# Certified Penetration Testing Specialist

**Course Name:**
CPTS
**Duration:** 5 days
**Language:** English
**Format:**
Instructor-led Course (Lecture and Lab)
**Prerequisites:**
• A minimum of 12 months experience in networking technologies
• Sound knowledge of TCP/IP
• Computer hardware knowledge
• Knowledge of Microsoft packages
• Network+, Microsoft Security+
• Knowledge of Linux would be beneficial but not essential
**Student Materials:**
- Student Workbook
- Student Reference Manual
- Software/Tools, 2xDVDs
**Certification Exam:**
CPTS – Certified Pen Testing Specialist™ (Thompson rometric – Globally)

## BENEFITS OF CPTS COURSE

Certified Penetration Testing Specialist graduates would have obtained real world security knowledge that will enable them to recognize vulnerabilities, expose system weaknesses and help safeguard against threats. Graduates will learn the art of Ethical Hacking, but with a professional edge (Penetration Testing).

## COURSE OVERVIEW

CPTS is built upon proven hands-on Penetration Testing methodologies as utilized by our international group of vulnerability consultants. Our trainers keep abreast of their expertise by practicing what they teach because we believe that an equal emphasis on theoretical and real world experience is essential for effective knowledge transfer to you, the student. The CPTS presents information on the latest vulnerabilities and defenses. This class also 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. We go far beyond simply teaching youto “Hack” -- the norm with the classes that have been available until now. Ourcourse is developed based on principles and methods used by malicious hackers, but its focus is professional penetration testing and securing information assets.

## UPON COMPLETION

Upon completion, CPTS students will be able to confidently undertake the Thompson Prometric CPTS examination (recommended) or the Certified Ethical Hacker examination (312-50). Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security environment. This course offers up-to-date proprietary laboratories that have been researched and developed by leading security professionals from around the world.

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

## COURSE DETAILS

**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:** Hacking Windows

**Module 9:** Advanced Vulnerability and Exploitation Techniques

**Module 10:** Malware – Software Goes Undercover

**Module 11:** Attacking Wireless Networks

**Module 12:** 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 spending too much time on theories, 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.

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

## DETAILED MODULE DESCRIPTION

**Module 1: Business and Technical Logistics of Pen Testing**

- Definition of a Penetration Test
- The Evolving Threat
- Vulnerability Life Cycle
- Exploit Time Line
- What You May Not Have Known
- Zombie Statistics
- Zombie Definition
- Botnet Definition
- Defense In Depth
- Types of Penetration Testing
- Pen Testing Methodology
- Hacker vs. Penetration Tester
- Methodology for Penetration
- Tools vs. Technique
- Penetration Testing Methodologies
- OSSTMM - Open Source Security Testing Me
- Website Review
- 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.Ihackstuff.com.
- Site Digger
- Internet Archive: The WayBack Machine
- Domain Name Registration
- Whois
- DNS Databases
- Using NSlookup
- Dig for Unix / Linux
- Traceroute Operation
- EDGAR for USA Company Info.
- People Search Tool
- 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 System
- Gentoo = Simple Software Install Portal
- 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

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

• Company House For British Company Info

**Module 4: Detecting Live Systems**
• Port Scanning Intro
• Port Scan Tips
• Ping
• 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
• Popular Port Scanning Tools
• Tool: Superscan
• Tool: LookatLan
• Tool: Hping2 – BackTrack Distro
• Tool Practice: 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
• 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
• Null Session Countermeasures
• Enumeration Tools Summary
• Case Study and Lab

**Module 6: Cryptography**
• Cryptography Introduction
• Encryption
• 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

