Ethical Hacking & Countermeasures

EC-Council

Hackers are here. Where are you?

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help.

The term "hacker" has a dual usage in the computer industry today. Originally, the term was defined as:

HACKER *noun*. 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

This complimentary description was often extended to the verb form "hacking," which was used to describe the rapid crafting of a new program or the making of changes to existing, usually complicated software.

Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of “computer criminal,” the media began using the term “hacker” to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a “hacker” was originally meant as a compliment, computer security professionals prefer to use the term “cracker” or “intruder” for those hackers who turn to the dark side of hacking. There are two types of hackers “ethical hacker” and “criminal hacker”.

What is Ethical Hacking?

With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being “hacked.” At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses.

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these “tiger teams” or “ethical hackers” would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems’ security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

Who are Ethical Hackers?

"One of the best ways to evaluate the intruder threat is to have an independent computer security professionals attempt to break their computer systems"

Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy. While testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses. During an evaluation, the ethical hacker often holds the "keys to the company," and therefore must be trusted to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation requires that strong measures be taken to ensure the security of the systems being employed by the ethical hackers themselves: limited-access labs with physical security protection and full ceiling-to-floor walls, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing.

Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., Linux or Windows 2000) used on target systems. These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors. It should be noted that an additional specialization in security is not always necessary, as strong skills in the other areas imply a very good understanding of how the security on various systems is maintained. These systems management skills are necessary for the actual vulnerability testing, but are equally important when preparing the report for the client after the test.

Given these qualifications, how does one go about finding such individuals? The best ethical hacker candidates will have successfully mastered hacking tools and their exploits.

What do Ethical Hackers do?

An ethical hacker's evaluation of a system's security seeks answers to these basic questions:

- What can an intruder see on the target systems?
- What can an intruder do with that information?
- Does anyone at the target notice the intruder's at tempts or successes?
- What are you trying to protect?
- What are you trying to protect against?
- How much time, effort, and money are you willing to expend to obtain adequate protection?

Once answers to these questions have been determined, a security evaluation plan is drawn up that identifies the systems to be tested, how they should be tested, and any limitations on that testing.

"What can be the best way to help organizations or even individuals tackle hackers? The solution is students trained in the art of ethical hacking"

A Career in Ethical Hacking

In a society so dependent on computers, breaking through anybody's system is obviously considered anti-social. What can organizations do when in spite of having the best security policy in place, a break-in still occurs! While the "best of security" continues to get broken into by determined hackers, what options can a helpless organization look forward to? The answer could lie in the form of ethical hackers, who unlike their more notorious cousins (the black hats), get paid to hack into supposedly secure networks and expose flaws. And, unlike mock drills where security consultants carry out specific tests to check out vulnerabilities a hacking done by an ethical hacker is as close as you can get to the real one. Also, no matter how extensive and layered the security architecture is constructed, the organization does not know the real potential for external intrusion until its defenses are realistically tested.

Though companies hire specialist security firms to protect their domains, the fact remains that security breaches happen due to a company's lack of knowledge about its system. What can be the best way to help organizations or even individuals tackle hackers? The solution is students trained in the art of ethical hacking, which simply means a way of crippling the hacker's plans by knowing the ways one can hack or break into a system. But a key impediment is the shortage of skill sets. Though you would find thousands of security consultants from various companies, very few of them are actually aware of measures to counter hacker threats.

How much do Ethical Hackers get Paid?

Globally, the hiring of ethical hackers is on the rise with most of them working with top consulting firms. In the United States, an ethical hacker can make upwards of $120,000 per annum. Freelance ethical hackers can expect to make $10,000 per assignment. For example, the contract amount for IBM's Ethical Hacking typically ranges from $15,000 to

$45,000 for a standalone ethical hack. Taxes and applicable travel and living expenses are extra.

Note: Excerpts taken from Ethical Hacking by C.C Palmer.

Certified Ethical Hacker Certification

If you want to stop hackers from invading your network, first you've got to invade their minds.

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

To achieve CEH certification, you must pass exam 312-50 that covers the standards and language involved in common exploits, vulnerabilities and countermeasures. You must also show knowledge of the tools used by hackers in exposing common vulnerabilities as well as the tools used by security professionals for implementing countermeasures.

