Ethical Hacking & Countermeasures

EC-Council

Ethical Hacking

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 attempts 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.

Duration

5 Days

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.

Course Outline

v2.3

Module 1: Ethics and Legality

- What is an Exploit?
- The security functionality triangle
- The attacker's process
- Passive reconnaissance
- Active reconnaissance
- Types of attacks
- Categories of exploits
- Goals attackers try to achieve
- Ethical hackers and crackers - who are they
- Self proclaimed ethical hacking
- Hacking for a cause (Hacktivism)
- Skills required for ethical hacking
- Categories of Ethical Hackers
- What do Ethical Hackers do?
- Security evaluation plan
- Types of Ethical Hacks
- Testing Types
- Ethical Hacking Report
- Cyber Security Enhancement Act of 2002
- Computer Crimes
- Overview of US Federal Laws
- Section 1029
- Section 1030
- Hacking Punishment

Module 2: Footprinting

- What is Footprinting
- Steps for gathering information
- Whois
- http://tucows.com
- Hacking Tool: Sam Spade
- Analyzing Whois output
- NSLookup
- Finding the address range of the network
- ARIN
- Traceroute
- Hacking Tool: NeoTrace
- Visual Route
- Visual Lookout
- Hacking Tool: Smart Whois
- Hacking Tool: eMailTracking Pro
- Hacking Tool: MailTracking.com

Module 3: Scanning

- Determining if the system is alive?
- Active stack fingerprinting

- Passive stack fingerprinting
- Hacking Tool: Pinger
- Hacking Tool: WS_Ping_ Pro
- Hacking Tool: Netscan Tools Pro 2000
- Hacking Tool: Hping2
- Hacking Tool: icmpenum
- Detecting Ping sweeps
- ICMP Queries
- Hacking Tool: netcraft.com
- Port Scanning
- TCPs 3-way handshake
- TCP Scan types
- Hacking Tool: IPEye
- Hacking Tool: IPSECSCAN
- Hacking Tool: nmap
- Port Scan countermeasures
- Hacking Tool: HTTrack Web Copier
- Network Management Tools
- SolarWinds Toolset
- NeoWatch
- War Dialing
- Hacking Tool: THC-Scan
- Hacking Tool: PhoneSweep War Dialer
- Hacking Tool: Queso
- Hacking Tool: Cheops
- Proxy Servers
- Hacking Tool: SocksChain
- Surf the web anonymously
- TCP/IP through HTTP Tunneling
- Hacking Tool: HTTPort

Module 4: Enumeration

- What is Enumeration
- NetBios Null Sessions
- Null Session Countermeasures
- NetBIOS Enumeration
- Hacking Tool: DumpSec
- Hacking Tool: NAT
- SNMP Enumertion
- SNMPUtil
- Hacking Tool: IP Network Browser
- SNMP Enumeration Countermeasures
- Windows 2000 DNS Zone transfer
- Identifying Win2000 Accounts
- Hacking Tool: User2SID
- Hacking Tool: SID2User
- Hacking Tool: Enum
- Hacking Tool: UserInfo
- Hacking Tool: GetAcct
- Active Directory

Enumeration

Module 5: System Hacking

- Administrator Password Guessing
- Performing Automated Password Guessing
- Legion
- NTInfoScan
- Defending Against Password Guessing
- Monitoring Event Viewer Logs
- VisualLast
- Eavesdroppin on Network Password Exchange
- Hacking Tool: LOphtCrack
- Hacking Tool: KerbCrack
- Privilege Escalation
- Hacking Tool: GetAdmin
- Hacking Tool: hk
- Manual Password Cracking Algorithm
- Automatic Password Cracking Algorithm
- Password Types
- Types of Password Attacks
- Dictionary Attack
- Brute Force Attack
- Distributed Brute Force Attack
- Password Change Interval
- Hybrid Attack
- Cracking Windows 2000 Passwords
- Retrieving the SAM file
- Redirecting SMB Logon to the Attacker
- SMB Redirection
- Hacking Tool: SMBRelay
- Hacking Tool: SMBRelay2
- SMBRelay Man-in-the-Middle (MITM)
- SMBRelay MITM Countermeasures
- Hacking Tool: SMBGrinder
- Hacking Tool: SMBDie
- Hacking Tool: NBTDeputy
- NetBIOS DoS Attack
- Hacking Tool: nbname
- Hacking Tool: John the Ripper
- LanManager Hash
- Password Cracking Countermeasures
- Keystroke Logger
- Hacking Tool: Spector
- AntiSpector
- Hacking Tool: eBlaster
- Hacking Tool: SpyAnywhere
- Hacking Tool: IKS

