Risks
- Threats in Online Gaming
- Online Gaming Theft
- How Passwords for Online Games are Stolen
- Social Engineering and Phishing
- An Example of a Phishing Email
- Exploiting Game Server Vulnerabilities
- Vulnerability in-game chat in Lineage 2
- Using Malware
- Malicious Programs and Malware
- Email-Worm.Win32.Lewor.a
- Part of a file infected by Virus.Win32.Alman.a
- Online Gaming Malware from 1997-2007
- How Modern Attacks are Conducted
- Geographical Considerations
- Statistics
- Best Practices for Secure Online Gaming

Module 52: Hacking RSS and Atom

- Introduction
- Areas Where RSS and Atom is Used
- Building a Feed Aggregator
- Routing Feeds to the Email Inbox

- Monitoring the Server with Feeds
- Tracking Changes in Open Source Projects
- Risks by Zone
 - Remote Zone risk
 - Local Zone Risk
- Reader Specific Risks
- Utilizing the Web Feeds Vulnerabilities
- Example for Attacker to Attack the Feeds
- Tools
 - Perseptio FeedAgent
 - RssFeedEater
 - Thingamablog
 - RSS Builder
 - RSS Submit
 - FeedDemon
 - FeedForAll
 - FeedExpress
 - RSS and Atom Security

Module 53: Hacking Web Browsers

- Introduction
- How Web Browsers Work
- How Web Browsers Access HTML Documents
- Protocols for an URL
- Hacking Firefox
 - Firefox Proof of Concept Information Leak Vulnerability
 - Firefox Spoofing Vulnerability
 - Password Vulnerability

- Concerns With Saving Form Or Login Data
- Cleaning Up Browsing History
- Cookies
- Internet History Viewer: Cookie Viewer
- Firefox Security
 - Blocking Cookies Options
 - Tools For Cleaning Unwanted Cookies
 - Tool: CookieCuller
 - Getting Started
 - Privacy Settings
 - Security Settings
 - Content Settings
 - Clear Private Data
 - Mozilla Firefox Security Features
- Hacking Internet Explorer
 - Redirection Information Disclosure Vulnerability
 - Window Injection Vulnerability
- Internet Explorer Security
 - Getting Started
 - Security Zones
 - Custom Level
 - Trusted Sites Zone
 - Privacy
 - Overwrite Automatic Cookie Handling
 - Per Site Privacy Actions
 - Specify Default Applications
 - Internet Explorer Security Features
- Hacking Opera

- JavaScript Invalid Pointer Vulnerability
- BitTorrent Header Parsing Vulnerability
- Torrent File Handling Buffer Overflow Vulnerability
- Security Features of Opera
 - Security and Privacy Features
- Hacking Safari
 - Safari Browser Vulnerability
 - iPhone Safari Browser Memory Exhaustion Remote Dos Vulnerability
- Securing Safari
 - Getting started
 - Preferences
 - AutoFill
 - Security Features
- Hacking Netscape
 - Netscape Navigator Improperly Validates SSL Sessions
 - Netscape Navigator Security Vulnerability
- Securing Netscape
 - Getting Started
 - Privacy Settings
 - Security Settings
 - Content Settings
 - Clear Private Data

Module 54: Proxy Server Technologies

- Introduction: Proxy Server
- Working of Proxy Server
- Types of Proxy Server
- Socks Proxy

- Free Proxy Servers
- Use of Proxies for Attack
- Tools
 - WinGate
 - UserGate Proxy Server
 - Advanced FTP Proxy Server
 - Trilent FTP Proxy
 - SafeSquid
 - AllegroSurf
 - ezProxy
 - Proxy Workbench
 - ProxyManager Tool
 - Super Proxy Helper Tool
 - MultiProxy
- How Does MultiProxy Work
- TOR Proxy Chaining Software
- TOR Proxy Chaining Software
- AnalogX Proxy
- NetProxy
- Proxy+
- ProxySwitcher Lite
- Tool: JAP
- Proxomitron
- SSL Proxy Tool
- How to Run SSL Proxy

