
# CEH v6
# Resource Guide

C|EH™
Certified Ethical Hacker

http://www.eccouncil.org

EC-Council

# CEHv6 Resource Guide

# 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.

# 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 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



## Module 1: Introduction to Ethical Hacking

- Problem Definition -Why Security?
- Essential Terminologies
- Elements of Security
- The Security, Functionality and Ease of Use Triangle
- Case Study
- What does a Malicious Hacker do?
  - Phase1-Reconnaissaance
    - 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
- Hacktivism
- 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)
    - 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

- Federal Managers Financial Integrity Act of 1982
- The Freedom of Information Act 5 U.S.C. § 552
- Federal Information Security Management Act (FISMA)
- The Privacy Act Of 1974 5 U.S.C. § 552a
- USA Patriot Act of 2001
- 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 INFORMTION 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:
- 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
  - Website Watcher
- Steps to Create Fake Login Pages
- How to Create Fake Login Pages
- 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 Honeypot
- 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
        - HPing2
        - Ping Sweep
        - Firewalk Tool
        - Firewalk Commands
        - Firewalk Output
        - Nmap
        - Nmap: Scan Methods
        - NMAP Scan Options
        - NMAP Output Format
        - 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
- 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
  - P0f – Banner Grabbing Tool
  - p0f for Windows
  - Httprint 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
  - Cheops
  - Friendly Pinger
  - LANsurveyor
  - Ipsonar
  - LANState
    - Insightix Visibility
    - IPCheck Server Monitor

        - PRTG Traffic Grapher
- Preparing Proxies
    - Proxy Servers
    - Free 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
    - Additional Proxy Tools
    - Anonymizers
        - Surfing Anonymously
        - Primedius Anonymizer
        - StealthSurfer
        - Anonymous Surfing: Browzar
        - Torpark Browser
        - GetAnonymous
        - IP Privacy
        - Anonymity 4 Proxy (A4Proxy)
        - Psiphon
        - Connectivity Using Psiphon
        - 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: LOphtcrack
- 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: NBTDeputy
    - NetBIOS DoS Attack

- Hacking Tool: John the Ripper

- Password Sniffing
- How to Sniff SMB Credentials?
- SMB Replay Attacks
- Replay Attack Tool: SMBProxy
- 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

- 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
    - DCPP – 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
- Video Steganography
- Case Study: Al-Qaida members Distributing Propaganda to Volunteers using Steganography
- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Stegdetect
- 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
  - PhatBooster

## Module 8: Trojans and Backdoors

- Effect on Business
- 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
- Trojans
    - Trojan: iCmd
    - MoSucker Trojan
    - Proxy Server Trojan
    - SARS Trojan Notification
    - Wrappers
    - Wrapper Covert Program
    - Wrapping Tools
    - One Exe Maker / YAB / Pretator Wrappers
    - Packaging Tool: WordPad
    - RemoteByMail
    - Tool: Icon Plus
    - Defacing Application: Restorator
    - Tetris

- 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
- ICMP Backdoor Trojan
- Microsoft Network Hacked by QAZ Trojan
- 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
- FTP Trojan - TinyFTPD
- VNC Trojan
- Webcam Trojan
- DJI RAT
- Skiddie Rat
- Biohazard RAT
- Troya
- ProRat
- Dark Girl
- DaCryptic
- Net-Devil

- Classic Trojans Found in the Wild
  - Trojan: Tini
  - Trojan: NetBus

- Trojan: Netcat
- Netcat Client/Server
- Netcat Commands
- Trojan: Beast
- Trojan: Phatbot
- Trojan: Amitis
- 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

- Hacking Tool: Loki
- Loki Countermeasures
- Atelier Web Remote Commander
- Trojan Horse Construction Kit
- 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
- Registry- What's Running
- 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
- How is a Worm Different from a Virus
- Indications of a Virus Attack
- Hardware Threats
- Software Threats
- Virus Damage
    - Mode of Virus Infection
- Stages of Virus Life
- 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 Virus/Worms – I Love You Virus
- Famous Virus/Worms – Melissa
- Famous Virus/Worms – JS/Spth
- Klez Virus Analysis
- 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.Neworld
    - W32/WBoy.a

- ExeBug.d
- W32/Voterai.worm.e
- W32/Lecivio.worm
- W32/Lurka.a
- W32/Vora.worm!p2p

- Writing a Simple Virus Program
- Virus Construction Kits
- Virus Detection Methods
- Virus Incident Response
- What is Sheep Dip?
- Virus Analysis – IDA Pro Tool
- Prevention is better than Cure
- Anti-Virus Software
  - AVG Antivirus
  - Norton Antivirus
  - McAfee
  - Socketsheild
  - BitDefender
  - ESET Nod32
  - CA 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

## Module 10: Sniffers

- Definition - Sniffing
- Protocols Vulnerable to Sniffing
- Tool: Network View – Scans the Network for Devices
- The Dude Sniffer
- Wireshark
- Display Filters in Wireshark
- Following the TCP Stream in Wireshark
- Cain and Abel
- Tcpdump
- Tcpdump Commands
- Types of Sniffing
  - Passive Sniffing
  - Active Sniffing
- What is ARP
  - ARP Spoofing Attack
  - How does ARP Spoofing Work
  - ARP Poising
  - MAC Duplicating
  - MAC Duplicating Attack

- Tools for ARP Spoofing
    - Ettercap
    - ArpSpyX
- MAC Flooding
    - Tools for MAC Flooding
        - Linux Tool: Macof
        - Windows Tool: Etherflood
- Threats of ARP Poisoning
- Irs-Arp Attack Tool
- ARPWorks Tool
- Tool: Nemesis

- IP-based sniffing
    - Linux Sniffing Tools (dsniff package)
- Linux tool: Arpspoof
- Linux Tool: Dnssppoof
- Linux Tool: Dsniff
- Linux Tool: Filesnarf
- Linux Tool: Mailsnarf
- Linux Tool: Msgsnarf
- Linux Tool: Sshmitm
- Linux Tool: Tcpkill
- Linux Tool: Tcpnice
- Linux Tool: Urlsnarf
- Linux Tool: Webspy
- Linux Tool: Webmitm

- DNS Poisoning Techniques
  - Intranet DNS Spoofing (Local Network)
  - Internet DNS Spoofing (Remote Network)
  - Proxy Server DNS Poisoning
  - DNS Cache Poisoning
- Interactive TCP Relay
- Interactive Replay Attacks
- Raw Sniffing Tools
- Features of Raw Sniffing Tools
  - HTTP Sniffer: EffeTech
  - Ace Password Sniffer
  - Win Sniffer
  - MSN Sniffer
  - SmartSniff
  - Session Capture Sniffer: NetWitness
  - Session Capture Sniffer: NWreader
  - Packet Crafter Craft Custom TCP/IP Packets
  - SMAC
  - NetSetMan Tool
  - Ntop
  - EtherApe
  - 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
- EffeTech HTTP Sniffer
- AnalogX Packetmon
- Colasoft MSN Monitor
- IPgrab
- EtherScan Analyzer

- How to Detect Sniffing
- Countermeasures
  - Antisniff Tool
  - Arpwatch Tool
  - PromiScan
  - proDETECT

## 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
  - Online
  - Telephone
  - 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: Feb' 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

- Ways for Getting Email Account Information
- Stealing Cookies
- Social Engineering
- Password Phishing
- Fraudulent e-mail Messages
- Vulnerabilities
  - Web Email
  - Reaper Exploit
- 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
- 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
- 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: Trinoo
  - DDoS Tool: Tribal Flood Network
  - DDoS Tool: TFN2K
  - DDoS Tool: Stacheldraht
  - DDoS Tool: Shaft
  - DDoS Tool: Trinity
  - DDoS Tool: Knight and Kaiten
  - DDoS Tool: Mstream
- 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

- 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?
- 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: Packet Sniffer
- UDP Hijacking
- Application Level Hijacking

- Programs that Performs Session Hacking
  - Juggernaut
  - Hunt
  - TTY-Watcher
  - IP watcher
  - Session Hijacking Tool: T-Sight
  - Remote TCP Session Reset Utility (SOLARWINDS)
  - Paros HTTP Session Hijacking Tool
  - Dnshijacker Tool
  - Hjksuite Tool
- Dangers that hijacking Pose
- Protecting against Session Hijacking
- Countermeasures: 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
  - IIS Components
  - IIS Directory Traversal (Unicode) Attack
- Unicode
  - Unicode Directory Traversal Vulnerability

- 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
- Tool: Immunity CANVAS Professional
- Tool: Core Impact
- Tool: MPack
- Tool: Neosploit
- Hotfixes and Patches
- What is Patch Management

- Patch Management Checklist
  - Solution: UpdateExpert
  - Patch Management Tool: qfecheck
  - Patch Management Tool: HFNetChk
  - cacls.exe utility
  - Shavlik NetChk Protect
  - Kaseya Patch Management
  - IBM Tivoli Configuration Manager
  - LANDesk Patch Manager
  - BMC Patch Manager
  - ConfigureSoft Enterprise Configuration Manager (ECM)
  - BladeLogic Configuration Manager
  - Opsware Server Automation System (SAS)
  - Best Practices for Patch Management
- 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 Setup
- 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: Mapper

## Module 18: Web-Based Password Cracking Techniques

- 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
- 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 Crackers Available
  - L0phtCrack (LC4)
  - John the Ripper
  - Brutus
  - ObiWaN
  - Authforce
  - Hydra
  - Cain & Abel
  - RAR
  - Gammaprog
  - 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
- WebPassword
- Password Administrator
- Password Safe
- Easy Web Password
- PassReminder
- My Password Manager

- Countermeasures

## Module 19: SQL Injection

- 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 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
  - Blind SQL Injection Schema
- 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
  - Introduction to 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 Concepts and Devices
    - Related Technology and Carrier Networks

- Antennas
- Cantenna – www.cantenna.com
- Wireless Access Points
- SSID
- Beacon Frames
- Is the SSID a Secret
- Setting up a WLAN
- Authentication and Association
- Authentication Modes
- The 802.1X Authentication Process

- WEP and WPA
  - Wired Equivalent Privacy (WEP)
  - WEP Issues
  - WEP - Authentication Phase
  - WEP - Shared Key Authentication
  - WEP - Association Phase
  - WEP Flaws
  - What is WPA
  - WPA Vulnerabilities
  - WEP, WPA, and WPA2
  - WPA2 Wi-Fi Protected Access 2
  - Attacks and Hacking Tools
    - Terminologies
    - WarChalking
    - Authentication and (Dis) Association Attacks

