

Certified Penetration Testing Specialist (CPTS) with CEH Backtrack

- **Course Number:** CPTS-CEH
- **Length:** 5 Day(s)

Certification Exam

This course will help you prepare for the following exam:

- **Exam 312-50:** Certified Ethical Hacker

Course Overview

This course enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk. Its focus is developed based on principles and methods used by malicious hackers, but its focus is professional penetration testing and securing information assets.

Prerequisites

Students attending this course should have:

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Computer hardware knowledge
- Knowledge of Microsoft packages
- Network+, Security+
- Knowledge of Linux would be beneficial but not essential

Audience

This course is geared towards experienced IT and Security professionals.

Course Outline

- **Module 1 - Business and Technical Logistics for Pen Testing**
- Business and Technical Logistics for Pen Testing
- Definition of a Penetration Test
- Benefits of a Penetration Test
- ID Theft Statistics
- Demo - ID theft center website
- VA loses another 48,000 records
- TK Maxx hit by theft of 46m credit cards
- Demo - Security Focus Website
- The Evolving Threat
- Demo - ANI Zero-Day

- Security Vulnerability Life Cycle
- Exploit Timeline
- Zombie Statistics
- Zombie Definition
- Botnet Definition
- Types of Penetration Testing
- Methodology for Penetration Testing / Ethical Hacking
- Hacker vs. Penetration Tester
- Not Just Tools
- Demo - OSSTMM Methodology
- Demo - NIST Methodology
- Demo - FFIEC ISSAF Methodology
- Penetration Testing Methodologies
- OSSTMM - Open Source Security Testing Methodologies
- Demo – WebSite
- Website Review
- Tool: SecurityNOW! SX
- Demo - Cioview SecurtyNow SX Tool
- Lab – Overview
- Lab - Exercise 1
- Lab - Exercise 2
- Lab - Exercise 3
- Module 1 Review
- **Module 2 - Information Gathering - Reconnaissance 1: Passive**
- Information Gathering - Reconnaissance 1: Passive
- What Information is Gathered by the Hacker
- Methods of Obtaining Information
- Physical Access
- Demo - Bump Key
- Social Access
- Digital Access
- Passive vs. Active Reconnaissance
- Footprinting Defined
- Footprinting Tool: Kartoo Website
- Demo - Kartoo Search Engine
- Footprinting tools
- Google and Query Operators
- Demo - Google Hacking
- Johnny.Ihackstuff.com
- Aura : Google API Utility Tool
- Myspace.com
- Facebook.com
- Identity Theft and MySpace
- Blogs, Forums & Newsgroups
- Internet Archive: The WayBack Machine
- Demo - Way Back Machine

- Domain Name Registration
- WHOIS
- WHOIS Output
- Demo - Searching For Information
- DNS Databases
- Using Nslookup
- Dig for Unix / Linux
- Traceroute Operation
- Visual Mapping
- Answers.com
- EDGAR For USA Company Info
- Company House For British Company Info
- Demo - Information discovery
- Fbweb.com
- Intelius info and Background Check Tool
- Web Server Info Tool: Netcraft
- Countermeasure: Domainsbyproxy.com
- Footprinting Countermeasures
- Lab - Exercise 1
- Module 2 Review
- **Module 3 - Linux Fundamentals**
- Linux Fundamentals
- Linux History – Linus + Minix = Linux
- The GNU Operating System
- Linux Introduction
- Linux GUI Desktops
- Demo - Linux GUI Desktops
- Linux Shell
- Demo - Linux Shell
- Linux Bash Shell
- Recommended Linux Book
- Password & Shadow File Formats
- User Account Management
- Demo - User Account Files
- Changing a user account password
- Demo - Creating User Accounts
- Configuring Network Interfaces with Linux
- Demo - ifconfig usage
- Mounting Drives with Linux
- Demo - Mounting Drives
- Tarballs and Zips
- Compiling Programs in Linux
- Demo - Compiling programs using gcc
- Typical Linux Operating Systems
- Gentoo = Simple Software Install Portal
- Gentoo