Module 55: Data Loss Prevention

- Introduction: Data Loss
- Causes of Data Loss
- How to Prevent Data Loss
- Impact Assessment for Data Loss Prevention
- Tools
 - Security Platform
 - Check Point Software: Pointsec Data Security
 - Cisco (IronPort)
 - Content Inspection Appliance
 - CrossRoads Systems: DBProtector
 - Strongbox DBProtector Architecture
 - DeviceWall
 - Exeros Discovery
 - GFi Software: GFiEndPointSecurity
 - GuardianEdge Data Protection Platform
 - ProCurve Identity Driven Manager (IDM)
 - Imperva: SecureSphere
 - MailMarshal
 - WebMarshal
 - Marshal EndPoint
 - Novell ZENworks Endpoint Security Management
 - Prism EventTracker
 - Proofpoint Messaging Security Gateway
 - Proofpoint Platform Architecture
 - Summary Dashboard
 - End-user Safe/Block List
 - Defiance Data Protection System

- Sentrigo: Hedgehog
- Symantec Database Security
- Varonis: DataPrivilege
- Verdasys: Digital Guardian
- VolumeShield AntiCopy
- Websense Content Protection Suite

Module 56: Hacking Global Positioning System (GPS)

- Global Positioning System (GPS)
- Terminologies
- GPS Devices Manufacturers
- Gpsd-GPS Service Daemon
- Sharing Waypoints
- Wardriving
- Areas of Concern
- Sources of GPS Signal Errors
- Methods to Mitigate Signal Loss
- GPS Secrets
 - GPS Hidden Secrets
 - Secret Startup Commands in Garmin
 - Hard Reset/ Soft Reset
- Firmware Hacking
 - Firmware
 - Hacking GPS Firmware: Bypassing the Garmin eTrex Vista Startup Screen
 - Hacking GPS Firmware: Bypassing the Garmin eTrex Legend Startup Screen
 - Hacking GPS Firmware: Bypassing the Garmin eTrex Venture Startup Screen
- GPS Tools
 - Tool: GPS NMEA LOG

- Tool: GPS Diagnostic
- Tool: RECSIM III
- Tool: G7toWin
- Tool: G7toCE
- Tool: GPS Security Guard
- GPS Security Guard Functions
- UberTracker

Module 57: Computer Forensics and Incident Handling

- Computer Forensics
 - What is Computer Forensics
 - Need for Computer Forensics
 - Objectives of Computer Forensics
 - Stages of Forensic Investigation in Tracking Cyber Criminals
 - Key Steps in Forensic Investigations
 - List of Computer Forensics Tools
- Incident Handling
 - Present Networking Scenario
 - What is an Incident
 - Category of Incidents: Low Level
 - Category of Incidents: Mid Level
 - Category of Incidents: High Level
 - How to Identify an Incident
 - How to Prevent an Incident
 - Defining the Relationship between Incident Response, Incident Handling, and Incident Management
 - Incident Response Checklist
 - Handling Incidents

- Procedure for Handling Incident
 - Stage 1: Preparation
 - Stage 2: Identification
 - Stage 3: Containment
 - Stage 4: Eradication
 - Stage 5: Recovery
 - Stage 6: Follow-up
- Incident Management
- Why don't Organizations Report Computer Crimes
- Estimating Cost of an Incident
- Whom to Report an Incident
- Incident Reporting
- Vulnerability Resources
- What is CSIRT
 - CSIRT: Goals and Strategy
 - Why an Organization needs an Incident Response Team
 - CSIRT Case Classification
 - Types of Incidents and Level of Support
 - Incident Specific Procedures-I (Virus and Worm Incidents)
 - Incident Specific Procedures-II (Hacker Incidents)
 - Incident Specific Procedures-III (Social Incidents, Physical Incidents)
 - How CSIRT Handles Case: Steps
 - Example of CSIRT
 - Best Practices for Creating a CSIRT
 - Step 1: Obtain Management Support and Buy-in
 - Step 2: Determine the CSIRT Development Strategic Plan
 - Step 3: Gather Relevant Information
 - Step 4: Design your CSIRT Vision