- WEP Attack
- 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
- Aircrack-ng
- WEP Tool: AirSnort
- WEP Tool: WEPCrack
- WEP Tool: WepLab
- Attacking WPA Encrypted Networks
- Attacking WEP with WEPCrack on Windows using Cygwin
- Attacking WEP with WEPCrack on Windows using PERL Interpreter
- Tool: Wepdecrypt
- WPA-PSK Cracking Tool: CowPatty
- 802.11 Specific Vulnerabilities
- Evil Twin: Attack
- 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
- ClassicStumbler

- AirFart
- AP Radar
- Hotspotter
- Cloaked Access Point
- WarDriving Tool: shtumble
- Temporal Key Integrity Protocol (TKIP)
- LEAP: The Lightweight Extensible Authentication Protocol
- LEAP Attacks
- LEAP Attack Tool: ASLEAP
- Working of ASLEAP
- MAC Sniffing and AP Spoofing
- Defeating MAC Address Filtering in Windows
- Manually Changing the MAC Address in Windows XP and 2000
- Tool to Detect MAC Address Spoofing: Wellenreiter
- Man-in-the-Middle Attack (MITM)
- Denial-of-Service Attacks
- DoS Attack Tool: Fatajack
- Hijacking and Modifying a Wireless Network
- Phone Jammers
- Phone Jammer: Mobile Blocker
- Pocket Cellular Style Cell Phone Jammer
- 2.4Ghz Wi-Fi & Wireless Camera Jammer
- 3 Watt Digital Cell Phone Jammer
- 3 Watt Quad Band Digital Cellular Mobile Phone Jammer
- 20W Quad Band Digital Cellular Mobile Phone Jammer

- 40W Digital Cellular Mobile Phone Jammer
- Detecting a Wireless Network

- Scanning Tools
  - Scanning Tool: Kismet
  - Scanning Tool: Prismstumbler
  - Scanning Tool: MacStumbler
  - Scanning Tool: Mognet V1.16
  - Scanning Tool: WaveStumbler
  - Scanning Tool: Netchaser V1.0 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
- Sniffing Tool: Ssidsniff
- Multiuse Tool: THC-RUT
- Tool: WinPcap
- Tool: AirPcap
- AirPcap: Example Program from the Developer's Pack
- Microsoft Network Monitor

- Hacking 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

- Wireless Security
  - WIDZ: Wireless Intrusion Detection System
  - Radius: Used as Additional Layer in Security
  - Securing Wireless Networks
  - Wireless Network Security Checklist
  - WLAN Security: Passphrase
  - Don'ts in Wireless Security
- Wireless Security Tools
  - WLAN Diagnostic Tool: CommView for WiFi PPC
  - WLAN Diagnostic Tool: AirMagnet Handheld Analyzer

- Auditing Tool: BSD-Airtools
- 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 Room
  - Workstation Area
  - Wireless Access Point
  - Other Equipments
  - Access Control
    - Biometric Devices

- Biometric Identification Techniques
- 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: Xcrack
- 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 Indication of Intrusion: System Indications
- General Indication of Intrusion: File System Indications
- General Indication of Intrusion: Network Indications
- 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

- 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 HTTPTunnel
  - 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: IDS Informer
  - IDS Testing Tool: Evasion Gateway
  - IDS Tool: Event Monitoring Enabling Responses to Anomalous Live Disturbances (Emerald)
  - IDS Tool: BlackICE
  - IDS Tool: Next-Generation Intrusion Detection Expert System (NIDES)
  - IDS Tool: SecureHost
  - IDS Tool: Snare
  - IDS Testing Tool: Traffic IQ Professional
  - IDS Testing Tool: TCPOpera
  - IDS testing tool: Firewall Informer
  - Atelier Web Firewall Tester
- What is Honeypot?
  - The Honeynet Project
  - Types of Honeypots
    - 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

- 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
    - A Simple Uncontrolled Overflow of the Stack
    - Stack Based Buffer Overflows
- Types of Buffer Overflows: Heap-based Buffer Overflow
    - Heap Memory Buffer Overflow Bug
    - Heap-based Buffer Overflow
- Understanding Assembly Language
    - Shellcode
- How to Detect Buffer Overflows in a Program
    - Attacking a Real Program
- NOPs

- How to Mutate a Buffer Overflow Exploit
- Once the Stack is Smashed
- Defense Against Buffer Overflows
  - Tool to Defend Buffer Overflow: Return Address Defender (RAD)
  - Tool to Defend Buffer Overflow: StackGuard
  - Tool to Defend Buffer Overflow: Immunix System
  - Vulnerability Search: NIST
  - Valgrind
  - Insure++
- Buffer Overflow Protection Solution: Libsafe
  - Comparing Functions of libc and Libsafe
- Simple Buffer Overflow in C
  - Code Analysis

## Module 25: Cryptography

- Introduction to Cryptography
- Classical Cryptographic Techniques
  - Encryption
  - Decryption
- Cryptographic Algorithms
- RSA (Rivest Shamir Adleman)
  - Example of RSA Algorithm
  - RSA Attacks
  - RSA Challenge
- Data Encryption Standard (DES)
  - DES Overview

- RC4, RC5, RC6, Blowfish
  - RC5
- Message Digest Functions
  - One-way Bash Functions
  - MD5
- SHA (Secure Hash Algorithm)
- SSL (Secure Sockets Layer)
- What is SSH?
  - SSH (Secure Shell)
- Algorithms and Security
- Disk Encryption
- Government Access to Keys (GAK)
- Digital Signature
  - Components of a Digital Signature
  - Method of Digital Signature Technology
  - Digital Signature Applications
  - Digital Signature Standard
  - Digital Signature Algorithm: Signature Generation/Verification
  - Digital Signature Algorithms: ECDSA, ElGamal Signature Scheme
  - Challenges and Opportunities
- Digital Certificates
  - Cleversafe Grid Builder http://www.cleversafe.com/
- PGP (Pretty Good Privacy)
- CypherCalc
- Command Line Scriptor
- CryptoHeaven
- Hacking Tool: PGP Crack
- Magic Lantern
- Advanced File Encryptor

- Encryption Engine
- Encrypt Files
- Encrypt PDF
- Encrypt Easy
- Encrypt my Folder
- Advanced HTML Encrypt and Password Protect
- Encrypt HTML source
- Alive File Encryption
- Omziff
- ABC CHAOS
- EncryptOnClick
- CryptoForge
- SafeCryptor
- CrypTool
- Microsoft Cryptography Tools
- Polar Crypto Light
- CryptoSafe
- Crypt Edit
- CrypSecure
- Cryptlib
- Crypto++ Library
- Code Breaking: Methodologies

- Cryptanalysis
- Cryptography Attacks
- Brute-Force Attack

- Cracking S/MIME Encryption Using Idle CPU Time
- distributed.net
- Use Of Cryptography

## Module 26: Penetration Testing

- Introduction to Penetration Testing (PT)
- Categories of security assessments
- Vulnerability Assessment
- Limitations of Vulnerability Assessment
- 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
- 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
- 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 Compliment
- 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 Prorgam
- 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: MAC OS X Hacking

- Introduction to MAC OS
- Vulnerabilities in MAC
  - Crafted URL Vulnerability
  - CoreText Uninitialized Pointer Vulnerability
  - ImageIO Integer overflow Vulnerability
  - DirectoryService Vulnerability
  - iChat UPnP buffer overflow Vulnerability
  - ImageIO Memory Corruption Vulnerability
  - Code Execution Vulnerability
  - UFS filesystem integer overflow Vulnerability
  - Kernel "fpathconf()" System call Vulnerability
  - UserNotificationCenter Privilege Escalation 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

- Anti-Viruses in MAC
  - VirusBarrier
  - McAfee Virex for Macintosh
  - 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
  - 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
  - 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
- 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/QQRob-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: Introduction
- Basics of Game Hacking
- Threats in Online Gaming
- Cheating in Online Computer Games
- Types of Exploits
- Example of popular game exploits
- Stealing Online Game Passwords
    - Stealing Online Game Passwords: Social Engineering and Phishing
- Online Gaming Malware from 1997-2007
- Best Practices for Secure Online Gaming
- Tips 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 (Firefox, IE)

- 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)

- Geographical 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
- Dripper
- 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

- Domain Level Policies
  - Account Policies
  - Password Policy
  - Password Policy
  - Password Policy - Policies
- Enforce Password History
  - Enforce Password History - Vulnerability
  - Enforce Password History - Countermeasure
  - Enforce Password History - Potential Impact
- Maximum Password Age
  - Password Age - Vulnerability
  - Maximum Password Age - Countermeasure
  - Maximum Password Age - Potential Impact
  - Maximum Password Age

- Minimum Password Age
- Minimum Password Age - Vulnerability
- Minimum Password Age - Countermeasure
- Minimum Password Age - Potential Impact
- Minimum Password Age

- Minimum Password Length
  - Minimum Password Length - Vulnerability
  - Minimum Password Length - Countermeasure
  - Minimum Password Length - Potential Impact
  - Minimum Password Length
- Passwords Must Meet Complexity Requirements
  - Passwords must Meet Complexity Requirements - Vulnerability
  - Passwords must Meet Complexity Requirements - Countermeasure
  - Passwords must Meet Complexity Requirements - Potential Impact
  - Passwords must Meet Complexity Requirements
- Store Password using Reversible Encryption for all Users in the Domain
- Account Lockout Policy
  - Account Lockout Policy - Policies
- Account Lockout Duration
  - Account Lockout Duration - Vulnerability
  - Account Lockout Duration - Countermeasure
  - Account Lockout Duration - Potential Impact
  - Account Lockout Duration
- Account Lockout Threshold
  - Account Lockout Threshold - Vulnerability

- Account Lockout Threshold - Countermeasure
- Account Lockout Threshold - Potential Impact

- Reset Account Lockout Counter After
- Kerberos Policy
  - Kerberos Policy - Policies
- Enforce User Logon Restrictions
- Maximum Lifetime for Service Ticket
  - Maximum Lifetime for User Ticket
  - Maximum Lifetime for User Ticket Renewal
- Maximum Tolerance for Computer Clock Synchronization
- Audit Policy
  - Audit Settings
  - Audit Account Logon Events
  - Audit Account Management
  - Audit Directory Service Access
  - Audit Logon Events
  - Audit Object Access
  - Audit Policy Change
  - Audit Privilege Use
  - Audit Process Tracking
  - Audit System Events
- User Rights
- Access this Computer from the Network
- Act as Part of the Operating System
- Add Workstations to Domain