To achieve the Certified Ethical Hacker Certification, you must pass the following exam:

Ethical Hacking and Countermeasures (312-50)

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 Objectives

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, Open Source Intelligence, Incident Handling and Log Interpretation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in internet security.

Who should attend?

This class is a must for networking professionals, IT managers and decision-makers that need to understand the security solutions that exist today. Companies and organizations interested in developing greater e-commerce capability need people that know information security. This class provides a solid foundation in the security technologies that will pave the way for organizations that are truly interested in reaping the benefits and tapping into the potential of the Internet.

Prerequisites

Working knowledge of TCP/IP, Linux and Windows 2000.

Duration

5 Days

CEH v4 Course Outline

Module 1: Introduction to Ethical Hacking

- Why Security?
- The Security, functionality and ease of use Triangle
- Can Hacking be Ethical?
- Essential Terminology.
- Elements of Security.
- What does a Malicious Hacker do?
- Difference between Penetration Testing and Ethical Hacking.
- Hacker Classes.
- What do Ethical Hackers do?
- Skill Profile of an Ethical Hacker.
- Modes of Ethical Hacking.
- Security Testing.
- Deliverables.
- Computer Crimes and Implications.
- Legal Perspective (US Federal Law).

Module 2: Footprinting

- Defining Footprinting.
- Information Gathering Methodology.
- Locate the Network Range.
- Hacking Tools:
  - Whois
  - Nslookup
  - ARIN
  - Traceroute
  - NeoTrace
  - VisualRoute Trace

  - SmartWhois
  - Visual Lookout
  - VisualRoute Mail Tracker
  - eMailTrackerPro
  - e-mail Spider
  - Wayback machine

Module 3: Scanning

- Definition of Scanning.
- Types of scanning
- Objectives of Scanning
- Scanning Methodology
- Classification of Scanning
- Hacking Tools
  - Nmap
  - Nessus
  - Retina
  - Saint
  - HPing2
  - Firewalk
  - NIKTO
  - GFI Languard
  - ISS Security Scanner
  - Netcraft
  - IPsec Scan
  - NetScan Tools pro 2003
  - Super Scan
  - Floppyscan
- War Dialer
- Hacking Tools

  - THC Scan
  - Friendly Pinger
  - Cheops
  - Security Administrator's Tool for Analyzing Network (SATAN)
  - SAFEsuite Internet Scanner
  - IdentTCPScan
  - PortScan Plus
  - Strobe
  - Blaster Scan
- OS Fingerprinting
- Active Stack fingerprinting
- Tool for Active Stack fingerprinting
  - XPROBE2
- Passive Fingerprinting
- Proxy Servers
- Hacking Tools
  - Socks Chain
  - Anonymizers
  - HTTP Tunnel
  - HTTPort
- Countermeasures

Module 4: Enumeration

- What is Enumeration?
- NetBios Null Sessions
- Hacking Tools
  - DumpSec
  - Winfo

- NetBIOS Auditing Tool (NAT)

- Null Session Countermeasures
- NetBIOS Enumeration
- Hacking Tool :NBTScan
- Simple Network Management Protocol (SNMP) Enumeration
- Hacking Tools
  - Solarwinds
  - Enum
  - SNScan
- SNMP Enumeration Countermeasures
- Management Information Base (MIB)
- Windows 2000 DNS Zone Transfer
- Blocking Win 2k DNS Zone Transfer
- Enumerating User Accounts
- Hacking Tools
  - User2sid and Sid2user
  - UserInfo
  - GetAcct
  - DumpReg
  - Trout
  - Winfingerprint
  - PsTools (PSFile,PSLoggedOn,PSGetSid,PSInfo,PSService,PSList,PSKill, PSSuspend, PSLogList, PSExec, PSShutdown)
- Active Directory Enumeration and Countermeasures

