THE MINDCENTER
COMPUTER EDUCATION PROFESSIONALS

Ethical Hacking and Countermeasures 5.0

Instructor-led

Course Length: 5 days

Course Objectives:

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. You will understand and know how to look for weaknesses and vulnerabilities in targeted systems, and use the same knowledge and tools as a malicious hacker.

Course Outline

Module 1: Introduction to Ethical Hacking

Labs:

- 1.1 Visit the Securiteam Website and Analyze Vulnerabilities
- 1.2 Visit the U.S. Cybercrime Website
- 1.3 Visit Various Hacker Websites
- 1.4 Read Ethical Hacking Agreement

Module 2: Footprinting

Labs:

- 2.1 Use SamSpade
- 2.2 Use Web Data Extractor to Footprint a Website
- 2.3 Use GEO spider to Footprint a Website
- 2.4 Use NEOTRACE to Footprint a Website
- 2.5 Use Which ISP Owns IP to Footprint a Network Address
- 2.6 Use WhereIsIP to Footprint a Network Address
- 2.7 Use My IP Suite to Footprint a Network Address
- 2.8 Use Way Back Machine to View Web History
- 2.9 Use Public Websites for Footprinting
- 2.10 Use Kartoo Visual Browser for Footprinting a Company's Network
- 2.11 Use Yahoo People for Footprinting an Individual
- 2.12 Use Intellius for Footoprinting an Individual
- 2.13 Use Google Earth
- 2.14 Mirror a Website
- 2.15 Email Tracking
- 2.16 Search the Internet for Email Addresses
- 2.17 GeoWhere – Query multiple search engines at once, find and test proxies, get daily topnews
- 2.18 Web The Ripper
- 2.19 Website Watcher
- 2.20 Whois

Module 3: Scanning

Labs:

- 3.1 Use NMAP to Portscan a Website
- 3.2 Use Angry IP to Check for Live Hosts
- 3.3 Scan the Network Using Hping2 for Windows
- 3.4 Scan the Network Using NetScan Tools Pro
- 3.5 Scan the Network Using SuperScan 4
- 3.6 Scan the Network Using Floppyscan
- 3.7 Banner Grabbing Using Telnet
- 3.8 Banner Grabbing Using Netcraft
- 3.9 HTTP Tunneling
- 3.10 Block and restore Cookies G-Zapper
- 3.11 Global Network Inventory
- 3.12 Mega Ping

Module 4: Enumeration

Labs:

- 4.1 Connect via a Null Session
- 4.2 Use GetAcct to Enumerate Users
- 4.3 Use SuperScan 4 to Enumerate Users
- 4.4 Use SNMP Scanner
- 4.5 Use Winfingerprint to Enumerate Services

Module 5: System Hacking

Labs:

- 5.1 Use L0phtrack to Bruteforce SAM Passwords
- 5.2 Extract SAM Hashes Using Pwdump
- 5.3 Privilege Escalation Using X.EXE
- 5.4 Execute Commands on a Remote Computer
- 5.5 Email Keylogger
- 5.6 Use the "Klogger" Keylogger
- 5.7 Use Desktop Spy to Capture Screen Images
- 5.8 NTFS Streams
- 5.9 Use Fu Rootkit to Hide Files and Processes
- 5.10 Use Camera/Shy to View Hidden Files
- 5.11 Use Spammimic to Hide Messages

- 5.12 Use Snow to Hide Information
- 5.13 Use Auditpol to Enable/Disable Auditing
- 5.14 ADS Spy
- 5.15 Brute Force Password Estimation Tool
- 5.16 Masker Stenography Tool
- 5.17 Max File Encryption
- 5.18 Merge Streams
- 5.19 Rootkit Revealer – Rootkit Detection Utility
- 5.20 Traceless
- 5.21 Rainbowcrack
- 5.22 Invisible Secrets 4