- Adjust Memory Quotas for a Process
- Allow Log On Locally
- Allow Log On through Terminal Services
- Back Up Files and Directories
- Bypass Traverse Checking
- Change the System Time
- Create a Page File
- Create a Token Object
- Create Global Objects
- Create Permanent Shared Objects
- Debug Programs
- Deny Access to this Computer from the Network
- Deny Log On as a Batch Job
- Deny Log On as a Service
- Deny Log On Locally
- Deny Log On through Terminal Services
- Enable Computer and User Accounts to be Trusted for Delegation
- Force Shutdown from a Remote System
- Generate Security Audits
- Impersonate a Client after Authentication
- Increase Scheduling Priority
- Load and Unload Device Drivers
- Lock Pages in Memory
- Log On as a Batch Job
- Log On as a Service

- Manage Auditing and Security Log
- Modify Firmware Environment Values
- Perform Volume Maintenance Tasks
- Profile Single Process
- Profile System Performance
- Remove Computer from Docking Station
- Replace a Process Level Token
- Restore Files and Directories
- Shut Down the System
- Synchronize Directory Service Data
- Take Ownership of Files or Other Objects
- Security Options
- Accounts: Administrator Account Status
    - Accounts: Administrator Account Status - Vulnerability
    - Accounts: Administrator Account Status
    - Accounts: Guest Account Status
    - Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only
    - Accounts: Rename Administrator Account
    - Accounts: Rename Guest Account
- Audit: Audit the Access of Global System Objects
    - Audit: Audit the Use of Backup and Restore Privilege
    - Audit: Shut Down System Immediately if Unable to Log Security Audits
- DCOM: Machine Access/Launch Restrictions in Security Descriptor Definition Language (SDDL)
    - DCOM: Machine Access/Launch Restrictions in Security Descriptor Definition Language (SDDL)
- Devices: Allow Undock without having to Log On

- Devices: Allowed to Format and Eject Removable Media
- Devices: Prevent Users from Installing Printer Drivers
- Devices: Restrict CD-ROM/Floppy Access to Locally Logged-on User Only
- Devices: Restrict CD-ROM Access to Locally Logged-on User Only
- Devices: Unsigned Driver Installation Behavior
- Domain Controller: Allow Server Operators to Schedule Tasks
- Domain Controller: LDAP Server Signing Requirements
- Domain Controller: Refuse Machine Account Password Changes
- Domain Member: Digitally Encrypt or Sign Secure Channel Data
- Domain Member: Disable Machine Account Password Changes
- Domain Member: Maximum Machine Account Password Age
- Domain Member: Require Strong (Windows 2000 or Later) Session Key
- Interactive Logon: Do Not Display Last User Name
- Interactive Logon: Do Not Require CTRL+ALT+DEL
- Interactive Logon: Message Text for Users Attempting to Log On
- Interactive Logon: Number of Previous Logons to Cache
- Interactive Logon: Prompt User to Change Password before Expiration
- Interactive Logon: Require Domain Controller Authentication to Unlock Workstation
- Interactive Logon: Require Smart Card
- Interactive Logon: Smart Card Removal Behavior
- Microsoft Network Client and Server: Digitally Sign Communications (Four Related Settings)
- Microsoft Network Client: Send Unencrypted Password to Third-party SMB Servers
- Microsoft Network Server: Amount of Idle Time Required before Suspending Session
- Microsoft Network Server: Disconnect Clients when Logon Hours Expire
- Network Access: Allow Anonymous SID/Name Translation

- Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts
- Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication
- Network Access: Let Everyone Permissions Apply to Anonymous Users
- Network Access: Named Pipes that can be Accessed Anonymously
- Network Access: Remotely Accessible Registry Paths
- Network Access: Remotely Accessible Registry Paths and Sub-paths
- Network Access: Restrict Anonymous Access to Named Pipes and Shares
- Network Access: Shares that can be Accessed Anonymously
- Network Access: Sharing and Security Model for Local Accounts
- Network Security: Do Not Store LAN Manager Hash Value on Next Password Change
- Network Security: Force Logoff when Logon Hours Expire
- Network Security: LAN Manager Authentication Level
- Network Security: LDAP Client Signing Requirements
- Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients/Servers
- Network Security: Minimum Session Security for NTLM SSP based (Including Secure RPC) Clients
- Recovery Console: Allow Automatic Administrative Logon
- Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders
- Shutdown: Allow System to be Shut Down Without Having to Log On
- Shutdown: Clear Virtual Memory Page File
- System Cryptography: Force Strong Key Protection for User Keys Stored on the Computer
- System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing
- System Objects: Default Owner for Objects Created by Members of the Administrators Group
- System Objects: Require Case Insensitivity for Non-Windows Subsystems
- System Objects: Strengthen Default Permissions of Internal System Objects
- System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

- Event Log
  - Maximum Event Log Size
  - Prevent Local Guests Group from Accessing Event Logs
  - Retain Event Logs
  - Retention Method for Event Log
  - Delegating Access to the Event Logs
- System Services
- Services Overview
- Do Not Set Permissions on Service Objects
- Manually Editing Security Templates
- System Services - Alerter
- Application Experience Lookup Service
- Application Layer Gateway Service
- Application Management
- ASP .NET State Service
- Automatic Updates
- Background Intelligent Transfer Service (BITS)
- Certificate Services
- Client Service for NetWare
- ClipBook
- Cluster Service
- COM+ Event System
- COM+ System Application
- Computer Browser
- Cryptographic Services

- DCOM Server Process Launcher
- DHCP Client
- DHCP Server
- Distributed File System
- Distributed Link Tracking Client
- Distributed Link Tracking Server
- Distributed Transaction Coordinator
- DNS Client
- DNS Server
- Error Reporting Service
- Event Log
- Fast User Switching Compatibility
- Fax Service
- File Replication
- File Server for Macintosh
- FTP Publishing Service
- Help and Support
- HTTP SSL
- Human Interface Device Access
- IAS Jet Database Access
- IIS Admin Service
- IMAPI CD-Burning COM Service
- Indexing Service
- Infrared Monitor
- Internet Authentication Service

- Intersite Messaging
- IP Version 6 Helper Service
- IPSec Policy Agent (IPSec Service)
- IPSec Services
- Kerberos Key Distribution Center
- License Logging Service
- Logical Disk Manager
  - Logical Disk Manager Administrative Service
- Machine Debug Manager
- Message Queuing
  - Message Queuing Down Level Clients
  - Message Queuing Triggers
  - Messenger
- Microsoft POP3 Service
- Microsoft Software Shadow Copy Provider
- MSSQL$UDDI
- MSSQLServerADHelper
- .NET Framework Support Service
- Net Logon
- NetMeeting Remote Desktop Sharing
- Network Connections
- Network DDE
- Network DDE DSDM
- Network Location Awareness (NLA)
- Network Provisioning Service

- Network News Transfer Protocol (NNTP)
- NTLM Security Support Provider
- Performance Logs and Alerts
- Plug and Play
- Portable Media Serial Number
- Print Server for Macintosh
- Print Spooler
- Protected Storage
- QoS RSVP Service
- Remote Access Auto Connection Manager
    - Remote Access Connection Manager
- Remote Administration Service
- Help Session Manager
    - Remote Desktop Help Session Manager
- Remote Installation
    - Remote Procedure Call (RPC)
    - Remote Procedure Call (RPC) Locator
    - Remote Registry Service
    - Remote Server Manager
    - Remote Server Monitor
    - Remote Storage Notification
    - Remote Storage Server
- Removable Storage
- Resultant Set of Policy Provider
- Routing and Remote Access

- SAP Agent
- Secondary Logon
- Security Accounts Manager
- Security Center
- Server
- Shell Hardware Detection
- Simple Mail Transport Protocol (SMTP)
- Simple TCP/IP Services
- Smart Card
- Special Administration Console Helper
- System Event Notification
- System Restore Service
- Task Scheduler
- TCP/IP NetBIOS Helper Service
- TCP/IP Print Server
- Telnet
- Terminal Services
  - Terminal Services Licensing
  - Terminal Services Session Directory
- Trivial FTP Daemon
- Uninterruptible Power Supply
- Upload Manager
- Virtual Disk Service
- WebClient
- Web Element Manager

- Windows Firewall /Internet Connection Sharing
  - Windows Installer
  - Windows System Resource Manager
  - Windows Time
- WinHTTP Web Proxy Auto-Discovery Service
- Wireless Configuration
- Workstation
- World Wide Web Publishing Service
- Software Restriction Policies
- The Threat of Malicious Software
- Windows XP and Windows Server 2003 Administrative Templates
- Computer Configuration Settings
- NetMeeting
- Disable Remote Desktop Sharing
- Internet Explorer Computer Settings
- Disable Automatic Install of Internet Explorer Components
- Disable Periodic Check for Internet Explorer Software Updates
- Disable Software Update Shell Notifications on Program Launch
- Make Proxy Settings Per-Machine (Rather than Per-User)
- Security Zones: Do Not Allow Users to Add/Delete Sites
- Turn off Crash Detection
- Do Not Allow Users to Enable or Disable Add-ons
- Internet Explorer\Internet Control Panel\Security Page
- Internet Explorer\Internet Control Panel\Advanced Page
- Allow Software to Run or Install Even if the Signature is Invalid

- Allow Active Content from CDs to Run on User Machines
- Allow Third-party Browser Extensions
- Check for Server Certificate Revocation
- Check for Signatures On Downloaded Programs
- Do Not Save Encrypted Pages to Disk
- Empty Temporary Internet Files Folder when Browser is Closed
- Internet Explorer\Security Features
- Binary Behavior Security Restriction
- MK Protocol Security Restriction
- Local Machine Zone Lockdown Security
- Consistent MIME Handling
- MIME Sniffing Safety Features
- Scripted Window Security Restrictions
- Restrict ActiveX Install
- Restrict File Download
- Network Protocol Lockdown
- Internet Information Services
- Prevent IIS Installation
- Terminal Services
- Deny Log Off of an Administrator Logged in to the Console Session
- Do Not Allow Local Administrators to Customize Permissions
- Sets Rules for Remote Control of Terminal Services User Sessions
- Client/Server Data Redirection
- Allow Time Zone Redirection
- Do Not Allow COM Port Redirection

- Do Not Allow Client Printer Redirection
- Do Not Allow LPT Port Redirection
- Do Not Allow Drive Redirection
- Encryption and Security
- Set Client Connection Encryption Level
- Always Prompt Client For A Password On Connection
- RPC Security Policy
- Secure Server (Require Security)
- Sessions
- Set Time Limit For Disconnected Sessions
- Allow Reconnection From Original Client Only
- Windows Explorer
- Turn Off Shell Protocol Protected Mode
- Windows Messenger
- Windows Update
- Configure Automatic Updates
- Reschedule Automatic Updates Scheduled Installations
- System
- Turn off Autoplay
- Do Not Process The Run Once List
- Logon
- Don't Display The Getting Started Welcome Screen At Logon
- Do Not Process The Legacy Run List
- Group Policy
- Internet Explorer Maintenance Policy Processing