Module 5: System Hacking

- Administrator Password Guessing
- Manual Password Cracking Algorithm
- Automated Password Cracking
- Password Types
- Types of Password Attacks
- Hacking Tool
    - NTInfoScan (CIS)
- Performing Automated Password Guessing
- Hacking Tool
- Legion
- Password Sniffing
- Hacking Tools
    - LOphtcrack
    - pwdump2 and pwdump3
    - KerbCrack
    - NBTdeputy
- NetBIOS DoS Attack
- Hacking Tools
    - NBName
    - John the Ripper
- LAN Manager Hash
- Password Cracking Countermeasures
- Syskey Utility
- Cracking NT/2000 Passwords
- Hacking Tool
    - NTFSDOS
- SMB Logon

- Hacking Tool: SMBRelay
- SMBRelay Man-in-the-Middle Scenario
- Hacking Tool : SMBRelay2
- SMBRelay Weaknesses and Countermeasures
- Hacking Tools
  - SMBGrind
  - SMBDie
- Privilege Escalation
- Hacking Tools
  - GetAdmin
  - hk.exe
- Keystroke Loggers
- Hacking Tools
  - IKS Software Keylogger
  - Ghost Keylogger
  - Hardware Key Logger
  - Spyware Spector
  - eBlaster
- Hiding Files
- Creating Alternate Data Streams
- ADS creation and detection
- Hacking Tools
  - Makestream
  - ads_cat
  - Streams
  - LADS (List Alternate Data Streams)
- NTFS Streams Countermeasures
- Stealing Files Using Word Documents
- Field Code Countermeasures
- Steganography

- Spyware Tool - Desktop Spy
- Hacking Tools
    - Steganography tools
        - DiSi-Steganograph
        - EZStego
        - Gif-It-Up v1.0
        - Gifshuffle
        - Hide and Seek
        - JPEG-JSTEG
        - MandelSteg and GIFExtract
        - Mp3Stego
        - Nicetext
        - Pretty Good Envelope
        - OutGuess
        - SecurEngine
        - Stealth
        - Snow
        - Steganography Tools 4
        - Steganos
        - Steghide
        - Stegodos
        - Stegonosaurus
        - StegonoWav
        - wbStego
    - Image Hide
    - MP3Stego
    - StegonoWav
    - Snow.exe
    - Camera/Shy
- Steganography Detection
- Hacking Tool

- diskprobe.exe
- Covering Tracks
- Disabling Auditing and clearing Event Logs
- Hacking Tool
    - Dump Event Log
    - elsave.exe
    - WinZapper
    - Evidence Eliminator
- RootKit
- Planting the NT/2000 RootKit
- Hacking Tools
    - Fu
    - Vanquish
- Rootkit Countermeasures
- Hacking Tool
    - Patchfinder 2.0

Module 6: Trojans and Backdoors

- Effect on Business
- What is a Trojan?
- Overt and Covert Channels
- Working of Trojans
- Different Types of Trojans
- What Trojan Creators look for?
- Different ways a Trojan can get into a system
- Indications of a Trojan Attack
- Some famous Trojans and ports used by them
- How to determine which ports are “Listening”?
- Different Trojans found in the Wild

  - Beast 2.06
  - Phatbot
  - Senna Spy
  - CyberSpy
  - Remote Encrypted Callback UNIX Backdoor (RECUB)
  - Amitis
  - QAZ
  - Back Orifice
  - Back Orifice 2000
  - Tini
  - NetBus
  - SubSeven
  - Netcat
  - Subroot
  - Let me Rule 2.0 Beta 9
  - Donald Dick
  - Graffiti.exe
  - EliteWrap
  - IconPlus
  - Restorator
  - Whack-a-mole
  - Firekiller 2000
- BoSniffer
- Wrappers
- Packaging Tool : Wordpad
- Hard Disk Killer (HDKP 4.0)
- ICMP Tunneling
- Hacking Tool: Loki
- Loki Countermeasures
- Reverse WWW Shell – Covert Channels using HTTP

- Hacking Tools
    - fPort
    - TCP View
- Tripwire
- Process Viewer
- Inzider-Tracks Processes and Ports
- System File Verification
- Trojan horse Construction Kit
- Anti-Trojan
- Evading Anti-Trojan/Anti-Virus using Stealth Tools v 2.0
- Reverse Engineering Trojans
- Backdoor Countermeasures

