

Course Outline: CEH-Certified Ethical Hacker

Learning Method: Instructor-led Classroom Learning

Duration: 6.00 Day(s)/ 48 hrs

Overview:

This ethical hacker course will immerse the student into an interactive environment, where they will be shown how to scan, test, hack and secure their own system. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems.

Who Should Attend:

This course is course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure. IT consultants who want to learn more about hacking tools and techniques will also benefit.

Outline:

Module 1: Ethics and Legality

- What is an Exploit?
- The security functionality triangle
- The attacker's process
- Types of attacks
- Categories of Exploit
- Goals attackers try to achieve
- Ethical hackers and crackers
- Skills required for ethical hacking
- Categories of ethical hackers
- Security evaluation plan
- Types of ethical hacks
- Testing Types
- Ethical hacking report
- Computer crimes
- Hacking Punishment

- Who is <http://tucows.com>
- Hacking tool: sam spade
- Analyzing who is input
- Traceroute
- Hacking tool: neo trace
- Visual Route
- Visual lookout
- Hacking tool: Smart who is
- Hacking tool: email tracking Pro
- Hacking tool: mailtracking.com

Module 2: Foot printing

- What is foot printing
- Steps of gathering information

Module 3: Scanning

- Determining if the system is alive?

Phone: +357 70002770
www.computrain.com.cy



- Active stack fingerprinting
- Passive stack fingerprinting
- Hacking Tool: Pinger
- Hacking Tool: netcraft.com
- Detecting Ping Sweeps
- Hacking tool: IPEye
- Hacking Tool: nmap
- Neo Watch

Module 4: Enumeration

- What is enumeration?
- NetBios Null Sessions
- Null Sessions Countermeasures
- NetBios Enumeration
- Hacking Tool: Dumpsec
- Hacking Tool: NAT
- Hacking Tool: IP Network Browser
- Hacking Tool: User 2SID
- Hacking Tool: SID2User
- Hacking Tool: Enum
- Hacking Tool: Userinfo
- Hacking Tool: GetAcct
- Active directory Enumeration
- War Dialing
- Proxy Servers

Lesson 5: System Hacking

- Administrator Password Guessing
- Legion
- NTInfo Scan
- Visual Last
- Privilege Escalation
- Password Types
- Types of Password Attacks
- Dictionary attack

- Hybrid attack

Module 6: Trojans and Backdoors

- What is Trojan Horse
- Overt and Covert
- Hacking tool: QAZ
- Hacking tool: Tini
- Hacking tool: Netcat
- Hacking tool: Donald Dick
- Back orifice Plug-ins
- Wrappers
- Bo Sniffer
- Covert Channels
- fPort
- TCPView
- Process Viewer
- Trip Wire
- Covering Tracks
- Disabling Auditing
- Auditpol
- Clearing the event log
- Hidding files
- LNS
- Buffer Overflows

Module 7: Sniffers

- What is a Sniffer?
- Passive sniffing
- Active sniffing
- Hacking tool: EtherFlood
- How APR Works
- Hacking Tool: ArpSpoof
- How APR works?

Module 8: Denial of Service

- What is Denial of service attack?
- Types of DoS Attack?
- How DoS WORK?
- What is DDoS
- MAC Changer

Phone: +357 70002770
www.computrain.com.cy



- Hacking Tool: Macof
- Hacking Tool: mailsnarf
- Hacking Tool: webspay
- Hacking Tool: Ettercap
- Hacking Tool: sTerm
- Hacking Tool: SMAC
- Network tool: IRIS
- Network tool: WinSniffer

Module 9: Social Engineering

- What is social engineering?
- Art of manipulation
- Human Weakness
- Important user
- Teach Support
- In person
- Shoulder Surfing
- Computer impersonation
- Mail attachments
- Website Faking
- Reverse Social Engineering
- Policies and Procedures
- The importance of employee education

Module 10: Session Hijacking

- What is session hijacking?
- Session Hijacking steps
- Active Session Hijacking
- Passive Session Hijacking
- Sequence numbers
- Sequence numbers examples
- Hacking tool: Hunt
- Hacking tool: IP Watcher
- Danger posed by session reset utility

Module 11: Hacking Web Servers

- Ttacks against IIS
- IIS COMPONENTS
- Oversized Print Requests
- Hacking Tool: Jill32
- IPP Printer overflow
- Msw3prt.dll

Module 12: WEB APPLICATION VULNERABILITIES

- Documenting the application structure
- Manually inspecting applications
- Using google to inspect applications
- Directory structure
- Java classes and applets
- HTML Comments and contents
- Defacing Web Pages
- Directory Listing
- Clearing IIS Logs
- Attack signature
- Microsoft Hot Fix Problems
- Update Expert

Module 13: WEB BASED PASSWORD CRACKING TECHNIQUES

- Basic Authentication
- Message Digest Authentication
- Digital certificates
- Microsoft Passport Authentication
- Forms Based Authentication
- Creating fake certificates
- Password Guessing
- Password Dictionary Files
- Query Strings

Module 14: SQL INJECTION

- What is SQL Injection Vulnerability?
- SQL Insertion Discovery
- Blank Password
- Simple input validation
- 1=1
- Stealing credit card information
- Preventing SQL Injection
- Post data
- Stealing cookies

Phone: +357 70002770
www.computrain.com.cy



Module 15: HACKING WIRELESS NETWORKS

- What is WEP?
- Finding WLAN's
- Cracking WEP keys
- Sniffing traffic
- Wireless Dos Attacks
- WLAN Scanners
- WLAN Sniffers
- Access point spoofing
- Securing wireless networks
- Hacking tool: net tumbler
- Hacking tool: Aircrack-ng
- Hacking tool: airopeek
- Hacking tool: kismet

Module 16: VIRUS AND WORMS

- Cheroby
- I love you
- Melissa
- Pretty Park
- BugBear
- Nimda
- Codr red
- SQL Slammer
- How to write your own virus?

Module 17: NOVEL HACKING

- Common accounts and passwords
- Accessing password file
- Bindery
- Kock
- Buglar
- Spooflog
- Pandora
- Novelfs

Module 18: LINUX HACKING

- Why linux

- Linux basics
- Compiling programs in linux
- Scanning Networks
- Mapping networks
- Password Cracking in Linux
- SARA
- TARA
- Sniffing
- Linux Rootkits

Module 19: IDS FIREWALLS AND HONEYPOTS

- Intrusion detection system
- System integrity verifies
- Anomaly detection
- Signature recognition
- Traffic?
- SNORT
- IDS DETECTION
- Hacking through firewalls
- Placing backdoors through firewalls
- What is honey pot?
- Honey pot vendors?

Module 20: BUFFER OVERFLOWS

- What is buffer overflow?
- Exploitation
- Assembly language basics
- Skills required
- Understanding stacks
- Stack based buffer overflows
- Programs
- Stack Guard
- Immunix

Module 21: CRYPTOGRAPHY

- What is PKI?

Phone: +357 70002770
www.computrain.com.cy



- Digital certificates
- RSA
- MD-5
- RC-5
- SHA
- SSL
- PGP

**Module 22: PENETRATION TESTING
METHODOLOGIES**

Phone: +357 70002770
www.computrain.com.cy