- IP Security Policy Processing
- Registry Policy Processing
- Security Policy Processing
- Error Reporting
- Display Error Notification
- Report Errors
- Internet Communications Management
- Distributed COM
- Browser Menus
- Disable Save This Program To Disk Option
- Attachment Manager
- Inclusion List For High Risk File Types
- Inclusion List For Moderate Risk File Types
- Inclusion List For Low File Types
- Trust Logic For File Attachments
- Hide Mechanisms To Remove Zone Information
- Notify Antivirus Programs When Opening Attachments
- Windows Explorer
- Remove Security Tab
- System\Power Management
- Additional Registry Entries
- How to Modify the Security Configuration Editor User Interface
- TCP/IP-Related Registry Entries
- Disableipsourcerouting: IP Source Routing Protection Level (Protects Against Packet Spoofing)
- Enabledeadgwdetect: Allow Automatic Detection Of Dead Network Gateways (Could Lead To Dos)

- Enableicmpredirect: Allow ICMP Redirects To Override OSPF Generated Routes
- Keepalivetime: How Often Keep-alive Packets Are Sent In Milliseconds (300,000 Is Recommended)
- Synattackprotect: Syn Attack Protection Level (Protects Against Dos)
- Tcpmaxconnectresponseretransmissions: SYN-ACK Retransmissions When A Connection Request Is Not Acknowledged
- Tcpmaxdataretransmissions: How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default)
- Miscellaneous Registry Entries
- Configure Automatic Reboot from System Crashes
- Enable Administrative Shares
- Disable Saving of Dial-Up Passwords
- Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List
- Configure Netbios Name Release Security: Allow the Computer to Ignore Netbios Name Release Requests Except from WINS Servers
- Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended)
- Security Log Near Capacity Warning: Percentage Threshold for the Security Event Log at which the System will Generate a Warning
- Registry Entries Available In Windows XP With SP2 And Windows Server 2003 With SP1
- RunInvalidSignatures
- Registry Entries Available in Windows XP with SP2
- Security Center Registry Entries for XP
- StorageDevicePolicies\WriteProtect
- Registry Entries Available in Windows Server 2003 with SP1
- UseBasicAuth
- DisableBasicOverClearChannel
- Additional Countermeasures
- Securing the Accounts

- NTFS
- Data and Application Segmentation
- Configure SNMP Community Name
- Disable NetBIOS and SMB on Public Facing Interfaces
- Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger
- Configure IPsec Policies
- Configuring Windows Firewall



## Module 62: Case Studies

# Classroom Lecture Hours



| Classroom Lecture Hours | Topics |
|---|---|
| 1 hour | Introduction to Ethical Hacking |
| 20 minutes | Hacking Laws |
| 1 hour | Footprinting |
| 1 hour | Google Hacking |
| 2 hours | Scanning |
| 1 hour | Enumeration |
| 2 hours | System Hacking |
| 2 hours | Trojans and Backdoors |
| 45 minutes | Viruses and Worms |
| 1 hour | Sniffers |
| 45 minutes | Social Engineering |
| 30 minutes | Phishing and Identity Theft |
| 30 minutes | Hacking Email Accounts |
| 45 Minutes | Denial-of-Service |
| 30 minutes | Session Hijacking |
| 1 hour | Hacking Web Servers |
| 1 hour | Web Application Vulnerabilities |
| 1 hour | Web-Based Password Cracking Techniques |
| 1 hour | SQL Injection |
| 45 Minutes | Hacking Wireless Networks |

| | |
|---|---|
| 45 Minutes | Physical Security |
| 45 Minutes | Linux Hacking |
| 1 hour | Evading IDS, Firewalls and Detecting Honey Pots |
| 1 hour | Buffer Overflows |
| 20 minutes | Cryptography |
| 1 hour | Penetration Testing |
| 20 minutes | Covert Hacking |
| 20 minutes | Writing Virus Codes |
| 20 minutes | Assembly Language Tutorial |
| 20 minutes | Exploit Writing |
| 20 minutes | Smashing the Stack for Fun and Profit |
| 20 minutes | Windows Based Buffer Overflow Exploit Writing |
| 20 minutes | Reverse Engineering |
| 45 Minutes | Mac OS X Hacking |
| 45 Minutes | Hacking Routers, Cable Modems and Firewalls |
| 45 Minutes | Mobile Phone and Handheld Devices (PDAs) Hacking |
| 20 minutes | Bluetooth Hacking |
| 45 Minutes | VoIP Hacking |
| 45 Minutes | RFID Hacking |
| 45 Minutes | Spamming |
| 45 Minutes | Hacking USB Devices |
| 45 Minutes | Hacking Database Servers |
| 20 minutes | Cyber Warfare- Hacking, Al-Qaida and Terrorism |
| 20 minutes | Internet Content Filtering Techniques |

| | |
|---|---|
| 20 minutes | Privacy on Internet- Anonymous |
| 20 minutes | Securing Laptop Computers |
| 20 minutes | Spying Technologies |
| 20 minutes | Corporate Espionage- Hacking Using Insiders |
| 20 minutes | Creating Security Policies |
| 20 minutes | Software Piracy and Warez |
| 20 minutes | Hacking and Cheating Online Games |
| 20 minutes | Hacking RSS and Atom |
| 20 minutes | Hacking Web Browsers (Firefox, IE) |
| 20 minutes | Proxy Server Technologies |
| 45 Minutes | Data Loss Prevention |
| 20 minutes | Hacking Global Positioning System (GPS) |
| 1 hour | Computer Forensics and Incident Handling |
| 20 minutes | Credit Card Frauds |
| 20 minutes | How to Steal Passwords |
| 20 minutes | Firewall Technologies |
| 20 minutes | Threats and Countermeasures |
| 20 minutes | Case Studies |

# CEH v6 Labs



## Module 01 Introduction to Ethical Hacking (Lab time: 45 minutes)

**Lab 1.1** Go through Ethical Hacking document

**Lab 1.2** Understand what is ethical hacking?

**Lab 1.3** Differentiate Security vs. Safety

**Lab 1.4** Read Ethical Hacking Strategies and Benefits

**Lab 1.5** Visit various hacker websites

**Lab 1.6** Read Ethical Hacking Agreement

## Module 02 Hacking Laws (Self Do Labs)

**Lab 2.1** Visit US Cybercrime Website

**Lab 2.1** Go through Florida Computer Crime Act

**Lab 2.2** Hacking Offences whitepaper

## Module 03 – Footprinting (Lab time: 45 minutes)

**Lab 3.1** Use SamSpade

**Lab 3.2** Use Web Data Extractor to Footprint a Website

**Lab 3.3** Use GEO Spider to Footprint a Website

**Lab 3.4** Use NEOTRACE to Footprint a Website

**Lab 3.5** Use Which ISP Owns IP to Footprint a Network Address

**Lab 3.6** Use "Where is IP" to Footprint a Network Address

**Lab 3.7** Use "My IP Suite" to Footprint a Network Address

**Lab 3.8** Use "Way Back Machine" to View Web History

**Lab 3.9** Use "Public Websites" for Footprinting

**Lab 3.10** Use "Kartoo Visual Browser" for Footprinting a Company's Network

**Lab 3.11** Use "Yahoo People" for Footprinting an Individual

**Lab 3.12** Use "Intellius" for Footprinting an Individual

**Lab 3.13** Use Google Earth

**Lab 3.14** Mirror a Website

**Lab 3.15** Use E-Mail Tracker to track emails

**Lab 3.16** Search the Internet for E-Mail Addresses

**Lab 3.17** Use **http://finance.google.com/finance** to find the information of stocks, mutual funds, public and private companies.

**Lab 3.18** Use **http://finance.yahoo.com/** to get free stock quotes, up to date news, portfolio management resources, international market data, message boards, and mortgage rates.