Module 7: Sniffers

- Definition of sniffing
- How a Sniffer works?
- Passive Sniffing
- Active Sniffing
- Hacking Tool: EtherFlood
- Man-in-the-Midle Attacks
- Spoofing and Sniffing Attacks
- ARP Poisoning and countermeasures
- Hacking Tools
    - Ethereal
    - Dsniff
    - Sniffit
    - Aldebaran
    - Hunt
    - NGSSniff

  - Ntop
  - pf
  - IPTraf
  - Etherape
  - Netfilter
  - Network Probe
  - Maa Tec Network Analyzer
  - Snort
  - Macof, MailSnarf, URLSnarf, WebSpy
  - Windump
  - Etherpeek
  - Ettercap
  - SMAC
  - Mac Changer
  - Iris
  - NetIntercept
  - WinDNSSpoof
  - NetIntercept
  - Win DNSpoof
  - TCPDump
  - Network Monitor
  - Gobbler
  - ETHLOAD
  - Esniff
  - Sunsniff
  - Linux_sniffer
  - Sniffer Pro
- Countermeasures

Module 8: Denial of Service

- What is Denial of Service?

- Goal of DoS(Denial of Service)
- Impact and Modes of Attack
- DoS Attack Classification
  - Smurf
  - Buffer Overflow Attacks
  - Ping Of death
  - Teardrop
  - SYN
  - Tribal Flow Attack
- Hacking Tools
  - Jolt2
  - Bubonic.c
  - Land and LaTierra
  - Targa
- Distributed DOS Attacks and Characteristics
- Agent Handler Model
- IRC-Based DDoS Attack Model
- DDoS Attack taxonomy
- DDoS Tools
  - Trin00
  - Tribe Flow Network (TFN)
  - TFN2K
  - Stacheldraht
  - Shaft
  - Trinity
  - Knight
  - Mstream
  - Kaiten
- Reflected DOS Attacks
- Reflection of the Exploit

- Countermeasures for Reflected DoS
- Tools for Detecting DDOS Attacks
  - ipgrep
  - tcpdstat
  - findoffer
- DDoS Countermeasures
- Defensive Tool: Zombie Zapper
- Worms: Slammer and MyDoom.B

Module 9: Social Engineering

- What is Social Engineering?
- Art of Manipulation
- Human Weakness
- Common Types of Social Engineering
- Human Based Impersonation
- Example of social engineering
- Computer Based Social Engineering
- Reverse Social Engineering
- Policies and procedures
- Security Policies-checklist

Module10: Session Hijacking

- Understanding Session Hijacking
- Spoofing vs Hijacking
- Steps in Session Hijacking

- Types of Session Hijacking
- TCP Concepts 3 Way Handshake
- Sequence numbers
- Hacking Tools
    - Juggernaut
    - T-Sight
    - TTY Watcher
    - IP Watcher
    - Hunt
    - Paros v3.1.1
    - TTY-Watcher
    - IP Watcher
    - T-sight
    - Remote TCP Session Reset Utility
- Dangers Posed by Session Hijacking
- Protection against Session Hijacking
- Countermeasures: IP Security

Module 11: Hacking Web Servers

- How Web Servers Work?
- How are Web Servers Compromised?
- Popular Web Servers and Common Security Threats
- Apache Vulnerability
- Attack against IIS
- IIS Components
- Sample Buffer Overflow Vulnerabilities
- Hacking Tool: IISHack.exe
- ISAPI.DLL Exploit
- Code Red and ISAPI.DLL Exploit
- Unicode

- Unicode Directory Traversal Vulnerability
- Hacking Tools
  - Unicodeuploader.pl
  - IISxploit.exe
  - execiis-win32.exe
- Msw 3prt IPP Vulnerability
- Hacking Tool: Jill.c
- IPP Buffer Overflow Countermeasures
- Unspecified Executed Path Vulnerability
- File System Traversal Countermeasures
- WebDAV/ ntdll.dll Vulnerability
- Real World instance of WebDAV Exploit
- Hacking Tool: "KaHT"
- RPCDCOM Vulnerability
- ASN Exploits
- IIS Logs
- Network Tool: Log Analyzer
- Hacking Tool: Clean IISLog
- Escalating Privileges on IIS
- Hacking Tools
  - hk.exe
  - cmdasp.asp
  - iiscrack.dll
  - ispc.exe
  - Microsoft IIS 5.0 - 5.1 remote denial of service Exploit Tool
  - Microsoft Frontpage Server Extensions fp30reg.dll Exploit Tool
  - GDI+ JPEG Remote Exploit Tool
  - Windows Task Scheduler Exploit Tool