Software Logger

- Hardware Tool: Hardware Key Logger
- Hacking Tool: Rootkit
- Planting Rootkit on Windows 2000 Machine
- _rootkit_ embedded TCP/IP Stack
- Rootkit Countermeasures
- MD5 Checksum utility
- Tripwire
- Covering Tracks
- Disabling Auditing
- Auditpol
- Clearing the Event Log
- Hacking Tool: Elslave
- Hacking Tool: Winzapper
- Hacking Tool: Evidence Eliminator
- Hidding Files
- NTFS File Streaming
- Hacking Tool: makestrm
- NTFS Streams Countermeasures
- LNS
- Steganography
- Hacking Tool: ImageHide
- Hacking Tool: MP3Stego
- Hacking Tool: Snow
- Hacking Tool: Camera/ Shy
- Steganography Detection
- StegDetect
- Encrypted File System
- Hacking Tool: dskprobe
- Hacking Tool: EFSView
- Buffer Overflows
- Creating Buffer Overflow Exploit
- Outlook Buffer Overflow
- Hacking Tool: Outoutlook

Module 6: Trojans and Backdoors

- What is a Trojan Horse?
- Overt and Covert
- Hacking Tool: QAZ
- Hacking Tool: Tini
- Hacking Tool: Netcat
- Hacking Tool: Donald Dick
- Hacking Tool: SubSeven
- Hacking Tool: BackOrifice 2000
- Back Oriffice Plug-ins
- Hacking Tool: NetBus
- Wrappers
- Hacking Tool: Graffiti
- Hacking Tool: Silk Rope 2000
- Hacking Tool: EliteWrap
- Hacking Tool: IconPlus
- Packaging Tool: Microsoft WordPad

- Hacking Tool: Whack a Mole
- Trojan Construction Kit
- BoSniffer
- Hacking Tool: FireKiller 2000
- Covert Channels
- ICMP Tunneling
- Hacking Tool: Loki
- Reverse WWW Shell
- Backdoor Countermeasures
- BO Startup and Registry Entries
- NetBus Startup and Registry Keys
- Port Monitoring Tools
- fPort
- TCPView
- Process Viewer
- Inzider - Tracks Processes and Ports
- Trojan Maker
- Hacking Tool: Hard Disk Killer
- Man-in-the-Middle Attack
- Hacking Tool: dsniff
- System File Verification
- TripWire

Module 7: Sniffers

- What is a Sniffer?
- Hacking Tool: Etheral
- Hacking Tool: Snort
- Hacking Tool: WinDump
- Hacking Tool: EtherPeek
- Passive Sniffing
- Active Sniffing
- Hacking Tool: EtherFlood
- How ARP Works?
- Hacking Tool: DSniff
- Hacking Tool: Macof
- Hacking Tool: mailsnarf
- Hacking Tool: URLsnarf
- Hacking Tool: Webspy
- Hacking Tool: Ettercap
- Hacking Tool: SMAC
- MAC Changer
- ARP Spoofing Countermeasures
- Hacking Tool: WinDNSSpoof
- Hacking Tool: WinSniffer
- Network Tool: IRIS
- Network Tool: NetInterceptor
- SniffDet
- Hacking Tool: WinTCPKill