## Module 04 – Google Hacking (Lab time: 20 minutes)

**Lab 4.1** Making Searching Even Easier topic in Google Guide whitepaper

**Lab 4.2** Go through Advanced Google Searching

**Lab 4.3** Field Searching whitepaper

**Lab 4.4** Go through Advanced Operators for Google search

**Lab 4.5** Visit the Website http://johnny.ihackstuff.com/index.php?module=prodreviews

## Module 05 – Scanning (Lab time: 50 minutes)

**Lab 5.1** Use NMAP to Portscan a Website

**Lab 5.2** Use AngryIP to Check for Live Hosts

**Lab 5.3** Scan the Network Using Hping2 for Windows

**Lab 5.4** Scan the Network Using NetScan Tools Pro

**Lab 5.5** Scan the Network Using SuperScan 4

**Lab 5.6** Scan the Network Using Floppyscan

**Lab 5.7** Banner Grabbing Using Telnet

**Lab 5.8** Banner Grabbing Using Netcraft

**Lab 5.9** HTTP Tunneling

**Lab 5.10** Use HoverIP to perform NsLookup queries, Trace route, Ping, and port scanning.

**Lab 5.11** Use Port Detect tool to find open/blocked ports on the target computer

## Module 06 - Enumeration (Lab time: 30 minutes)

**Lab 6.1** Connect via Null Session

**Lab 6.2** Use GetAcct to Enumerate Users

**Lab 6.3** Use SuperScan 4 to Enumerate Users

**Lab 6.4** Use SNMP Scanner

**Lab 6.5** Use Winfingerprint to Enumerate Services

**Lab 6.6** Use DumpSec tool to reveal shares over a null session with the target computer

**Lab 6.7** Use FreeNetEnumerator tool to enumerate computers on the target domain.

## Module 07 – System Hacking (Lab time: 1 hour)

**Lab 7.1** Use L0phtcrack to Bruteforce SAM Passwords

**Lab 7.2** Extract SAM Hashes Using Pwdump

**Lab 7.3** Privilege Escalation Using X.EXE

**Lab 7.4** Execute Commands on Remote Computer

**Lab 7.5** E-Mail Keylogger

**Lab 7.6** Use “Klogger” Keylogger

**Lab 7.7** Use Desktop Spy to Capture Screen Images

**Lab 7.8** NTFS Streams

**Lab 7.9** Use Fu Rootkit to Hide Files and Process

**Lab 7.10** Use Camera/Shy to View Hidden Files

**Lab 7.11** Use Spammimic to Hide Messages

**Lab 7.12** Use Snow to Hide Information

**Lab 7.13** Use Auditpol to Enable/Disable Auditing

**Lab 7.14** Use Alchemy Remote Executor to execute programs on remote network computers.

**Lab 7.15** Use Ardamax KeyLogger to capture user's activity and save it to an encrypted log file.

**Lab 7.16** Use Asterisk Key to view passwords hidden under asterisks.

## Module 08 Trojans and Backdoors (Lab time: 1 hour)

**Lab 8.1** Tini Trojan

**Lab 8.2** NetBus Trojan

**Lab 8.3** Netcat Trojan

**Lab 8.4** Beast Trojan

**Lab 8.5** Use Wrappers

**Lab 8.6** Proxy Trojan

**Lab 8.7** Atelier Web Commander

**Lab 8.8** Use TCPVIEW to Monitor the Network Connections

**Lab 8.9** What's on My Computer

**Lab 8.10** Use Process Viewer to View the Running Processes

**Lab 8.11** Use MSCONFIG to View the Startup Programs

**Lab 8.12** Use MD5SUM to Create Digital File Signatures

**Lab 8.13** Check the Registry for Trojan Startup Entries

## Module 09 Viruses and Worms (Lab time: 25 minutes)

**Lab 9.1** Write a Simple Virus

**Lab 9.2** Use Virus Construction Kits

**Lab 9.3** Virus Analysis Using IDA Pro

## Module 10 – Sniffers (Lab time: 45 minutes)



**Lab 10.1** Use Ethereal to Sniff the Network

**Lab 10.2** Use Windump to Sniff the Network

**Lab 10.3** Network View

**Lab 10.4** Ettercap

**Lab 10.5** Ettercap-NG (Next Generation)

**Lab 10.6** Mac Flooding

**Lab 10.7** DNS Poisoning

**Lab 10.8** EffeTech Sniffer

**Lab 10.9** Password Sniffer

**Lab 10.10** Can and Abel

**Lab 10.11** Packet Crafter

**Lab 10.12** SMAC – Spoofing MAC Address

**Lab 10.13**Use **AnalogXPacketMon Tool** to capture IP packets that pass through network interface - whether they originated from machine on which PacketMon is installed, or a completely different machine on network.

**Lab 10.14**Use **Colasoft MSN Monitor** to capture MSN Messenger conversations along with all related details, including usernames, usage statistics and more.