Module 6: Trojans and Backdoors

Labs:
- 6.1 Tini Trojan
- 6.2 NetBus Trojan
- 6.3 Netcat Trojan
- 6.4 Beast Trojan
- 6.5 Use Wrappers
- 6.6 Proxy Trojan
- 6.7 Atelier Web Commander
- 6.8 Use TCPVIEW to Monitor the Network Connections
- 6.9 What's on My Computer
- 6.10 Use Process Viewer to View the Running Processes
- 6.11 Use MSCONFIG to View the Startup Programs
- 6.12 Use MD5SUM to Create Digital File Signatures
- 6.13 Check the Registry for Trojan Startup Entries
- 6.14 CurrPorts
- 6.15 Fast Sum – Using MD5 Checksum
- 6.16 Netstat
- 6.17 Additional Labs

NDA: Non-Disclosure Agreement

Module 7: Sniffers

Labs:
- 7.1 Use Ethereal to Sniff the Network
- 7.2 Use Windump to Sniff the Network
- 7.3 Network View
- 7.4 Ettercap
- 7.5 Ettercap-NG (Next Generation)
- 7.6 Mac Flooding
- 7.7 DNS Poisoning
- 7.8 EffeTech Sniffer
- 7.9 Passowrd Sniffer
- 7.10 Cain and Abel
- 7.11 Packet Crafter
- 7.12 SMAC – Spoofing MAC Address

Module 8: Denial of Service

Labs:
- 8.1 Freak88 – Distributed Denial-of-Service
- 8.2 Ping of Death
- 8.3 ImageWolf Bot
- 8.4 DoS Attack Using Nemesys
- 8.5 DoS Attack Using Panther
- 8.6 DDOS Ping Attack

Module 9: Social Engineering

Labs:
- 9.1 Read Social Engineering Story
- 9.2 Phishing Attack – Fake Address Bar
- 9.3 Phishing Attack – Fake Status Bar
- 9.4 Phishing Attack – Fake Toolbar
- 9.5 IP Address Conversion
- 9.6 NETCRAFT Anti-Phishing Toolbar

Module 10: Session Hijacking

Labs:
- 10.1 Session Hijacking Analysis
- 10.2 Session Hijacking Using Paros

Module 11: Hacking Web Servers

Labs:
- 11.1 Exploit Windows 2000
- 11.2 RPC Exploit
- 11.3 Metaspoit Exploit
- 11.4 Vulnerability Assessment Using Shadow Security Scanner
- 11.5 Nessus for Windows
- 11.6 Microsoft Baseline Security Analyzer
- 11.7 Qfecheck

Module 12: Web Application Vulnerabilities

Labs:
- 12.1 E-Shopping Using Hidden Values
- 12.2 Footprint a Website Using BlackWidow
- 12.3 Footprint a Website Using Wget
- 12.4 Footprint a Website Using an Access Diver
- 12.4 Unicode Strings
- 12.5 Acunetix Web Vulerability Scanner

Module 13: Web-Based Password Cracking Techniques

Labs:
- 13.1 ObiWan Password Cracking Tool
- 13.2 Brutus Password Cracking Tool
- 13.3 Dictionary Maker

- 13.4 SnadBoy – Password Revelation
- 13.5 Cookie Spy
- 13.6 Password Recovery Time Simulator
- 13.7 RockXP

Module 14: SQL Injection

Labs:
- 14.1 Juggybank SQL Interjection
- 14.2 SQL Interjection Whitepaper

Module 15: Hacking Wireless Networks

Labs:
- 15.1 AiroPeek

Module 16: Virus

Labs:
- 16.1 Write a Simple Virus
- 16.2 Use Virus Construction Kits
- 16.3 Virus Analysis Using IDA Pro
- 16.4 A2 Scanner
- 16.5 AVG Scanner
- 16.6 McAfee
- 16.7 Norton Internet Security

Module 17: Physical Security

Labs:
- 17.1 MIT Document

Module 18: Linux Hacking

Labs:
- 18.1

Module 19: Evading IDS, Firewalls and Detecting Honey Pots

Labs:
- 19.1 Install and Run Snort
- 19.2 Install and TrapServer

Module 20: Buffer Overflows

Labs:
- 20.1 Compile and Execute a Simple Buffer Overflow Program

Module 21: Cryptography

Module 22: Penetration Testing

Labs:
- 22.1 Azure Web Log
- 22.2 iInventory
- 22.3 Link Utility
- 22.4 MaxCrypt
- 22.5 Sniff'em
- 22.6 SQL Stripes
- 22.7 Trace Route
- 22.8 Windows Security Officer

Modules 23-26: Advanced Modules