- Microsoft Windows POSIX Subsystem Local Privilege Escalation Exploit Tool
- Hot Fixes and Patches
- Solution: UpdateEXPERT
- cacls.exe Utility
- Vulnerability Scanners
- Network Tools
  - Whisker
  - N-Stealth
  - Webinspect
  - Shadow Security Scanner
- Countermeasures
- Increasing Web Server Security

Module 12: Web Application Vulnerabilities

- Web Application Set-up
- 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
- Buffer Overflow

- Countermeasures
- Directory Traversal/Forceful Browsing
- Countermeasures
- Cryptographic Interception
- Authentication Hijacking
- Countermeasures
- Log Tampering
- Error Message Interception
- Attack Obfuscation
- Platform Exploits
- Internet Explorer Exploits
- DMZ Protocol Attacks
- DMZ
- Countermeasures
- Security Management Exploits
- Web Services Attacks
- Zero Day Attacks
- Network Access Attacks
- TCP Fragmentation
- Hacking Tools:
    - Instant Source
    - Wget
    - WebSleuth
    - Black Widow
    - Window Bomb

- Burp: Positioning Payloads
- Burp: Configuring Payloads and Content Enumeration
- Burp
- Burp Proxy: Intercepting HTTP/S Traffic

- Burp Proxy: Hex-editing of Intercepted Traffic
- Burp Proxy: Browser Access to Request History
- Hacking Tool: cURL
- Carnivore
- Google Hacking

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
- Microsoft Passport Authentication
- What is a Password Cracker?
- Modus Operandi of an Attacker using Password Cracker
- How does a Password Cracker work?
- Attacks- Classification
- Password Guessing
- Query String
- Cookies
- Dictionary Maker
- Password Crackers Available
    - LOphtcrack
    - John The Ripper

  - Brutus
  - Obiwan
  - Authforce
  - Hydra
  - Cain and Abel
  - RAR
  - Gammaprog
- Hacking Tools:
  - WebCracker
  - Munga Bunga
  - PassList
  - Read Cookies
  - SnadBoy
  - WinSSLMiM
- “Mary had a Little Lamb” Formula
- Countermeasures

Module 14: SQL Injection

- Attacking SQL Servers
- SQL Server Resolution Service (SSRS)
- Osql-L Probing
- Port Scanning
- Sniffing, Brute Forcing and finding Application Configuration Files
- Tools for SQL Server Penetration Testing
  - SQLDict
  - SqlExec
  - SQLbf
  - SQLSmack

- SQL2.exe
- AppDetective
- Database Scanner
- SQLPoke
- NGSSQLCrack
- NGSSQuirreL
- SQLPing v2.2

- OLE DB Errors
- Input Validation Attack
- Login Guessing & Insertion
- Shutting Down SQL Server
- Extended Stored Procedures
- SQL Server Talks
- Preventive Measures

Module 15: Hacking Wireless Networks

- Introduction to Wireless Networking
- Business and Wireless Attacks
- Basics
- Components of Wireless Network
- Types of Wireless Network
- Setting up WLAN
- Detecting a Wireless Network
- How to access a WLAN
- Advantages and Disadvantages of Wireless Network
- Antennas
- SSIDs
- Access Point Positioning
- Rogue Access Points

- Tools to Generate Rogue Access Points
  - Fake AP
  - NetStumbler
  - MiniStumbler
- What is Wireless Equivalent Privacy (WEP)?
- WEP Tool:
  - AirSnort
  - WEPCrack
- Related Technology and Carrier Networks
- MAC Sniffing and AP Spoofing
- Tool to detect MAC Address Spoofing: Wellenreiter v2
- Terminology
- Denial of Service Attacks
- DoS Attack Tool: FATAjack
- Man-in-the-Middle Attack (MITM)
- Scanning Tools:
  - Redfang
  - Kismet
  - THC- WarDrive v2.1
  - PrismStumbler
  - MacStumbler
  - Mognet v1.16
  - WaveStumbler
  - StumbVerter v1.5
  - NetChaser v1.0 for Palm tops
  - AP Scanner
  - Wavemon
  - Wireless Security Auditor (WSA)
  - AirTraf 1.0
  - Wifi Finder