## Module 11 Social Engineering (Self Do Labs)

**Lab 11.1** Read Social Engineering Story

**Lab 11.**Intrusion Detection Systems bypass techniques whitepaper

**Lab 11.3** Identity Theft Assistance whitepaper

## Module 12 Phishing (Lab time: 30 minutes)

**Lab 12.1** Phishing Attack – Fake Address Bar

**Lab 12.2** Phishing Attack – Fake Status Bar

**Lab 12.3** Phishing Attack – Fake toolbar

**Lab 12.4** IP Address Conversion

**Lab 12.5** Go through Phishing History

**Lab 12.6** Spy Phishing whitepaper

**Lab 12.7** Why Phishing Works whitepaper

## Module 13 –Hacking Email Account (Self Do Labs)

**Lab 13.1** Tricks Used in Fraudulent Emails whitepaper

**Lab 13.2** Email Virus Propagation Model whitepaper

**Lab 13.3** Evolving Threat Environment whitepaper

**Lab 13.4** Sign-in Seal whitepaper

## Module 14 – Denial of Service (Lab time: 45 minutes)

**Lab 14.1** Freak88 – Distributed Denial of Service

**Lab 14.2** Ping of Death

**Lab 14.3** ImageWolf Bot

**Lab 14.4** DoS Attack Using Nemesys

**Lab 14.5** DoS Attack Using Panther

**Lab 14.6** DDOS Ping Attack

## Module 15 – Session Hijacking (Lab time: 30 minutes)

**Lab 15.1** Session Hijacking Analysis

**Lab 15.2** Session Hijacking Using Paros

## Module 16 Hacking Web Servers (Lab time: 45 minutes)

**Lab 16.1** Exploit Windows 2000 Server Unicode Vulnerability Using IISEXploit

**Lab 16.2** RPC Exploit

**Lab 16.3** Metasploit Exploit

**Lab 16.4** Vulnerability Assessment Using Shadow Security Scanner

**Lab 16.5** Nessus for Windows

**Lab 16.6** Microsoft Baseline Security Analyzer

**Lab 16.7** Hack Proofing Your Web Server whitepaper

**Lab 16.8** Go through CLIENT-SIDE ATTACKS

**Lab 16.9** Web Server Attacks whitepaper

## Module 17 - Web Application Vulnerabilities (Lab time: 45 minutes)

**Lab 17.1** E-Shopping Using Hidden Values

**Lab 17.2** Footprint a Website Using BlackWidow

**Lab 17.3** Footprint a Website Using Wget

**Lab 17.4** Footprint a Website Using Access Diver

**Lab 17.4** Unicode Strings

**Lab 17.5** Site Scope Tool

**Lab 17.6** SSL Digger Tool

## Module 18– Web Based Password Cracking Techniques (Lab time: 45 minutes)

**Lab 18.1** ObiWan Password Cracking Tool

**Lab 18.2** Brutus Password Cracking Tool

**Lab 18.3** Dictionary Maker

**Lab 18.4** SnadBoy – Password Revelation

**Lab 18.5** Cookie Spy

**Lab 18.6** Password Recovery Time SimulatorLab

**Lab 18.7** Easy Web Password

**Lab 18.8** Microsoft Password Checker

**Lab 18.9** RAR Password Cracker

## Module 19 SQL Injection (Lab time: 45 minutes)

**Lab 19.1** Juggybank SQL Injection Lab

**Lab 19.2** SQL Injection Whitepaper

## Module 20 Hacking Wireless Networks (Lab time: 25 minutes)

**Lab 20.1** AiroPeek

**Lab 20.2** WarDrive whitepaper

## Module 21 Physical Security (Lab time: 10 minutes)

**Lab 21.1** MIT Document

**Lab 21.2** Physical Security and Operations whitepaper

## Module 22 Linux Hacking (Lab time: 40 minutes)

**Lab 22.1** Ethical Hacking using BackTrack CD-ROM

**Lab 22.2** Security Evaluation of the Linux Operating System whitepaper

**Lab 22.3** Unreliable Guide To Hacking The Linux Kernel whitepaper

## Module 23 – Evading IDS, Firewalls & Honeypot (Lab time: 45 minutes)

**Lab 23.1** Install and run Snort

**Lab 23.2** Install and run TrapServer

**Lab 23.3** Install and run Atelier Web Firewall Tester

**Lab 23.4** Install and run KFSensor



## Module 24 Buffer Overflows (Lab time: 45 minutes)

**Lab 20.1** Compile and execute Simple Buffer Overflow program

**Lab 24.2** Stack Overflow and Heap Overflow whitepaper

**Lab 24.3** Buffer Overflow Exploits whitepaper

## Module 25 Cryptography (Self Do Labs)

**Lab 25.1** New Directions in Cryptography whitepaper

**Lab 25.2** How Digital Signature Technology Works whitepaper

**Lab 25.3** Signature Generation and Signature Verification whitepaper

## Module 26 Penetration Testing (Self Do Labs)

**Lab 26.1** Develop a penetration test plan whitepaper

**Lab 26.2** Penetration testing today whitepaper

**Lab 26.3** Network Vulnerability Scanning whitepaper

**Lab 26.4** Establishing Objectives whitepaper

## Module 27 Covert Hacking (Self Do Labs)

**Lab 27.1** Covert Channels whitepaper

**Lab 27.2** Firewall Piercing (Inside-Out Attacks) whitepaper

**Lab 27.3** Covert channels are the principle enablers in a DDoS attack whitepaper

**Lab 27.4** Covert channels whitepaper

## Module 30 Writing Exploits (Lab time: 45 minutes)

**Lab 30.1:** example1.c

**Lab 30.2:** example2.c

**Lab 30.3:** example3.c

**Lab 30.4:** shellcode.c

**Lab 30.5:** exit.c

**Lab 30.6:** testsc.c

**Lab 30.7:** exploit.c

## Module 34 Mac OS X Hacking (Self Do Labs)

**Lab 34.1** Security Hardening Guideline whitepaper

**Lab 34.2** Secure Default Settings whitepaper

**Lab 34.3** OS X Security Architecture whitepaper

**Lab 34.4** Mac OS X Hacking Poses Wide Risk… for Windows whitepaper

## Module 35 Hacking Routers, Cable Modems and Firewalls (Self Do Labs)

**Lab 35.1** Firewall Identification whitepaper

**Lab 35.2** Compromised Router Sniffing whitepaper

**Lab 35.3** Read Access management whitepaper

**Lab 35.4** 8 Steps to protect your Cisco router whitepaper

**Lab 35.5** How to Build a Console Port whitepaper

## Module 36 Hacking Mobile Phones, PDA and Handheld Devices (Self Do Labs)

**Lab 36.1** Quick start to taking control of an iPhone whitepaper

**Lab 36.2** 10 reasons not to buy an iphone whitepaper

**Lab 36.3** iPhone keyboarding tricks whitepaper

**Lab 36.4** iPhone hardware unlock whitepaper

**Lab 36.5** How to unlock an iPhone whitepaper

**Lab 36.6** The changing threat landscape whitepaper

**Lab 36.7** Understanding the threats to your mobile workforce whitepaper

**Lab 36.8** Security issues on mobile devices whitepaper

**Lab 36.9** Increased use of mobile devices in the workplace whitepaper

**Lab 36.10** Mobile Malware: Threats and Prevention whitepaper

## Module 37 Bluetooth Hacking (Self Do Labs)

**Lab 37.1** Bluetooth introduction whitepaper

**Lab 37.2** Key Agreement Protocol in Bluetooth whitepaper

**Lab 37.3** Overview on bluetooth technology whitepaper

**Lab 37.4** On-Line PIN cracking script whitepaper

**Lab 37.5** Key Replay Attack on improved bluetooth encryption whitepaper

## Module 38 VoIP Hacking (Self Do Labs)

**Lab 38.1** Introduction to VoIP Security whitepaper

**Lab 38.2** Internal Access whitepaper

**Lab 38.3** Security considerations for VoIP systems whitepaper

**Lab 38.4** VoIP building blocks whitepaper

**Lab 38.5** Reasons for VoIP security whitepaper

**Lab 38.6** Exploiting the VoIP network whitepaper

**Lab 38.7** Fun with online VoIP Hacking whitepaper

**Lab 38.8** Common VoIP security threats whitepaper

## Module 39 RFID Hacking (Self Do Labs)

**Lab 39.1** Introduction whitepaper

**Lab 39.2** RFID Background and Overview whitepaper

**Lab 39.3** The RFID threat whitepaper

## Module 40 – Spamming (Lab time: 15 minutes)

**Lab 40.1** AEVITA Stop SPAM email tool

**Lab 40.2** Purgy tool to block spam

**Lab 40.3** SpamEater tool

**Lab 40.4** Spytech Spam Agent

**Lab 40.5** Spam reader to extend Outlook functionality with a Bayesian spam filter

## Module 41 Hacking USB Devices (Self Do Labs)

**Lab 41.1** Hacking information whitepaper

## Module 42 Hacking Database Servers (Self Do Labs)

**Lab 42.1** SQL Server security concepts whitepaper

**Lab 42.2** Hacking Database Network Protocol whitepaper

**Lab 42.3** SQL Injection: Oracle versus Other Databases whitepaper

**Lab 42.4** Real-time database activity monitoring whitepaper

## Module 43 Cyber Warfare- Hacking, Al-Qaida and Terrorism (Self Do Labs)

**Lab 43.1** Cyber Terrorism whitepaper

**Lab 43.3** Definition: Terrorism and Cyber Terrorism

**Lab 43.4** Three Methods of Computer Attack

**Lab 43.5** Cyberterrorism-What Is It and Who Does It? whitepaper

**Lab 43.6** Computers-the weapons of the cyberterrorist whitepaper

**Lab 43.7** Cyberwar Strategies whitepaper

## Module 44 - Internet Content Filtering Techniques (Lab time: 15 minutes)

**Lab 44.1** Ad Cleaner tool

**Lab 44.2** AdsGone popup killer

**Lab 44.3** AdSubtract tool

## Module 45 – Privacy on Internet (Lab time: 15 minutes)

**Lab 45.1** HistoryKill

**Lab 45.3** Privacy Eraser

**Lab 45.5** TraceEraser Pro

## Module 46 - Securing Laptop Computers (Lab time: 15 minutes)

**Lab 46.1** Cryptex tool

**Lab 46.2** Data Protection Software

**Lab 46.3** Private disk multifactor

**Lab 46.4** Securing your Laptop Computers whitepaper

**Lab 46.5** Securing Your Windows Laptop whitepaper

## Module 47 Spying Technologies (Self Do Labs)

**Lab 47.1** Spyware whitepaper

**Lab 47.2** The science of spying whitepaper

**Lab 47.3** Stop the corporate spying whitepaper

## Module 48 Corporate Espionage- Hacking Using Insiders (Self Do Labs)

**Lab 48.1** Modeling techniques whitepaper

**Lab 48.2** The insider threat whitepaper

**Lab 48.3** Corporate Espionage whitepaper

## Module 49 Creating Security Policies (Self Do Labs)

**Lab 49.1** Remote Access Policy whitepaper

**Lab 49.2** Information Security Guidelines whitepaper

**Lab 49.3** Implementing Internet Firewall Security Policy whitepaper

**Lab 49.4** Password Policy whitepaper

**Lab 49.5** Developing a Security Policy whitepaper

**Lab 49.6** Network Security Policy whitepaper

## Module 50 - Software Piracy and Warez (Lab time: 15 minutes)

**Lab 50.1** Software license manager

**Lab 50.2** Quick License Manager

**Lab 50.3** Crack tool

**Lab 50.4** The Challenges of Regulating Warez Trading whitepaper

## Module 51 Hacking and Cheating Online Games (Self Do Labs)

**Lab 51.1** Avoiding Online Game Risks whitepaper

## Module 52 – Hacking RSS and Atom (Lab time: 15 minutes)

**Lab 52.1** Perseptio FeedAgent

**Lab 52.2** RssFeedEater

**Lab 52.3** RSS Submit

**Lab 52.4** FeedDemon

## Module 53 Hacking Web Browsers (Firefox, IE) (Self Do Labs)

**Lab 53.1** Firefox Hacks whitepaper

**Lab 53.2** Java Security Mechanisms whitepaper

**Lab 53.3** Browser Based Attacks on Tor whitepaper

**Lab 53.4** Turning Firefox to an Ethical Hacking Platform whitepaper

## Module 54 Proxy Server Technologies (Self Do Labs)

**Lab 54.1** Changing Proxy Server whitepaper

**Lab 54.2** Proxy server Access Limitations whitepaper

**Lab 54.3** Reverse Proxy Patterns whitepaper

**Lab 54.4** Socks for Proxy whitepaper

## Module 55 Preventing Data Loss (Lab time: 15 minutes)

**Lab 55.1** MailMarshal

**Lab 55.2** Marshal EndPoint Security

**Lab 55.3** WebMarshal Console

**Lab 55.4** Data Loss Prevention Technology whitepaper

**Lab 55.5** How to Prevent Data loss whitepaper

## Module 56 Hacking Global Positioning System (GPS) (Self Do Labs)

**Lab 56.1** GPS whitepaper

**Lab 56.2** OpenSource GPS whitepaper

**Lab 56.3** Introduction to GPS whitepaper

**Lab 56.4** Introduction to GPS and Paper Maps whitepaper

## Module 57 Computer Forensics and Incident Handling (Self Do Labs)

**Lab 57.1** Computer Crime and the Emergence of Computer Forensics whitepaper

**Lab 57.2** Ethics in computer forensics whitepaper

**Lab 57.3** Organizing a Computer Security Incident Response Capability whitepaper

**Lab 57.4** Computer Forensics whitepaper

# Module Briefing

## 1. Introduction to Ethical Hacking

Module Brief:

This module offers to professionals an understanding of the subject "Ethical Hacking". It is important to bear in mind that hackers break into a system for various reasons and purposes. Therefore, it is important to comprehend how malicious hackers exploit systems and the probable reasons behind the attacks.

As Sun Tzu put it in the 'Art of War', "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." It is the duty of system administrators and network security professionals to guard their infrastructure against exploits by knowing the enemy (the malicious hacker(s), who seek to use that very infrastructure for illegal activities).



## 2. Hacking Laws

Module Brief:

This module discusses various Cyber Laws that are enforced in countries around the globe. SPY ACT, U.S. Federal Laws, United Kingdom's Cyber Laws, European Laws, Japan's Cyber Laws, Australia Cybercrime Act 2001, and Indian Law: The Information Technology Act, Germany's Cyber Laws, Singapore's Cyber Laws, Belgium Law, Brazilian Law, Canadian Laws, France Laws and Italian Laws are discussed.

## 3. Footprinting

Module Brief:

Note that there is no 'one way' for hackers to approach a system. The intent behind their activities cannot be foreknown and all activity must be treated as a threat. Note that the focus of this course is not to teach the finer aspects of hacking, rather to emphasize on the vulnerability – threat – attack methods – tools – countermeasures threads of discussion.

Therefore, the focus is not on the diverse details of 'how to' hack, rather the discussion is focused on where one must look for vulnerabilities, what threat the vulnerability poses, what are the ways in which a cracker can exploit the vulnerability, and what countermeasures should be advocated in the light of the threat. The objective of using tools is to save on time and resources, and defend resources in a proactive and efficient manner. It is assumed that readers possess good programming skills and are familiar with various technical environments. There are several tools available to the hacker and may range from simple code compilation software to source code text files available on the Internet.

## 4. Google Hacking

Module Brief:

Critical information of various websites can be obtained by using a mix of few operators in the search field of Google. This module showcases how an attacker can gather vital information related to web servers and vulnerabilities present on the websites.

## 5. Scanning

Module Brief:

After completing this module, one can gain an in-depth understanding of the hacking techniques involved in scanning and, subsequently, fingerprinting. It is strongly recommended that professionals possess a firm understanding of the various protocols such as TCP, UDP, ICMP, and IP to comprehend this module. Once an attacker has identified his/her target system and does the initial reconnaissance, as discussed in the previous module on foot printing, he/she concentrates on getting a mode of entry into the target system. It should be noted that scanning is not limited to intrusion alone. It can be an extended form of reconnaissance where the attacker learns more about his/her target, such as what operating system is used, the services that are being run on the systems and whether any configuration lapses can be identified. The attacker can then strategize his/her attack factoring these aspects.

## 6. Enumeration

Module Brief:

This module introduces the enumeration phase of hacking to the reader. It details different aspects of enumeration. The reader is urged to note that there isn't one sure way for hackers to approach a system. This is the basis behind stating that while countermeasures are suggested here, they are proposed in the light of the generic approach of hackers toward a system.

## 7. System Hacking

Module Brief:

The preceding modules dealt with the progressive intrusion that an attacker makes towards his/her target system(s). One should bear in mind that this does not indicate a culmination of the attack. After completing this module, the professionals will be able to deal with various methods of password cracking, password attacks, various types of password cracking tools, privilege escalating, role of key loggers and other spy ware that the attackers use for hiding files and methods for erasing evidences.

## 8. Trojans and Backdoors

Module Brief:

On completion of this module, professionals will become adept at dealing with malicious code in the form of Trojans and backdoors. This Module contains the familiarity with Trojan definition and its working, Effect of Trojan on Business, Types of Trojan and what Trojan creators look for? Different type of ways a Trojan can get into a system and indications of Trojan attack, some

popular Trojans and ports they use. How to determine that what ports are "listening" and How to avoid a Trojan infection? Type of different Trojans found in the wild, Wrappers, Tools for hacking, ICMP Tunneling and Anti-Trojans.

## 9. Viruses and Worms

Module Brief:

Computer virus is perceived as threat to both business and personnel. A virus at some point of time has infected most businesses worldwide. This module looks into the details of a computer virus; its function; classification and the manner in which it affects systems. This module will enhance the knowledge of various countermeasures one has to take against virus infections. Once a virus is activated it will infect other files on the computer with itself, Virus can infect outside machines only with the assistance of humans. Writing a simple but powerful virus is showcased in this module. The module also discusses the various countermeasures that need to be taken against virus.

## 10. Sniffers

Module Brief:

This module will explain the fundamental concepts of sniffing and its use in hacking activities. This module highlights the importance of sniffers for a network administrator. Various tools and techniques used in securing the network from anomalous traffic are explained. Professionals are advised to read the references cited in earlier modules regarding various network protocols for a better understanding of this module.

## 11. Social Engineering

Module Brief:

If you have seen the movie "War Games", you've already seen social engineering in action. It must be pointed out that the information contained in this chapter is for the purpose of overview. While it points out fallacies and advocates effective countermeasures, the possible ways to extract information from another human being

are only restricted by the ingenuity of the attacker's mind. While this aspect makes it an art and the psychological nature of some of these techniques makes it a science, the bottom line is that there is no one defense against social engineering; only constant vigilance can circumvent some of these advances.



## 12. Phishing and Identity Theft

Module Brief:

This module showcases different phishing attacks and tools to prevent them.

## 13. Hacking Email Accounts

Module Brief:

This module reveals different methods to hack email accounts and tools to prevent such attacks

## 14. Denial-of-Service

Module Brief:

This module looks at various aspects of denial-of-service attacks. The module starts with a discussion on denial-of-service attacks. Real world scenarios are cited to highlight the implications of such attacks.