- Demo - Gentoo Overview
- VLOS
- Why Use Live Linux Boot CDs
- Security Live Linux CDs
- FrozenTech's Complete Distro List
- Most Popular: BackTrack
- forums.remote-exploit.org
- My Slax Creator
- Slax Modules (Software Packages)
- Lab - Installing BackTrack into a VM
- Lab - Updating BackTrack Files
- Lab - BackTrack Services
- Module 3 Review
- **Module 4 - Detecting Live Systems - Reconnaissance 2: Active**
- Detecting Live Systems - Reconnaissance 2: Active
- Introduction to Port Scanning
- Port Scan Tips
- Expected Results
- Tools: Organizing Results
- Leo meta-text editor
- Demo - Methods to log your results
- Free Mind: Mind mapping
- Method: Ping
- Stealth Online Ping
- Demo - Port scanning know your tools
- NMAP: Is the Host Online
- The TCP/IP stack
- Recommended Video: It's Showtime
- Demo - Recommended Video and NMAP Basic Online Test
- Which services use which ports?
- TCP 3-Way Handshake
- TCP Flags
- Demo - Tool Engage Packet Builder
- Vanilla (TCP Connect Port Scan)
- NMAP TCP Connect Scan
- Demo - NMAP TCP Connect Scan
- Demo - NMAP SYN Scan
- Half-open Scan
- Tool Practice: TCP half-open & Ping Scan
- Firewallled Ports
- NMAP Service Version Detection
- Demo - NMAP sV Scan and export results
- Saving NMAP results
- Output results
- UDP Port Scan
- Advanced Technique

- Popular Port Scanning Tools
- Tool: Superscan
- Tool: LookatLan
- Demo - Look at Lan Tool
- Tool: Hping2
- Demo - Hping2 Tool
- Tool: Auto Scan
- Demo - Auto Scan Tool
- Advanced Port Scanning / Packet Crafting
- OS Fingerprinting
- Demo - OS Fingerprinting with NMAP
- OS Fingerprinting: Xprobe2
- Demo - OS Fingerprinting with Xprobe AMAP POF
- Xprobe2 Options
- What Is Fuzzy Logic?
- Tool: P0f - Passive OS Finger Printing Utility
- Tool Practice: Amap
- Packet Crafting
- Tool Fragrouter: Fragmenting Probe Packets
- Countermeasures: Scanning
- Scanning Tools Summary
- Lab - Exercise 1
- Lab - Exercise 2
- Lab - Exercise 3
- Module 4 Review
- **Module 5 - Enumeration - Reconnaissance 3: Active**
- Enumeration - Reconnaissance 3: Active
- Methodology Recap
- Web Server Banners
- Demo - Web Server Banner Grabbing with Telnet
- Practice: Banner Grabbing with Telnet
- Demo - Windows 2003 and SMTP Banner Grabbing with Telnet
- Sam Spade Tool: Banner Grabbing
- SuperScan 4 Tool: Banner Grabbing
- SMTP Server Banner
- Demo - DNS Zone Transfer using nslookup
- DNS Enumeration
- Zone Transfers from Windows 2000 DNS
- Countermeasure: DNS Zone Transfers
- SNMP Insecurity
- SNMP Enumeration
- Demo - SNMP enumeration using Windows and Linux
- SNMP Enumeration Countermeasures
- Active Directory Enumeration
- AD Enumeration countermeasures
- Null sessions

- Syntax for a Null Session
- Viewing Shares
- Tool: DumpSec
- Tool: USE42
- Tool: Enumeration with Cain and Abel
- Demo - Null Sessions and tool usage
- NAT Dictionary Attack Tool
- Demo - Null Sessions and NAT
- Injecting Abel Service
- Demo - Injecting Abel
- Null Session Countermeasures
- Enumeration Tools Summary
- Lab - Exercise 1
- Module 5 Review
- **Module 6 - Cryptography Decrypted**
- Cryptography Decrypted
- Introduction
- Encryption
- Encryption Algorithm
- Implementation
- Symmetric Encryption
- Symmetric Algorithms
- Demo – Cryptool
- Crack Times
- Asymmetric Encryption
- Key Exchange
- Hashing
- Hash Collisions
- Common Hash Algorithms
- Demo - Hashing Tools
- Hybrid Encryption
- Digital Signatures
- Demo - Digital Signature with Cryptool
- SSL Hybrid Encryption
- IPsec
- Demo – IPSEC
- Transport Layer Security – SSH
- Public Key Infrastructure
- PKI-Enabled Applications
- Quantum Cryptography
- Hardware Encryption: DESlock
- Demo - Hardware Encryption
- Attack Vectors
- Lab - Exercise 1
- Module 6 Review
- **Module 7 - Vulnerability Assessments**