- Sniffing Tools:
  - AiroPeek
  - NAI Sniffer Wireless
  - Ethereal
  - Aerosol v0.65
  - vxSniffer
  - EtherPEG
  - Drifnet
  - AirMagnet
  - WinDump 3.8 Alpha
  - ssidsniff
- Multi Use Tool: THC-RUT
- Tool: WinPcap
- Auditing Tool: bsd-airtools
- WIDZ- Wireless Detection Intrusion System
- Securing Wireless Networks
- Out of the box Security
- Radius: Used as Additional layer in security
- Maximum Security: Add VPN to Wireless LAN

Module 16 : Virus

- Virus Characteristics
- Symptoms of ‘virus-like’ attack
- What is a Virus Hoax?
- Terminologies
- How is a worm different from virus?
- Indications of a Virus Attack
- Virus History
- Virus damage

- Effect of Virus on Business
- Access Methods of a Virus
- Mode of Virus Infection
- Life Cycle of a virus
- What Virus Infect?
- How virus infect?
- Virus/worm found in the wild:
  - W32.CIH.Spacefiller (a.k.a Chernobyl)
  - Win32/Explore.Zip Virus
  - I Love You Virus
  - Melissa Virus
  - Pretty Park
  - Code red Worm
  - W32/Klez
  - Bug Bear
  - SirCam Worm
  - Nimda
  - SQL Slammer
- Writing a simple virus program.
- Writing DDOS Zombie Virus
- Virus Construction Kits
- Virus Creation Scripts
- Virus Detection Methods
- Virus Incident Response
- What is Sheep Dip?
- Prevention is better than Cure
- Anti-Virus Software
- Popular Anti-Virus packages
- New Virus found in 2004
- Virus Checkers

- Blaster – Virus Analysis
- Nimda – Virus Analysis
- Sasser Worm – Virus Analysis
- Klez – Virus Analysis
- IDAPro
- Virus Analyzers

Module 17: Physical Security

- Security statistics
- Physical Security breach incidents
- Understanding Physical Security
- What is the need of Physical Security?
- Who is Accountable for Physical Security?
- Factors affecting Physical Security
- Physical Security checklist
  - Company surroundings
  - Premises
  - Reception
  - Server
  - Workstation Area
  - Wireless Access Points
  - Other Equipments such as fax, removable media etc
  - Access Control
  - Computer Equipment Maintenance
  - Wiretapping
  - Remote access
- Lock Picking Techniques
- Spying Technologies

Module 18: Linux Hacking

- Why Linux?
- Linux basics
- Chrooting
- Why is Linux Hacked?
- Linux Vulnerabilities in 2003
- How to apply patches to vulnerable programs
- Scanning Networks
- Scanning Tool: Nessus
- Cheops
- Port Scan detection tools:
  - Klaxon
  - Scanlogd
  - PortSentry
  - LIDS (Linux Intrusion Detection System)
- Password cracking in Linux.

- Password cracking tools:
  - John the Ripper
  - Viper
  - Slurpie
- IPChains
- IPTables
- ipchains vs. ipfwadm
- How to Organize Firewall Rules
- Security Auditor's Research Assistant (SARA)
- Hacking Tool:
  - Sniffit
  - HPing2

  - Hunt
  - TCP Wrappers
- Linux Loadable Kernel Modules
- Linux Rootkits:
  - Knark
  - Torn
  - Tuxit
  - Adore
  - Ramen
  - Beast
- Rootkit countermeasures:
  - Chkrootki
  - Tripwire
  - Bastille Linux
  - LIDS(Linux Intrusion Detection system)
  - Dtk
  - Rkdet
  - Rootkit Hunter
  - Carbonite
  - Rscan
  - Saint Jude
- Linux Security Tools:
  - Whisker
  - Flawfinder
- Advanced Intrusion Detection System (AIDE)
- Linux Security testing tools
  - NMap
  - LSOF
  - Netcat
  - Nemesis