Distributed denial-of-service attacks and the various tools to launch such attacks have been included to bring into spotlight the technologies involved. The countermeasures for preventing such attacks have also been taken into consideration. Viruses and worms have been briefly discussed to highlight their use in such attacks.

## 15. Session Hijacking

Module Brief:

This module covers the various hacking technologies that attackers use for session hijacking. It deals with spoofing methods, the three-way TCP handshake, and how attackers use these methods for the man-in-the-middle attacks. Various tools which can be used for this purpose have been highlighted to give professionals an insight into the concept of session hijacking. Finally, the countermeasures to prevent session hijacking have been discussed.

## 16. Hacking Web Servers

Module Brief:

The Internet is probably where security or the lack of security is seen the most. Often, a breach in security causes more damage in terms of goodwill than the actual quantifiable loss. This makes securing web servers critically important to the normal functioning of an organization. Most organizations consider their web presence to be an extension of themselves.

This module attempts to highlight the various security concerns in the context of web servers. It must be noted that exploring web server security is a vast domain and to delve into the finer details of the discussion is beyond the scope of this module. Readers are encouraged to supplement this module by following vulnerability discussions on various mailing lists such as Bugtraq and security bulletins that third party vendors issue for various integrated components.

## 17. Web Application Vulnerabilities

Module Brief:

The main objective of this module is to show the various kinds of vulnerabilities that can be discovered in web applications. The attacks exploiting these vulnerabilities will also be highlighted. The various hacking tools that can be used to compromise the web applications have been included, in order to showcase the technologies involved. Here, it should be mentioned that a single tool could be used to exploit multiple vulnerabilities in web applications.

The module starts with a detailed description of the web server application. The anatomy of the attack reveals the various steps involved in a planned attack. The different types of attacks that can take place on the web applications have been dealt with. The various tools that attackers use have been discussed to explain the way they exploit the vulnerabilities in Web applications. The countermeasures that can be taken to thwart any such attacks have also been highlighted

## 18. Web-Based Password Cracking Techniques

Module Brief:

Authentication is any process by which one verifies that someone is who they claim to be. Typically, this involves a user name and a password. It can also include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints.

In this module, the topics in the context of web-based authentication will be discussed. The objective is to familiarize the professionals with commonly used authentication methods and how these methods can be worked around, under certain circumstances.

## 19. SQL Injection

Module Brief:

In this module, professionals will be introduced to the concept of SQL injection and how an attacker can exploit this attack methodology on the Internet. The professionals will familiar with a variety of SQL Injection techniques, which is useful to gain access to a system. The module also focuses on SQL Injection Scripts, SQL Injection in Oracle, SQL Injection in MySQL, prevention and the countermeasures against SQL Injection.

## 20. Hacking Wireless Networks

Module Brief:

This module will familiarize professionals with the basic tools to detect a wireless network, hack a wirePage less network, the business implications of wireless hacks, and ways to protect a wireless network.

This module discusses about Wireless Networking Concept, the effect of wireless attack on business, basics of Wireless Networks, types of Wireless Network and Setting up a WLAN, to detect a WLAN and getting into a WLAN. Different types of Wireless Attacks and Hacking Tools. The module also discusses various countermeasures such as the WIDZ and RADIUS model against wireless attacks

## 21. Physical Security

Module Brief:

Physical security is as important as network security. Until now, most of the firms concentrated more on network security overlooking the loopholes in physically securing the organization's environment. There has been an increase in laptop thefts across the globe. The importance of securing computing assets physically cannot be overemphasized. Awareness of the need for physical security must be communicated to employees through appropriate security policies. These are simple but important steps to avoid any tampering of data as well as unauthorized access to systems. This module will look into the details of physical security and advocate measures to be taken to strengthen physical security.

## 22. Linux Hacking

Module Brief:

The advent of Linux was the true genesis of the open source movement. Backed by programmers who believed in breaking away from the proprietary movement for the right reasons, Linux made inroads into corporate world computing. Linux has evolved from being labeled as an unfriendly, unreliable operating system to an operating sysPage tem that is user friendly and used for supporting many critical applications.

The security issues related to Linux gains more attention when the Linux increases. Linux was a favorite among crackers and is so, still. While Linux has evolved to a robust operating system, the complex structure of Linux paves the way for security related threats. Today, several servers

around the globe are hosted on Linux servers. One of the primary reasons behind this is the inherent security offered by the platform. However, today there is as much vulnerability in Linux as in proprietary systems leading to their compromise by hackers. This module will look into various aspects of security related to Linux and other related issues.

## 23. Evading IDS, Firewalls and Detecting Honey Pots

Module Brief:

Today, hacking and computer system attacks are common, making the importance of intrusion detection and active protection all the more relevant. This module discusses Intrusion Detection Systems (IDS), Firewalls and Honeypots. After the completion of this module, professionals will be familiar with IDS, Firewalls and Honeypots.

## 24. Buffer Overflows

Module Brief:

Various security concerns, attack methods and countermeasures have been discussed in the preceding modules. Buffer overflow attacks have been a source of worry from time to time. This module looks at different aspects of buffer overflow exploits.

## 25. Cryptography

Module Brief:

Having dealt with various security concerns and countermeasures in the preceding modules, it is obvious that cryptography, as a security measure, is here to stay. This module will explain the use of cryptography over the Internet through.

This module will also explain the effort required to crack these encryption techniques and explore attacker methodologies, if any, which are relevant to the discussion. It is to be noted that, encryption can no longer be exempted while conducting e-commerce. It will always have its share of security concerns because of its significance in e-commerce. It cannot guarantee foolproof security on its own basis. It must be combined with good security policies and practices if an organization needs to protect its information assets and extend it to its stakeholders.

## 26. Penetration Testing

Module Brief:

This module marks a departure from the approach followed in earlier modules, where Professionals were encouraged to think 'out-of-the-box'. Hacking as it was defined originally portrayed a streak of genius or brilliance in the ability to conjure previously unknown ways of doing things. In this context, to advocate a methodology that can be followed to simulate a real-world hack through ethical hacking or penetration testing might come across as a contradiction. However, the reason behind advocating a methodology in penetration testing arises from the fact that most hackers follow a common underlying approach when it comes to penetrating a system.

In the context of penetration testing, the tester is limited by resources, namely time, skilled resources, access to equipment etc. as outlined in the penetration testing agreement. The paradox of penetration testing is in the fact that inability to breach a target does not necessarily indicate the absence of vulnerability. In other words, to maximize the returns from a penetration test, the tester must be able to apply his skills to the resources available in such a manner that the attack area of the target is reduced as much as possible. The community gives various names to these stages or phases to indicate various activities. The objective of this module is to frame a guideline that a penetration tester can adopt while doing a penetration test. The module is by no means an all-exhaustive one as it is not possible to map all the approaches that a hacker can adopt. It is not necessary that the test progress in the order of the steps outlined.

## 27. Covert Hacking

## 28. Writing Virus Codes

## 29. Assembly Language Tutorial

## 30. Exploit Writing

## 31. Smashing the Stack for Fun and Profit

## 32. Windows Based Buffer Overflow Exploit Writing

## 33. Reverse Engineering

## 34. Mac OS X Hacking

Module Brief:

This module showcases vulnerabilities in MAC OS X such as Crafted URL, CoreText Uninitialized Pointer, ImageIO Integer overflow, DirectoryService, iChat UPnP buffer overflow and many more are presented in this module which is used for hacking MAC OS X. Viruses and worms in MAC OS X are discussed in this module.

Anti-virus tools such as VirusBarrier, McAfee Virex for Macintosh, Sophos Endpoint Security and Control, and Norton Internet Security are discussed with their features. MAC OS X security tools MacScan, ClamXav,

IPNetsentryX, and FileGuard are discussed in this module.

## 35. Hacking Routers, Cable Modems and Firewalls

Module Brief:

This module explains different vulnerabilities in the networking devices and how to exploit the same.

## 36. Mobile Phone and Handheld Devices (PDAs) Hacking

Module Brief:

This module discusses about the threats to mobile devices, vulnerabilities in mobile devices and attacks against mobile devices. iPhone and other PDA hacking tools are showcased along with tools that ensure security to these devices.

## 37. Bluetooth Hacking

Module Brief:

This module explains different ways to compromise Bluetooth enabled devices. Bluejacking, BlueSpam, BlueSnarfing, BlueBug Attack, Blueprinting and other attacks are dealt in detail. Worms and viruses that infect Bluetooth enabled devices are also listed.

## 38. VoIP Hacking

Module Brief:

The Denial of Service attack, Replay Attack, ARP Spoofing Attack, H.323-Specific Attack, SIP Attacks are few VoIP attacks showcased in this module.

## 39. RFID Hacking

Module Brief:

RFID technology, its components and their collisions are mentioned in this module. This module looks into details of RFID security and privacy threats and protection against RFID attacks. Writing a simple but powerful

RFID virus and worm are showcased in this module. Vulnerabilities in RFID-enabled credit cards and RFID security controls are discussed in this module.



## 40. Spamming

Module Brief:

This module deals with the spamming attack methods used by spammers and different anti-spam techniques used to stop the spam. A statistical view tells about the top spammers, the top worst spam service ISPs and the top spamming countries. Various anti-spam techniques and tools are showcased in this module.

## 41. Hacking USB Devices

Module Brief:

This module discusses various USB devices and their privacy issues. Electrical and software attacks of USB devices are mentioned in this module. USB Attack on Windows, viruses and worms which spread through USB devices are discussed in this module. Some of the top USB devices hacking tools such as USB Dumper, USB Switchblade, and USB Hacksaw are discussed.

Tools such as MyUSBonly, USBDeview, USB-Blocker, USB CopyNotify, USB File Guard, Advanced USB Port Monitor and other USB security tools that protect user privacy are listed in this module.

## 42. Hacking Database Servers

Module Brief:

This module depicts how database servers are vulnerable to attacks. This module also deals with the security issues and type of Database attacks. This module gives an idea how attackers after getting the DBA privileges, attack the database.

## 43. Cyber Warfare- Hacking, Al-Qaida and Terrorism

Module Brief:

This module defines Cyber terrorism, Cyber crime and criminal impacts. It also describes the common forms of these terrorist attacks on the Internet such as Distributed Denial of Service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. This module shows the different types of Cyber warfare attacks.

This module gives an idea how Terrorists use Electronic Jihad and use their proprietary encryption tool "Mujahedeen Secrets Encryption Program" to spread terrorism over the Internet.



## 44. Internet Content Filtering Techniques

Module Brief:

In today's networked world Internet filters have become a necessary mean for Organizations to restrict specific content access over the Internet. Many tools to filter Internet content are discussed in this module. Internet safety guidelines for children are also mentioned in this module.