- Step 5: Communicate the CSIRT Vision
- Step 6: Begin CSIRT Implementation
- Step 7: Announce the CSIRT
- World CERTs <http://www.trusted-introducer.nl/teams/country.html>
- <http://www.first.org/about/organization/teams/>
- IRTs Around the World

Module 58: Credit Card Frauds

- E-Crime
- Statistics
- Credit Card
 - Credit Card Fraud
 - Credit Card Fraud
 - Credit Card Fraud Over Internet
 - Net Credit/Debit Card Fraud In The US After Gross Charge-Offs
- Credit Card Generators
 - Credit Card Generator
 - RockLegend's !Credit Card Generator
- Credit Card Fraud Detection
 - Credit Card Fraud Detection Technique: Pattern Detection
 - Credit Card Fraud Detection Technique: Fraud Screening
 - XCART: Online fraud Screening Service
 - Card Watch
 - MaxMind Credit Card Fraud Detection
 - 3D Secure
 - Limitations of 3D Secure
 - FraudLabs
 - www.pago.de

- Pago Fraud Screening Process
- What to do if you are a Victim of a Fraud
- Facts to be Noted by Consumers
- Best Practices: Ways to Protect Your Credit Cards

Module 59: How to Steal Passwords

- Password Stealing
- How to Steal Passwords
- Password Stealing Techniques
- Password Stealing Trojans
 - MSN Hotmail Password Stealer
 - AOL Password Stealer
 - Trojan-PSW.Win32.M2.14.a
 - CrazyBilets
 - Dropper
 - Fente
 - GWGhost
 - Kesk
 - MTM Recorded pwd Stealer
 - Password Devil
- Password Stealing Tools
 - Password Thief
 - Remote Password Stealer
 - POP3 Email Password Finder
 - Instant Password Finder
 - MessenPass
 - PstPassword
 - Remote Desktop PassView

- IE PassView
- Yahoo Messenger Password
- Recommendations for Improving Password Security
- Best Practices

Module 60: Firewall Technologies

- Firewalls: Introduction
- Hardware Firewalls
 - Hardware Firewall
 - Netgear Firewall
 - Personal Firewall Hardware: Linksys
 - Personal Firewall Hardware: Cisco's PIX
 - Cisco PIX 501 Firewall
 - Cisco PIX 506E Firewall
 - Cisco PIX 515E Firewall
 - CISCO PIX 525 Firewall
 - CISCO PIX 535 Firewall
 - Check Point Firewall
 - Nortel Switched Firewall
- Software Firewalls
 - Software Firewall
- Windows Firewalls
 - Norton Personal Firewall
 - McAfee Personal Firewall
 - Symantec Enterprise Firewall
 - Kerio WinRoute Firewall
 - Sunbelt Personal Firewall
 - Xeon Firewall

- InJoy Firewall
- PC Tools Firewall Plus
- Comodo Personal Firewall
- ZoneAlarm
- Linux Firewalls
 - KMyFirewall
 - Firestarter
 - Guarddog
 - Firewall Builder
- Mac OS X Firewalls
 - Flying Buttress
 - DoorStop X Firewall
 - Intego NetBarrier X5
 - Little Snitch

Module 61: Threats and Countermeasures

Module 62: Case Studies

Module 63: Botnets

- What Is a Botnet?
- The Botnet Life Cycle
- Uses of Botnets
- How to Identify Whether Your Computer is a Botnet
- Common Botnets
 - SDBot
 - RBot
 - Agobot

- Spybot
- Mytob
- Botnet Detection: Tools and Techniques
 - Abuse E-mail
 - Network Infrastructure: Tools and Techniques
 - Intrusion Detection
 - Darknets, Honeypots, and Other Snares
 - Forensics Techniques and Tools for Botnet Detection
- Tool: Ourmon
 - How Ourmon Works
- Anomaly Detection
 - TCP Anomaly Detection by Ourmon
 - UDP Anomaly Detection by Ourmon
 - Detecting E-mail Anomalies using Ourmon
- IRC Protocol
 - Ourmon's RRDTOOL Statistics and IRC Reports
- Detecting an IRC Client Botnet
- Detecting an IRC Botnet Server
- Automated Packet Capture
- Ourmon Event Log
 - DNS and C&C Technology
 - Tricks for Searching the Ourmon Logs
- Sniffing IRC Messages
- Sandboxes
- CWSandbox
 - Operations Revealed by CWSandbox
- Automated Analysis Suite (AAS)
- Responding to Botnets

