

Course: **CPTS Certified Penetration Testing Specialist**

Description:

Price: \$2,995.00

Category: Popular Courses

Duration: 5 days

Schedule:

[Request Dates](#)

Outline:

TOPICS COVERED

Module 0: Introduction
Module 1: Business and Technical Logistics of Penetration Testing
Module 2: Information Gathering
Module 3: Linux Fundamentals
Module 4: Detecting Live Systems
Module 5: Reconnaissance -- Enumeration
Module 6: Cryptography
Module 7: Vulnerability Assessments
Module 8: Malware – Software Goes Undercover
Module 9: Hacking Windows
Module 10: Advanced Vulnerability and Exploitation Techniques
Module 11: Attacking Wireless Networks
Module 12: Networks, Firewalls, Sniffing and IDS
Module 13: Injecting the Database
Module 14: Attacking Web Technologies

OBJECTIVE OF LABORATORY SCENARIOS

This is an intensive hands-on class; rather than spend too much time installing 300 tools, our focus will be on the Pen Testing model. The latest Pen Testing Tools and methods will be taught. Laboratories change weekly as new methods are found. We will be using many different tools from GUI to command line. As we work through structured attacks, we try and cover tools for both Windows and Linux systems.

DETAILED MODULE DESCRIPTION

Module 1: Business and Technical Logistics of Pen Testing

- Definition of a Penetration Test
- Benefits of a Penetration Test
- ID Theft Statistics
- Recent Hacking News



- The Evolving Threat
- Vulnerability Life Cycle
- Exploit Time Line
- Zombie Statistics
- Zombie Definition
- Botnet Definition
- Types of Penetration Testing
- Pen Testing Methodology
- Hacker vs. Penetration Tester
- Tools vs. Technique
- Penetration Testing Methodologies
- OSSTMM - Open Source Security Testing Methodologies
- Website Review
- SecurityNOW! SX
- Case Study and Lab

Module 2: Information Gathering

- What Information is Gathered by the Hacker
- Methods of Obtaining Information
- Physical Access
- Social Access
- Digital Access
- Passive vs. Active Reconnaissance
- Footprinting Defined
- Footprinting Tool: Kartoo Website.
- Footprinting Tools
- Google and Query Operators
- Johnny.lhackstuff.com.
- Aura
- Wikto
- Websites used for Information Gathering
- Internet Archive: The WayBack Machine
- Domain Name Registration
- Whois
- Websites used to Gather Whois Information
- DNS Databases
- Using NSlookup
- Dig for Unix / Linux
- Traceroute Operation
- EDGAR for USA Company Info.
- Company House For British Company Info
- Intelius info and Background Check Tool
- Web Server Info Tool: Netcraft
- Countermeasure: Domainsbyproxy.com
- Footprinting Countermeasures
- Review White Papers/Templates
- Case Study and Lab.



Module 3: Linux Fundamentals

- History of Linux
- The GNU Operating System
- Linux Introduction
- Desktop Environment
- Linux Shell
- Linux Bash Shell
- Recommended Linux Book
- Password and Shadow File Formats
- User Account Management
- Changing a user account password
- Configuring the Network Interface
- Mounting Drives
- Tarballs and Zips
- Compiling Programs
- Typical Linux Operating Systems
- Gentoo = Simple Software Install Portal
- VLOS and Emerge
- Why Use Live Linux Boot CDs
- Security Live Linux CDs
- FrozenTech's Complete Distro List
- Most Popular: BackTrack
- My Slax Creator
- Slax Modules (Software Packages)
- Case Study and Lab

Module 4: Detecting Live Systems

- Port Scanning Introduction
- Port Scan Tips
- What are the Expected Results
- How Do We Organize the Results
- Ping
- NMAP Introduction
- The TCP/IP Stack
- Ports and Services
- The TCP 3-way Handshake
- TCP Flags
- Vanilla Scan
- NMAP TCP Connect Scan
- Half-open Scan
- Tool Practice : TCP half-open and Ping Scan
- Fire-walled Ports
- NMAP Service Version Detection
- UDP Port Scanning