## 45. Privacy on Internet- Anonymous

Module Brief:

This module familiarizes the reader with privacy threats on the Internet and Internet privacy tools. Internet, proxy, and email privacy are mentioned in this module. Different privacy threats such as cookies, IRC, web browsers, electronic commerce, and web bugs are discussed. This module demonstrates various anonymizer tools which protect privacy while surfing.. This module also discusses step by step procedure of protecting search privacy and tips for online privacy.

## 46. Securing Laptop Computers

Module Brief:

Securing Laptop computers module familiarizes you with the different types of laptop threats. It features various techniques that can be used to protect your Laptop from different thefts (Example: Fingerprint reader, Face Recognition). It shows the different hardware laptop security devices and the software security tools that help you protect laptop data. This module also lists security tips that will be advantageous to restrict laptop thefts.

## 47. Spying Technologies

Module Brief:

The module introduces the reader to all the spying technologies that might be used by an attacker against to extract sensitive information. It also lists anti-spying tools to mitigate these threats.

## 48. Corporate Espionage- Hacking Using Insiders

Module Brief:

This module discusses corporate espionage and different type of insider attacks. Countermeasures to these attacks are mentioned.

## 49. Creating Security Policies

Module Brief:

This module explains about creating security policies which help to protect network infrastructures of your organization.

This module also discusses the key elements of security policy, goals of security policy roles of security policy, concepts of security policy, classifications of security policy and different types of security policies.

## 50. Software Piracy and Warez

Module Brief:

Software Piracy is illicit copying and distribution of software for personal or commercial use.

This module explains about Software Activation Process, Piracy, Impacts of Piracy, Piracy Blocking and Piracy over the Internet It also introduces the Warez and its types which are made available on the Internet by the crackers and the techniques to distribute the Warez. It also includes security tools which are used to protect software.

## 51. Hacking and Cheating Online Games

Module Brief:

This module highlights basic threats in online gaming, cheating in online computer games, types of exploits,

example of popular game exploits, and stealing online game passwords.

## 52. Hacking RSS and Atom

Module Brief:

RSS and Atom feeds offer users with updated web content and news. This module briefs you on how to build a feed aggregator, how to monitor the Server with Feeds, how to track changes in open source projects. It also explains about the risks involved like Remote Zone Risks, Local Zone Risk, and Reader Specific Risks. It lists a set of tools that are used to create and keep the RSS and Atom feeds up-to-date. Security measures that should be taken to keep the RSS and Atom feeds secured are mentioned in this module.



## 53. Hacking Web Browsers (Firefox, IE)

Module Brief**:**

Hacking Firefox using Firefox spoofing, information leak and password vulnerabilities are explained.

Different browser settings and browser security features are mentioned in this module. Different vulnerabilities present in Opera, Safari and Netscape are described.

## 54. Proxy Server Technologies

Module Brief:

This module discusses the role of proxy server, and different types of proxy servers. Different proxy server technologies are mentioned in this module.

## 55. Data Loss Prevention

Module Brief:

This module explains you about the steps that need to be taken when the data is lost unexpectedly. This module tells about how the data can be lost and the ways that are to be followed to prevent the data loss. This module showcases various tools that can prevent data loss.

## 56. Hacking Global Positioning System (GPS)

Module Brief:

This module introduces Differential GPS (DGPS), Wide Area Augmentation System (WAAS), European Geostationary Navigation Overlay Service (EGNOS), Local Area Augmentation System (LAAS), Geometric Dilution of Precision (GDOP), and Signal to Noise Ratio (SNR). This module introduces Secret Startup Commands, Firmware Hacking, Waypoints, GPS Tools, and Security Tools.



## 57. Computer Forensics and Incident Handling

Module Brief:

"Forensic Computing is the science of capturing, processing and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law."

This module introduces computer forensics and discusses incident handling steps.

## 58. Credit Card Frauds

Module Brief:

This module introduces E-Crimes and describes how credit card frauds occur. This module highlights effective steps to be taken by credit card users to protect from credit card fraud.

## 59. How to Steal Passwords

Module Brief:

This module lists different tools to steal passwords and effective countermeasures against the same.

## 60. Firewall Technologies

Module Brief:

This module lists various vendors that provide firewall technologies.

# CEH v6 Exam Objectives

Exam Code: 312-50

No. of questions: 150

Duration: 4 hours

Passing score: 70%

Delivery: The CEH exam is available at Prometric and VUE centers



## Introduction to Ethical Hacking

- Understand Ethical Hacking terminology
- Define the Job role of an ethical hacker
- Understand the different phases involved in ethical hacking
- Identify different types of hacking technologies
- List the 5 stages of ethical hacking?
- What is hacktivism?
- List different types of hacker classes
- Define the skills required to become an ethical hacker
- What is vulnerability research?
- Describe the ways in conducting ethical hacking
- Understand the Legal implications of hacking

## Hacking Laws

- Understand U.S. Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)
- Understand 18 U.S.C. § 1030 US Federal Law
- Understand Federal Managers Financial Integrity Act of 1982

- Understand The Freedom of Information Act 5 U.S.C. § 552
- Understand Federal Information Security Management Act (FISMA)
- Understand The Privacy Act Of 1974 5 U.S.C. § 552a
- Understand USA Patriot Act of 2001



## Footprinting

- Define the term Footprinting
- Describe information gathering methodology
- Describe competitive intelligence
- Understand DNS enumeration
- Understand Whois, ARIN lookup
- Identify different types of DNS records
- Understand how traceroute is used in Footprinting
- Understand how e-mail tracking works
- Understand how web spiders work

## Google Hacking

- Define Google hacking
- What a hacker can do with vulnerable site
- How to use Google as a Proxy Server
- What is Google Hacking Database (GHDB)
- Understand Traversal Techniques

## Scanning

- Define the term port scanning, network scanning and vulnerability scanning

- Understand the CEH scanning methodology
- Understand Ping Sweep techniques
- Understand nmap command switches
- Understand SYN, Stealth, XMAS, NULL, IDLE and FIN scans
- List TCP communication flag types
- Understand War dialing techniques
- Understand banner grabbing and OF fingerprinting techniques
- Understand how proxy servers are used in launching an attack
- How does anonymizers work
- Understand HTTP tunneling techniques
- Understand IP spoofing techniques

**Enumeration**

- What is Enumeration?
- What is meant by null sessions
- What is SNMP enumeration?
- What are the steps involved in performing enumeration?

**System Hacking**

- Understanding password cracking techniques
- Understanding different types of passwords
- Identifying various password cracking tools
- Understand Escalating privileges
- Understanding keyloggers and other spyware technologies
- Understand how to Hide files

- Understanding rootkits
- Understand Steganography technologies
- Understand how to covering your tracks and erase evidences



### Trojans and Backdoors

- What is a Trojan?
- What is meant by overt and covert channels?
- List the different types of Trojans
- What are the indications of a Trojan attack?
- Understand how "Netcat" Trojan works
- What is meant by "wrapping"
- How does reverse connecting Trojans work?
- What are the countermeasure techniques in preventing Trojans?
- Understand Trojan evading techniques

### Viruses and Worms

- Understand the difference between an virus and a Worm
- Understand the types of Viruses
- How a virus spreads and infects the system
- Understand antivirus evasion techniques
- Understand Virus detection methods

### Sniffers

- Understand the protocol susceptible to sniffing
- Understand active and passive sniffing

- Understand ARP poisoning
- Understand ethereal capture and display filters
- Understand MAC flooding
- Understand DNS spoofing techniques
- Describe sniffing countermeasures

## Social Engineering

- What is Social Engineering?
- What are the Common Types of Attacks
- Understand Dumpster Diving
- Understand Reverse Social Engineering
- Understand Insider attacks
- Understand Identity Theft
- Describe Phishing Attacks
- Understand Online Scams
- Understand URL obfuscation
- Social Engineering countermeasures

## Phishing and Identity Theft

- What are the reasons for successful phishing
- Understand different phishing methods
- Understand the phishing process
- Understand the type of phishing attacks
- Phishing countermeasures

### Hacking Email Accounts

- What are the different ways to get information of email account
- What do you understand by cookie stealing
- Understand password phishing
- Email security

### Denial-of-Service

- Understand the types of DoS Attacks
- Understand how DDoS attack works
- Understand how BOTs/BOTNETS work
- What is “smurf ” attack
- What is “SYN” flooding
- Describe the DoS/DDoS countermeasures

### Session Hijacking

- Understand Spoofing vs. Hijacking
- List the types of Session Hijacking
- Understand Sequence Prediction
- What are the steps in performing session hijacking
- Describe how you would prevent session hijacking

### Hacking Web Servers

- List the types of web server vulnerabilities
- Understand the attacks Against Web Servers
- Understand IIS Unicode exploits

- Understand patch management techniques
- Understand Web Application Scanner
- What is Metasploit Framework?
- Describe Web Server hardening methods

## Web Application Vulnerabilities

- Understanding how web application works
- Objectives of web application hacking
- Anatomy of an attack
- Web application threats
- Understand Google hacking
- Understand Web Application Countermeasures

## Web-Based Password Cracking Techniques

- List the Authentication types
- What is a Password Cracker?
- How does a Password Cracker work?
- Understand Password Attacks - Classification
- Understand Password Cracking Countermeasures

## SQL Injection

- What is SQL injection?
- Understand the Steps to conduct SQL injection
- Understand SQL Server vulnerabilities
- Describe SQL Injection countermeasures

## Hacking Wireless Networks

- Overview of WEP, WPA authentication systems and cracking techniques
- Overview of wireless Sniffers and SSID, MAC Spoofing
- Understand Rogue Access Points
- Understand Wireless hacking techniques
- Describe the methods in securing wireless networks

## Physical Security

- Physical security breach incidents
- Understanding physical security
- What is the need for physical security?
- Who is accountable for physical security?
- Factors affecting physical security

## Linux Hacking

- Understand how to compile a Linux Kernel
- Understand GCC compilation commands
- Understand how to install LKM modules
- Understand Linux hardening methods

## Evading IDS, Firewalls and Detecting Honey Pots

- List the types of Intrusion Detection Systems and evasion techniques
- List firewall and honeypot evasion techniques

## Buffer Overflows

- Overview of stack based buffer overflows
- Identify the different types of buffer overflows and methods of detection
- Overview of buffer overflow mutation techniques

## Cryptography

- Overview of cryptography and encryption techniques
- Describe how public and private keys are generated
- Overview of MD5, SHA, RC4, RC5, Blowfish algorithms

## Penetration Testing

- Overview of penetration testing methodologies
- List the penetration testing steps
- Overview of the Pen-Test legal framework
- Overview of the Pen-Test deliverables
- List the automated penetration testing tools