- Linux Encryption Tools:
    - Stunnel
    - OpenSSH/SSH
    - SSH
    - GnuPG
- Linux tools: Log and traffic monitors:
    - MRTG
    - Swatch
    - Timbersee
    - Logsurf
    - IPLog
    - IPTraf
    - Ntop
- Linux Security Auditing Tool (LSAT)
- Linux Security countermeasures

Module 19: Evading Firewalls, IDS and Honeypots

- Intrusion Detection Systems
- Ways to Detect Intrusion
- Types of Intrusion Detection System
- Intrusion Detection Tools
    - Snort 2.1.0
    - Symantec ManHunt
    - LogIDS 1.0
    - SnoopNetCop Standard
    - Prelude Hybrid IDS version 0.8.x
    - Samhain
- Steps to perform after an IDS detects an intrusion
- Evading IDS systems

- Tools to Evade IDS
  - SideStep
  - ADMutate
  - Mendax v.0.7.1
  - Stick
  - Fragrouter
  - Anzen NIDSbench
- Packet Generators
- Introduction to Firewalls
- Firewall Identification
- Firewalking
- Banner Grabbing
- Breaching Firewalls
- Placing Backdoors through Firewalls
- Hiding Behind Covert Channel: Loki
- ACK tunneling
- Tools to Breach Firewall
  - 007 Shell
  - ICMP Shell
  - AckCmd
  - Covert TCP1.0
- Tools for testing IDS and Firewalls
- Introduction to Honeypots
- Honeypot Project
- Types of Honeypots
- Honeypot: Specter
- Honeypot: Honeyd
- Honeypot: KFSensor
- Hacking Tool: Sebek
- Tools to Detect Honeypot

- Send-Safe Honeypot Hunter
- Nessus Security Scanner

Module 20 : Buffer Overflows

- Significance of Buffer Overflow Vulnerability
- Why are Programs/Applications Vulnerable?
- Buffer Overflows
- Reasons for Buffer Overflow Attacks
- Knowledge required writing Buffer Overflow Exploits
- How a Buffer Overflow occurs?
- Understanding Stacks
- Stack Implementation
- Stack based buffer overflow
- Shellcode
- Heap Based buffer overflow
- How to detect Buffer Overflows in a Program?
- Attacking a real program
- NOPS
- How to mutate a Buffer Overflow Exploit? featuring ADMutate
- Countermeasures
- Return Address Defender (RAD)
- StackGuard
- Immunix System
- Vulnerability Search - ICAT

Module 21 : Cryptography

- Public-key Cryptography
- Working of Encryption
- Digital Signature
- Digital Certificate
- RSA (Rivest Shamir Adleman)
- RSA Attacks
  - Brute forcing RSA factoring
  - Esoteric attack
  - Chosen cipher text attack
  - Low encryption exponent attack
  - Error analysis
  - Other attacks
- MD5
- SHA (Secure Hash Algorithm)
- SSL (Secure Socket Layer)
- RC5
- What is SSH?
- Government Access to Keys (GAK)
- RSA Challenge
- distributed.net
- PGP (Pretty Good Privacy)
- Code Breaking Methodologies
  - Using Brute Force
  - Frequency Analysis
  - Trickery and Deceit
  - One-Time Pad
- Cryptography Attacks
- Disk Encryption
- PGPCrack
- Magic Lantern
- WEPCrack

- Cracking S/MIME Encryption using idle CPU Time
- CypherCalc
- Command Line Scriptor
- CryptoHeaven

Module 22 : Penetration Testing

- Need for a Methodology
- Penetration Test vs. Vulnerability Test
- Reliance on Checklists and Templates
- Phases of Penetration Testing
- Passive Reconnaissance
- Best Practices
- Results that can be expected
- Indicative passive reconnaissance steps include (but are not limited to)
- Introduction to Penetration Testing
- Type of Penetration Testing Methodologies
- Open Source Vs Proprietary Methodologies
- Security Assessment Vs Security Auditing
- Risk Analysis
- Types of Penetration Testing
- Types Ethical Hacking
- Vulnerability Assessment Vs Penetration Testing
- Do-it Yourself Testing
- Firms Offering Penetration Testing Services
- Penetration Testing Insurance
- Explication of Terms of Engagement