- Vulnerability Assessments
- Vulnerability Assessment Intro
- Testing Overview
- Staying Abreast: Security Alerts
- Demo - Keeping up to date with Websites
- Vulnerability Scanners
- Qualys Guard
- Tool: Nessus Open Source
- Nessus Client Interface
- Nessus Report
- Tool: Retina
- Video Recommendation
- Nessus for Windows
- Tool: LANguard
- Demo - Nessus on Windows XP
- Analyzing the Scan Results
- Microsoft Baseline Analyzer
- MBSA Scan Report
- Dealing with the assessment results
- Patch Management
- Lab - Exercise 1
- Lab - Exercise 2
- Module 7 Review
- **Module 8 - Malware, Trojan's & Back Doors**
- Malware, Trojan's & Back Doors
- Defining Malware: Trojans and Backdoors
- Defining Malware: Virus & Worms
- Defining Malware: Spyware
- Company Surveillance Software
- Distributing Malware
- Malware Capabilities
- Auto starting Malware
- Countermeasure: Monitoring Autostart Methods
- Tool: Netcat
- Netcat Switches
- Demo - Exploiting and spawning a remote cmd with netcat
- Executable Wrappers
- Demo - Creating upload packages with elitewrap
- Benign EXE's Historically Wrapped with Trojans
- Tool: Restorator
- Tool: Exe Icon
- The Infectious CD-Rom Technique
- Trojan: Backdoor.Zombam.B
- Trojan: JPEG GDI+ All in One Remote Exploit
- Advanced Trojans: Avoiding Detection
- Typical Wired/Wireless Network

- Malware Countermeasures
- Demo - Gargoyle
- Spy Sweeper Enterprise
- Malware Reference: Glocksoft.com
- CM Tool: Port Monitoring Software
- CM Tools: File Protection Software
- CM Tool: Windows File Protection
- CM Tool: Windows Software Restriction Policies
- CM Tool: Hardware-based Malware Detectors
- Countermeasure: User Education
- Lab - Exercise 1
- Module 8 Review
- **Module 9 - Windows Hacking**
- Windows Hacking
- Types of Password Attacks
- Demo - Video Surveillance Sunglasses
- Keystroke Loggers
- Demo - Keystroke loggers
- Password Guessing
- Demo - Tsgriinder tutorial
- Password Cracking LM/NTLM Hashes
- LM Hash Encryption
- NT Hash Generation
- Syskey Encryption
- Demo - RainbowTables, Cain and Abel
- Salting
- Cracking Techniques
- Precomputation Detail
- Cain and Abel's Cracking Methods
- Free Rainbow Tables
- NTPASSWD:Hash Insertion Attack
- Password Sniffing
- Windows Authentication Protocols
- Hacking Tool: Kerbsniff & KerbCrack
- Countermeasure: Monitoring Event Viewer Log
- Hard Disk Security
- Free HD Encryption Software
- Tokens & Smart Cards
- Smart Cards
- Covering Tracks Overview
- Disabling Auditing
- Clearing and Event log
- Hiding Files with NTFS Alternate Data Stream
- Demo - Alternate Data Streams
- NTFS Streams countermeasures
- Stream Explorer

- What is Steganography
- Demo - Steganography tools
- Steganography Tools
- Shedding Files Left Behind
- Leaving No Local Trace
- More Anonymous Software
- Demo - Anonymizer tools
- Demo - Janus VM Appliance
- StealthSurfer II Privacy Stick
- Tor: Anonymous Internet Access
- How Tor Works
- Encrypted Tunnel Notes:
- Hacking Tool: RootKit
- Windows RootKit Countermeasures
- Lab - Exercise 1
- Lab - Exercise 2
- Lab - Exercise 3
- Lab - Exercise 4
- Lab - Exercise 5
- Lab - Exercise 6
- Module 9 Review
- **Module 10 - Advanced Exploit Techniques**
- Advanced Exploit Techniques
- How Do Exploits Work?
- Memory Organization
- Buffer OverFlows
- Demo - Buffer Overflow
- Stages Of Exploit Development
- Prevention
- The Metasploit Project
- Core Impact Overview
- Demo - Fuzzers in action
- Lab - Exercise 1
- Lab - Exercise 2
- Lab - Exercise 3
- Lab - Exercise 4
- Module 10 Review
- **Module 11 - Attacking Wireless Networks**
- Attacking Wireless Networks
- Wi-Fi Network Types
- Widely Deployed Standard's
- A vs B vs G
- 802.11n - MIMO
- SSID (Service Set Identity)
- MAC Filtering
- Wired Equivalent Privacy