- Advanced Scanning Technique
- Popular Port Scanning Tools
- Tool: Superscan
- Tool: LookatLan
- Tool: Hping2
- Tool: Auto Scan
- Packet Crafting and Advanced Scanning Methods
- OS Fingerprinting
- OS Fingerprinting: Xprobe2 – Auditor Distro
- Xprobe Practice
- Fuzzy Logic
- Tool: P0f – Passive OS Finger Printing Utility
- Tool Practice: Amap
- Packet Crafting
- Tool Fragrouter: Fragmenting Probe Packets
- Countermeasures: Scanning
- Scanning Tools Summary
- Case Study and Lab

Module 5: Reconnaissance – Enumeration

- Overview of Enumeration
- Web Server Banner
- Practice: Banner Grabbing with Telnet
- Sam Spade Tool: Banner Grabbing
- SuperScan 4 Tool: Banner Grabbing
- SMTP Banner
- DNS Enumeration Methods
- Zone Transfers
- Countermeasure: DNS Zone Transfer
- SNMP Insecurity
- SNMP Enumeration
- SNMP Enumeration Countermeasures
- Active Directory Enumeration
- AD Enumeration countermeasures
- Null Session
- Syntax for a Null Session
- Viewing Shares
- Tool: DumpSec
- Tool: USE42
- Tool: Enumeration with Cain and Abel
- NAT Dictionary Attack Tool
- Injecting the Able Service
- Null Session Countermeasures
- Enumeration Tools Summary
- Case Study and Lab

Module 6: Cryptography

- Cryptography Introduction
- Encryption
- Encryption Algorithm
- Implementation
- Symmetric Encryption
- Symmetric Algorithms
- Crack Times
- Asymmetric Encryption
- Key Exchange
- Hashing
- Hash Collisions
- Common Hash Algorithms
- Hybrid Encryption
- Digital Signatures
- SSL Hybrid Encryption
- IPSEC
- Transport Layer Security – SSH
- PKI ~ Public Key Infrastructure Models
- PKI-Enabled Applications
- Quantum Cryptography
- Hardware Encryption: DESlock
- Attack Vectors
- Case Study & Lab

Module 7: Vulnerability Assessments

- Vulnerability Assessments Introduction
- Testing Overview
- Staying Abreast: Security Alerts
- Vulnerability Scanners
- Qualys Guard
- Nessus Open Source
- Nessus Interface
- Scanning the Network
- Nessus Report
- Retina
- Nessus for Windows
- LANguard
- Analyzing the Scan Results
- Microsoft Baseline Analyzer
- MBSA Scan Report
- Dealing with the Assessment Results
- Patch Management
- Patching with LANguard Network Security Scanner
- Case Study and Lab



Module 8: Malware - Software Goes Undercover

- Defining Malware: Trojans and Backdoors
- Defining Malware: Virus & Worms
- Defining Malware: Spyware
- Company Surveillance Software
- Malware Distribution Methods
- Malware Capabilities
- Auto Start Methods
- Countermeasure: Monitoring Autostart Methods.
- Tool: Netcat
- Netcat Switches
- Executable Wrappers
- Benign EXEs Historically Wrapped with Trojans
- Tool: Restorator
- Tool: Exe Icon
- The Infectious CD-ROM Technique
- Backdoor.Zombam.B
- JPEG GDI+ All in One Remote Exploit
- Advanced Trojans: Avoiding Detection
- Malware Countermeasures
- Gargoyle Investigator
- Spy Sweeper Enterprise
- www.Glocksoft.com
- Port Monitoring Software
- File Protection Software
- Windows File Protection
- Windows Software Restriction Policies
- Hardware-based Malware Detectors
- Countermeasure: User Education
- Case Study and Lab

