

Certified Ethical Hacker (CEHv6.1)

Course Content:

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-Reconnaissance
- Reconnaissance Types
- Phase2-Scanning
- Phase3-Gaining Access
- Phase4-Maintaining Access
- Phase5-Covering Tracks
- Types of Hacker Attacks
- Operating System attacks
- Application-level attacks
- Shrink Wrap code attacks
- Misconfiguration attacks
- 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: 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 Whols 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 3: 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
- POf – Banner Grabbing Tool
- pOf for Windows
- Httpprint Banner Grabbing Tool
- Tool: Miart HTTP Header
- Tools for Active Stack Fingerprinting
- Xprobe2
- Ringv2
- Netcraft
- Disabling or Changing Banner
- IIS Lockdown Tool
- Tool: ServerMask
- Hiding File Extensions
- Tool: PageXchanger
- Vulnerability Scanning
- Bidiblah Automated Scanner
- Qualys Web Based Scanner
- SAINT
- ISS Security Scanner
- Nessus
- GFI Languard
- Security Administrator's Tool for Analyzing Networks (SATAN)
- Retina
- Nagios
- PacketTrap's pt360 Tool Suite
- NIKTO

- SAFESuite Internet Scanner, IdentTCPScan
- Draw Network Diagrams of Vulnerable Hosts
- 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
- HTTPPort
- Spoofing IP Address
- Spoofing IP Address Using Source Routing
- Detection of IP Spoofing
- Despoof Tool

- Scanning Countermeasures
- Tool: SentryPC

Module 4: Enumeration

- Overview of System Hacking Cycle
- What is Enumeration?
- Techniques for Enumeration
- NetBIOS Null Sessions
- 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 5: 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: LOphtrcrack
- 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
- DCPD – Hide an Operating System
- Tool: Camera/Shy
- www.spammimic.com
- Tool: Mp3Stego
- Tool: Snow.exe
- Steganography Tool: Fort Knox
- Steganography Tool: Blindside
- Steganography Tool: S- Tools
- Steganography Tool: Steghide
- Tool: Steganos
- Steganography Tool: Pretty Good Envelop
- Tool: Gifshuffle
- Tool: JPHIDE and JPSEEK
- Tool: wbStego
- Tool: OutGuess
- Tool: Data Stash
- Tool: Hydan
- Tool: Cloak
- Tool: StegoNote
- Tool: Stegomagic
- Steganos Security Suite
- C Steganography
- Isosteg
- FoxHole
- 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 6: 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 7: 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: Dnssppooof
- Linux Tool: Dsniff
- Linux Tool: Filesnarf
- Linux Tool: Mailsnarf
- Linux Tool: Msgsnarf
- Linux Tool: Sshmitm
- Linux Tool: Tcpcill
- Linux Tool: Tcpcnice
- 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
- Sniphire
- 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 8: 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 9: 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 10: 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 11: 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
- Opware 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 12: 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 13: 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
- LOphtCrack (LC4)
- John the Ripper
- Brutus
- ObiWaN
- Authforce
- Hydra
- Cain & Abel
- RAR
- Gammalog
- WebCracker
- Munga Bunga
- PassList
- SnadBoy
- MessenPass
- Wireless WEP Key Password Spy
- RockXP
- Password Spectator Pro
- Passwordstate
- Atomic Mailbox Password Cracker

- Advanced Mailbox Password Recovery (AMBPR)
- Tool: Network Password Recovery
- Tool: Mail PassView
- Tool: Messenger Key
- Tool: SniffPass
- WebPassword
- Password Administrator
- Password Safe
- Easy Web Password
- PassReminder
- My Password Manager
- Countermeasures

Module 14: 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)
- Osq -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 15: 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 16: 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.Newworld
- 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
- Socketsheld
- 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 17: 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 18: 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: LSOFS
- 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 19: 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 Intrusion 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 HTTP Tunnel
- Placing Backdoors through Firewalls
- Hiding Behind a Covert Channel: LOKI
- Tool: NCovert
- ACK Tunneling
- Tools to breach firewalls
- Common Tool for Testing Firewall and IDS
- IDS testing tool: 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 Honey pots
- Tools to Detect Honey pots
- What to do when hacked

Module 20: 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 21: 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 Hash 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 22: Introduction to Penetration Testing