- Weak IV Packets
- XOR – Basics
- WEP Weaknesses
- TKIP
- How WPA improves on WEP
- The WPA MIC Vulnerability
- 802.11i - WPA2
- WPA and WPA2 Mode Types
- WPA-PSK Encryption
- Tool: NetStumbler
- Demo - Using NetStumbler
- War Driving With KNSGEM
- Demo - War Driving Mapping
- Tool: Kismet
- Demo - Kismet Usage
- Analysis Tool: OmniPeek Personal
- Demo - OmniPeek Personal Capturing
- DOS: Deauth/disassociate attack
- What is Aircrack-ng?
- Demo - Linux Wireless Commands
- Tool: Airodump-ng
- Tool: Aireplay-ng
- Tool: Aircrack-ng
- ARP Injection (Failure)
- 802.1X: EAP Types
- EAP Advantages/Disadvantages
- Typical Wired/Wireless Network
- EAP/TLS Deployment
- Lab - Exercise 1
- Module 11 Review
- **Module 12 - Networks, Sniffing and IDS**
- Networks, Sniffing and IDS
- Packet Sniffers
- Example Packet Sniffers
- Tool: Pcap & WinPcap
- Tool: Wireshark (Ethereal)
- TCP Stream Re-assembling
- Tool: Packetyzer
- tcpdump & windump
- Tool: OmniPeek
- Demo - Network Sniffers
- Demo - TCP Dump Packet Sniffer
- Sniffer Detection using Cain & Abel
- Demo - Dsniff and ARP Cache Poisoning
- Passive Sniffing
- Active Sniffing

- Active Sniffing Methods
- Switch Table Flooding
- ARP Cache Poisoning
- ARP Normal Operation
- ARP Cache Poisoning (Cont.)
- Technique: ARP Cache Poisoning (Linux)
- Countermeasures
- Tool: Cain and Abel
- Demo - Cain & Abel ARP Cache Poisoning
- Ettercap
- Linux Tool Set:Dsniff Suite
- Dsniff Operation
- MailSnarf, MsgSnarf, FileSnarf
- What is DNS spoofing?
- Demo - Cain & Abel DNS Spoofing
- Tools: DNS Spoofing
- Breaking SSL Traffic
- Tool: Breaking SSL Traffic
- Tool: Cain and Abel (Cont..)
- Demo - Cain & Abel MITM SSL Interception
- Voice over IP (VoIP)
- Intercepting RDP
- Cracking RDP Encryption
- Routing Protocols Analysis
- Demo - Cain & Abel VOIP Interception
- Countermeasures for Sniffing
- Firewalls, IDS and IPS
- Firewall - First line of defense
- IDS - Second line of defense
- IPS - Last line of defense?
- Evading The Firewall and IDS
- Evasive Techniques
- Firewall - Normal Operation
- Evasive Technique – Example
- Evading with Encrypted Tunnels
- Demo - Engage Custom Packet Builder
- New Age' Protection
- Demo - SSH Tunnels
- SpySnare - Spyware Prevention System (SPS)
- Intrusion SecureHost Overview
- Intrusion Prevention Overview
- Secure Surfing or Hacking????
- Module 12 Review
- **Module 13 - Injecting the Database**
- Injecting the Database
- Overview of Database Server

- Types of databases
- Overview of Database Server Relational Databases
- Overview of Database Server
- Vulnerabilities and Common Attacks
- SQL Injection
- Why SQL “Injection”? SQL Connection Properties
- SQL Injection: Enumeration SQL Extended Stored Procedures Demo: SQL Injection
- Shutting Down SQL Server Direct Attacks
- Attacking Database Servers
- Obtaining Sensitive Information
- Hacking Tool: SQL Ping2
- Hacking Tool: osql.exe
- Hacking Tool: Query Analyzers
- Hacking Tool: SQLExec
- Hacking Tool: Metasploit
- Hardening Databases
- Module 13 Review
- **Module 14 - Attacking Web Technologies**
- Attacking Web Technologies
- Common Security Threats
- The Need for Monitoring
- Seven Management Errors
- Progression of The Professional Hacker
- The Anatomy of a Web Application Attack
- Demo: Banner Grabbing
- Demo: The Anatomy of a Web Application Attack
- Web Attack Techniques
- Components of a generic web application system
- URL mappings to the web application system
- Web Application Penetration Methodologies
- Assessment Tool: Stealth HTTP Scanner
- HTTrack Tool: Copying the website offline
- Httprint Tool: Web Server Software ID
- Wikto Web Assessment Tool
- Tool: Paros Proxy
- Tool: Burp Proxy
- Attacks against IIS
- IIS Directory Traversal
- Unicode
- IIS Logs
- What is Cross Side Scripting (XSS)?
- XSS Countermeasures
- Tool: Brutus
- Dictionary Maker
- Query String
- Cookies

- OWASP Top Ten Web Vulnerabilities
- Putting All This To The Test
- Lab - Exercise 1
- Lab - Exercise 2
- Lab - Exercise 3
- Lab - Final Exercise 1
- Lab - Final Exercise 2
- Lab – Summary
- Module 14 Review
- Course Closure