Module 64: Economic Espionage

- Economic Espionage
- Who are Behind This?
- Motives
- Economic Intelligence
- Trade Secrets
- How Foreign Competitors Get the Information
- Methods of Acquiring Trade Secrets
- How Economic Espionage Increases
- Difference Between Industrial Espionage and Economic Espionage
- Competitive Intelligence
 - Competitive Intelligence Is Not Corporate Espionage
- The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839
- Methods for Economic Espionage Protection

Module 65: Patch Management

- Hotfixes and Patches
- What is Patch Management
- Patch Testing
- Understanding Patch Monitoring and Management
- Types of Patches Defined by Microsoft
- Opware Server Automation System (SAS)
 - Tool: UpdateExpert
 - Tool: Qfecheck
 - Tool: HFNetChk
 - cacls.exe Utility
 - Tool: Shavlik NetChk Protect
 - Tool: Kaseya Patch Management

- Tool: IBM Tivoli Configuration Manager
- Tool: LANDesk Patch Manager
- Tool: ConfigureSoft Enterprise Configuration Manager (ECM)
- Tool: BladeLogic Configuration Manager
- Tool: Microsoft Baseline Security Analyzer (MBSA)
 - MBSA: Scanning Updates in GUI Mode
 - MBSA: Scanning Updates in Command-line Version
- Tool: QChain
- Tool: BigFix Enterprise Suite (BFS)
- Tool: Shavlik NetChk Protect
- Tool: PatchLink Update
- Tool: SecureCentral PatchQuest
- Tool: Patch Authority Ultimate
- Tool: ZENworks Patch Management
- Tool: Ecora Patch Manager
- Tool: Service Pack Manager
- Tool: Altiris Patch Management Solution
- Tool: BMC Patch Manager
- Tool: Hotfix Reporter
- Tool: Numara Patch Manager
- Tool: TrueUpdate
- Tool: FlashUpdate
- Tool: Microsoft Software Update Services (SUS)
- Tool: Prism Patch Manager
- Tool: Patch-Magic
- Patch Management Checklist
- Best Practices for Patch Management

Module 66: Security Convergence

- Security Convergence
- Challenges Confronting an Effective Security Convergence Policy
- Benefits of Using Risk Management in Planning IT Security Administration
- RAMCAP
- Open Security Exchange (OSE)
- CISO (Chief Information Security Officer)
- Elements of Building Secure Operations
- Enterprise Security Management (ESM)
 - ESM Deployment Strategies
- Convergence of Network Operations and Security Operations
- Log Collection
- Log Normalization
- Log Severity
- Log Time Correction
- Log Categorization
- Event Storage
- Discovering and Interacting with Patterns
 - Discovering and Interacting with Patterns: Data Sources
- Intelligent Platform Management Interface (IPMI) Standard

Appendix

- Trojan: Phatbot
- Trojan: Amittis
- Trojan: Senna Spy
- Trojan: QAZ
- Trojan: Back Orifice

- Trojan: Back Oriffice 2000
- Back Oriffice Plug-ins
- Trojan: SubSeven
- Trojan: CyberSpy Telnet Trojan
- Trojan: Subroot Telnet Trojan
- Trojan: Let Me Rule! 2.0 BETA 9
- Trojan: Donald Dick
- Trojan: RECUB

For Training Requirements, Please
Contact EC-Council ATC.

EC-Council

<http://www.eccouncil.org>
info@eccouncil.org

© 2010 EC-Council. All rights reserved.

This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. EC-Council and CEH logos is registered trademarks or trademarks of EC-Council in the United States and/or other countries.