Module 9: Hacking Windows

- Types of Password Attacks
- Keystroke Loggers
- Password Guessing
- Password Cracking LM/NTLM Hashes
- LanMan Password Encryption
- NT Password Generation
- SysKey Encryption
- Password Salting
- Password Extraction and Password Cracking
- Precomputation Detail
- Cain and Abel's Cracking Methods
- Free LM 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.
- Covering Tracks Overview
- Disabling Auditing
- Clearing the Event Log
- Hiding Files with NTFS Alternate Data Streams
- NTFS Streams Countermeasures
- Stream Explorer
- What is Steganography?
- Steganography Tools
- Shredding Files Left Behind
- Leaving No Local Trace
- SecurSURF
- StealthSurfer II Privacy Stick
- Tor: Anonymous Internet Access
- Encrypted Tunnel Notes
- Rootkits
- Rootkit Countermeasures
- Case Study and Lab.

Module 10: Advanced Vulnerability & Exploitation Techniques

- How Do Exploits Work?
- Memory Organization
- Buffer Overflows
- Stages of Exploit Development
- Prevention
- The Metasploit Project
- Defense in Depth
- Core Impact
- Case Study Lab

Module 11: Attacking Wireless Networks

- Wireless LAN Network Types
- Deployed Standards
- A vs. B vs. G
- 802.11n - MIMO
- SSID - Service Set Identifier
- MAC Filtering
- WEP – 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
- Tool: KNSGEM
- Tool: Kismet
- Analysis Tool: OmniPeek Personal
- Tool: Aircrack
- DOS: Deauth/disassociate attack
- Tool: Aireplay
- ARP Injection (Failure)
- ARP Injection (Success)
- EAP Types
- EAP Advantages/Disadvantages
- Typical Wired/Wireless Network
- EAP/TLS Deployment
- Case Study and Lab

Module 12: Networks, Firewalls, Sniffing and IDS

- Packet Sniffers
- WinPcap / Pcap
- Tool: Wireshark (Ethereal)
- Re-assembling TCP Session Packets
- Tool: Packetyzer
- tcpdump & windump
- Tool: OmniPeek
- Sniffer Detection
- Passive Sniffing Methods
- Active Sniffing Methods
- Flooding the Switch Forwarding Table
- ARP Cache Poisoning in Detail
- ARP Normal Operation
- ARP Cache Poisoning
- Technique: ARP Cache Poisoning (Linux)
- ARP Countermeasures
- Tool: Cain and Abel
- Ettercap
- Dsniff Suite
- MailSnarf, MsgSnarf, FileSnarf
- What is DNS Spoofing?
- DNS Spoofing Tools
- Intercepting and Cracking SSL



- Tool: Breaking SSL Traffic
- Tool: Cain and Abel
- VoIP Systems
- Intercepting VoIP
- Intercepting RDP
- Cracking RDP Encryption
- Routing Protocols Analysis
- Countermeasures for Sniffing
- Firewalls, IDS and IPS
- Firewall ~ 1st Line of Defense
- IDS ~ 2nd 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
- ‘New Age’ Protection
- SpySnare - Spyware Prevention System (SPS)
- Intrusion ‘SecureHost’ Overview
- Intrusion Prevention Overview
- Secure Surfing or Hacking?
- Case Study and Lab

Module 13: Injecting the Database

- Overview of Database Servers
- Types of Databases
- Tables, Records, Attributes, Domains
- Data Normalization, SQL , Object-Oriented Database Management
- Relational Database Systems
- Vulnerabilities and Common Attacks
- SQL Injection
- Why SQL “Injection
- SQL Connection Properties
- SQL Injection: Enumeration
- Extended Stored Procedures
- 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
- Case Study and Lab



Module 14: 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
- 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
- Top Ten Web Vulnerabilities
- Putting all this to the Test
- Case Study and Lab