Module 8: Denial of Service

- What is Denial of Service Attack?
- Types of DoS Attacks

- How DoS Work?
- What is DDoS?
- Hacking Tool: Ping of Death
- Hacking Tool: SSPing
- Hacking Tool: Land
- Hacking Tool: Smurf
- Hacking Tool: SYN Flood
- Hacking Tool: CPU Hog
- Hacking Tool: Win Nuke
- Hacking Tool: RPC Locator
- Hacking Tool: Jolt2
- Hacking Tool: Bubonic
- Hacking Tool: Targa
- Tools for Running DDoS Attacks
- Hacking Tool: Trinoo
- Hacking Tool: WinTrinoo
- Hacking Tool: TFN
- Hacking Tool: TFN2K
- Hacking Tool: Stacheldraht
- Hacking Tool: Shaft
- Hacking Tool: mstream
- DDoS Attack Sequence
- Preventing DoS Attack
- DoS Scanning Tools
- Find_ddos
- SARA
- DDoSPing
- RID
- Zombie Zapper

Module 9: Social Engineering

- What is Social Engineering?
- Art of Manipulation
- Human Weakness
- Common Types of Social Engineering
- Human Based Impersonation
- Important User
- Tech Support
- Third Party Authorization
- In Person
- Dumpster Diving
- Shoulder Surfing
- Computer Impersonation
- Mail Attachments
- Popup Windows
- Website Faking
- Reverse Social Engineering
- Policies and Procedures
- Social Engineering Security Policies
- The Importance of Employee Education

Module 10: Session Hijacking

- What is Session Hijacking?

- Session Hijacking Steps
- Spoofing Vs Hijacking
- Active Session Hijacking
- Passive Session Hijacking
- TCP Concepts - 3 way Handshake
- Sequence Numbers
- Sequence Number Example
- Guessing the Sequence Numbers
- Hacking Tool: Juggernaut
- Hacking Tool: Hunt
- Hacking Tool: TTYWatcher
- Hacking Tool: IP Watcher
- Hacking Tool: T-Sight
- Remote TCP Session Reset Utility
- Dangers Posed by Session Hijacking
- Protection against Session Hijacking

Module 11: Hacking Web Servers

- Apache Vulnerability
- Attacks against IIS
- IIS Components
- ISAPI DLL Buffer Overflows
- IPP Printer Overflow
- msw3prt.dll
- Oversized Print Requests
- Hacking Tool: Jill32
- Hacking Tool: IIS5-Koei
- Hacking Tool: IIS5Hack
- IPP Buffer Overflow Countermeasures
- ISAPI DLL Source Disclosure
- ISAPI.DLL Exploit
- Defacing Web Pages
- IIS Directory Traversal
- Unicode
- Directory Listing
- Clearing IIS Logs
- Network Tool: LogAnalyzer
- Attack Signature
- Creating Internet Explorer (IE) Trojan
- Hacking Tool: IISExploit
- Hacking Tool: UnicodeUploader.pl
- Hacking Tool: cmdasp.asp
- Escalating Privilages on IIS
- Hacking Tool: IISCrack.dll
- Hacking Tool: ispc.exe
- Unspecified Executable Path Vulnerability
- Hacking Tool: CleanIISLog
- File System Traversal Countermeasures

- Microsoft HotFix Problems
- UpdateExpert
- Cacls utility
- Network Tool: Whisker
- N-Stealth Scanner
- Hacking Tool: WebInspect
- Network Tool: Shadow Security Scanner

Module 12: Web Application Vulnerabilities

- Documenting the Application Structure
- Manually Inspecting Applications
- Using Google to Inspect Applications
- Directory Structure
- Hacking Tool: Instant Source
- Java Classes and Applets
- Hacking Tool: Jad
- HTML Comments and Contents
- Hacking Tool: Lynx
- Hacking Tool: Wget
- Hacking Tool: Black Widow
- Hacking Tool: WebSleuth
- Cross Side Scripting
- Session Hijacking using XSS
- Cookie Stealing
- Hacking Tool: IEEN

Module 13: Web Based Password Cracking Techniques

- Basic Authentication
- Message Digest Authentication
- NTLM Authentication
- Certificate based Authentication
- Digital Certificates
- Microsoft Passport Authentication
- Forms based Authentication
- Creating Fake Certificates
- Hacking Tool: WinSSLMiM
- Password Guessing
- Hacking Tool: WebCracker
- Hacking Tool: Brutus
- Hacking Tool: ObiWan
- Hacking Tool: Munga Bunga
- Password dictionary Files
- Attack Time
- Hacking Tool: Varient
- Hacking Tool: PassList
- Query Strings
- Post data
- Hacking Tool: cURL
- Stealing Cookies