- Pen-Test Service Level Agreements
- Offer of Compensation
- Starting Point and Ending Points of Testing
- Penetration Testing Locations
- Black Box Testing
- White Box Testing
- Grey Box Testing
- Manual Penetration Testing
- Automated Penetration Testing
- Selecting the Right Tools
- Pen Test Using Appscan
- HackerShield
- Pen-Test Using Cerberus Internet Scanner
- Pen-Test Using CyberCop Scanner
- Pen-Test Using Foundscan
- Pen-Test Using Nessus
- Pen-Test Using NetRecon
- Pen-Test Using Retina
- Pen-Test Using SAINT
- Pen-Test Using SecureNET
- Pen-Test Using SecureScan
- Pen-Test Using SATAN, SARA and Security Analyzer
- Pen-Test Using STAT Analyzer
- Pen-Test Using Twwscan
- VigilEnt
- WebInspect
- Evaluating Different Types of Pen-Test Tools
- Platform on Which Tools Will be Used
- Asset Audit

- Fault Tree and Attack Trees
- GAP Analysis
- Device Inventory
- Perimeter Firewall Inventory
- Web Server Inventory
- Load Balancer Inventory
- Local Area Network Inventory
- Demilitarized Zone Firewall
- Internal Switch Network Sniffer
- Application Server Inventory
- Database Server Inventory
- Name Controller and Domain Name Server
- Physical Security
- ISP Routers
- Legitimate Network Traffic Threat
- Unauthorized Network Traffic Threat
- Unauthorized Running Process Threat
- Loss of Confidential Information
- Business Impact of Threat
- Pre-testing Dependencies
- Post-testing Dependencies
- Failure Management
- Test Documentation Processes
- Penetration Testing Tools
    - Defect Tracking Tools
    - Configuration Management Tools
    - Disk Replication Tools
    - Pen-Test Project Scheduling Tools
    - Network Auditing Tools

  - DNS Zone Transfer Testing 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 site Crawlers
  - Web-Testing based Scripting Tools
  - Buffer Overflow Protection Tools
  - Buffer Overflow Generation Tools
  - Input Data Validation 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
- SANS Institute TOP 20 Security Vulnerabilities

- All Operating System Platforms
  - Default installs of operating systems and applications
  - Accounts with no passwords or weak passwords
  - Nonexistent or incomplete backups
  - Large number of open ports
  - Not filtering packets for correct incoming and outgoing addresses
  - Nonexistent or incomplete logging
  - Vulnerable Common Gateway Interface (CGI) programs
- Windows-specific
  - Unicode vulnerability-Web server folder traversal
  - Internet server application programming interface (ISAPI) extension buffer overflows
  - IIS Remote Data Services (RDS) exploit
  - Network Basic Input Output System (NetBIOS), unprotected Windows networking shares
  - Information leakage via null session connections
  - Weak hashing in SAM (Security Accounts Manager)-LanManager hash
- UNIX-specific
  - Buffer overflows in Remote Procedure Call (RPC) services
  - Sendmail vulnerabilities
  - Bind weaknesses

        - Remote system command (such as rcp, rlogin, and rsh) vulnerabilities
        - Line Printer Daemons (LPD) vulnerabilities
        - Sadmind and mountd exploits
        - Default Simple Network Management Protocol (SNMP) strings
- Penetration Testing Deliverable Templates
    - Test Status Report Identifier
    - Test Variances
    - Test Comprehensive Assessment
    - Summary of Results (Incidents)
    - Test Evaluation
    - Names of Persons (Approval)
    - Template Test Incident Report
    - Template Test Log
- Active Reconnaissance
- Attack Phase
- Activity: Perimeter Testing
- Activity: Web Application Testing – I
- Activity: Web Application Testing – II
- Activity: Wireless Testing
- Activity: Acquiring Target
- Activity: Escalating Privileges
- Activity: Execute, Implant & Retract
- Post Attack Phase & Activities
- Tool: CORE Impact

International Council of E-Commerce Consultants
67 Wall Street, 22nd Floor
New York, NY 10005-3198
USA

Phone: 212.709.8253
Fax: 212.943.2300

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

EC-Council