- Hacking Tool: CookieSpy
- Hacking Tool: ReadCookies
- Hacking Tool: SnadBoy

Module 14: SQL Injection

- What is SQL Injection Vulnerability?
- SQL Insertion Discovery
- Blank sa Password
- Simple Input Validation
- SQL Injection
- OLE DB Errors
- 1=1
- blah' or 1=1
- Stealing Credit Card Information
- Preventing SQL Injection
- Database Specific SQL Injection
- Hacking Tool: SQLDict
- Hacking Tool: SQLExec
- Hacking Tool: SQLbf
- Hacking Tool: SQLSmack
- Hacking Tool: SQL2.exe
- Hacking Tool: Oracle Password Buster

Module 15: Hacking Wireless Networks

- 802.11 Standards
- What is WEP?
- Finding WLANs
- Cracking WEP keys
- Sniffing Trafic
- Wireless DoS Attacks
- WLAN Scanners
- WLAN Sniffers
- MAC Sniffing
- Access Point Spoofing
- Securing Wireless Networks
- Hacking Tool: NetTumbler
- Hacking Tool: AirSnort
- Hacking Tool: AiroPeek
- Hacking Tool: WEP Cracker
- Hacking Tool: Kismet
- WIDZ- Wireless IDS

Module 16: Virus and Worms

- Cherobyl
- ExploreZip
- I Love You
- Melissa
- Pretty Park
- Code Red Worm
- W32/Klez
- BugBear
- W32/Opaserv Worm
- Nimda
- Code Red
- SQL Slammer

- How to write your own Virus?
- Worm Construction Kit

Module 17: Novell Hacking

- Common accounts and passwords
- Accessing password files
- Password crackers
- Netware Hacking Tools
- Chknull
- NOVELBFH
- NWPCRACK
- Bindery
- BinCrack
- SETPWD.NLM
- Kock
- userdump
- Burglar
- Getit
- Spooflog
- Gobbler
- Novelffs
- Pandora

Module 18: Linux Hacking

- Why Linux ?
- Linux Basics
- Compiling Programs in Linux
- Scanning Networks
- Mapping Networks
- Password Cracking in Linux
- Linux Vulnerabilities
- SARA
- TARA
- Sniffing
- A Pinger in Disguise
- Session Hijacking
- Linux Rootkits
- Linux Security Countermeasures
- IPChains and IPTables

Module 19: IDS, Firewalls and Honeypots

- Intrusion Detection System
- System Integrity Verifiers
- How are Intrusions Detected?
- Anomaly Detection
- Signature Recognition
- How does IDS match Signatures with Incoming Traffic?
- Protocol Stack Verification
- Application Protocol Verification
- What Happens after an IDS Detects an Attack?
- IDS Software Vendors
- SNORT
- Evading IDS

(Techniques)

- Complex IDS Evasion
- Hacking Tool: fragrouter
- Hacking Tool: TCPReplay
- Hacking Tool: SideStep
- Hacking Tool: NIDSbench
- Hacking Tool: ADMutate
- IDS Detection
- Tools to Detect Packet Sniffers
- Tools to inject strangely formatted packets onto the wire
- Hacking Through Firewalls
- Placing Backdoors through Firewalls
- Hiding behind Covert Channels
- What is a Honeypot?
- Honeypots Evasion
- Honeypots vendors

Module 20: Buffer Overflows

- What is a Buffer Overflow?
- Exploitation
- Assembly Language Basics
- How to Detect Buffer Overflows in a Program?
- Skills Required
- CPU/OS Dependency
- Understanding Stacks
- Stack Based Buffer Overflows
- Buffer Overflow Technical Implementation
- Writing your own Buffer Overflow Exploit in C
- Defense against Buffer Overflows
- Type Checking Tools for Compiling Programs
- StackGuard
- Immunix
- **Module 21: Cryptography**
- What is PKI?
- Digital Certificates
- RSA
- MD-5
- RC-5
- SHA
- SSL
- PGP
- SSH
- Encryption Cracking Techniques

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

© 2002 EC-Council. All rights reserved.
This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. EC-Council logo is registered trademarks or trademarks of EC-Council in the United States and/or other countries.