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

• Zone Transfers
• Countermeasure: DNS Zone Transfser

**Module 7: Vulnerability Assessments**
• Vulnerability Assessments Introduction
• Staying Abreast: Security Alerts
• Vulnerability Scanners
• Tool: Nessus Open Source
• Nessus Interface
• Scanning the Network
• Nessus Report
• Tool: Retina
• Nessus for Windows
• Tool: 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: Hacking Windows**
• Types of Password Attacks
• Keystroke Loggers
• Password Guessing
• Password Cracking LM/NTLM Hashes
• LanMan Password Encryption
• 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
• Privilege Escalation
• Countermeasure: Monitoring Event Viewer Log
• Hard Disk Security
• Free HD Encryption Software.
• Tokens & Smart Cards.
• Covering Tracks Overview
• Disabling Auditing
• Stream Explorer
• What is Steganography?
• Steganography Tools
• Shredding Files Left Behind
• Leaving No Local Trace
• Free Tool: JAP – Internet Anonymity
• StealthSurfer II Privacy Stick
• More Anonymous Software
• Tor: Anonymous Internet Access
• Encrypted Tunnel Notes
• Rootkits
• Rootkit Countermeasures
• Case Study and Lab.

**Module 9: 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 10: 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
• Remote Access Trojan Components
• Executable Wrappers
• Benign EXEs Historically Wrapped with Trojans
• Tool: Restorator
• Tool: Exe Icon The Infectious CD-ROM Technique

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

- Clearing the Event Log
- Hiding Files with NTFS Alternate Data Streams
- NTFS Streams Countermeasures
- Backdoor.Zombam.B
- JPEG GDI+ All in One Remote Exploit
- Advanced Trojans: Beast

- Advanced Trojans: Avoiding Detectio
- Malware Countermeasures
- 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 11: Attacking Wireless Networks**

- Wireless LAN Network Types
- Deployed Standards
- A vs. B vs. G
- MIMO
- SSID
- MAC Filtering
- WEP Packet Construction
- Weak IV Packets
- XOR Encryption
- WEP Weaknesses
- TKIP
- How WPA improves on WEP
- The WPA MIC Vulnerability WPA2
- WPA and WPA2 Mode Types
- WPA-PSK Encryption
- Tool: NetStumbler
- Tool: Kismet
- Analysis Tool: OmniPeek Personal
- Tool: Aircrack
- DOS: Deauth/disassociate attack
- DoS: VOID 11
- Tool: Aireplay
- ARP Injection (Failure)
- ARP Injection (Success)
- EAP Types
- EAP Advantages/Disadvantages
- Typical Wired/Wireless Network
- EAP/TLS Deployment
- Case Study and Lab
- 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)
- APR 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

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.

**Module 12: Firewalls, Sniffing and IDS**
- Packet Sniffers
- WinPcap / Pcap
- Intrusion Prevention Overview
- Secure Surfing or Hacking ????
- Case Study and Lab

| **Module 13: Injecting the Database** | **Module 14: Attacking Web Technologies** |
|---|---|
| • Overview of Database Servers<br>• Types of Databases<br>• Tables, Records, Attributes, Domains<br>• Data Normalization, SQL , Object-Oriented Database Management<br>• Relational Database Systems<br>• Vulnerabilities and Common Attacks<br>• SQL Injection<br>• Why SQL “Injection<br>• SQL Connection Properties<br>• SQL Injection: Enumeration<br>• Extended Stored Procedures<br>• Shutting Down SQL Server<br>• Direct Attacks<br>• Attacking Database Servers<br>• Obtaining Sensitive Information<br>• Hacking Tool: SQL Ping2<br>• Hacking Tool: osql.exe<br>• Hacking Tool: Query Analyzers<br>• Hacking Tool: SQLExec<br>• Hacking Tool: Metasploit<br>• Hardening Databases<br>• Case Study and Lab | • Common Security Threats<br>• The Need for Monitoring<br>• Seven Management Errors<br>• Progression of The Professional Hacker<br>• The Anatomy of a Web Application Attack<br>• Web Attack Techniques<br>• Components of a generic web application system<br>• URL mappings to the web application system Web Application Penetration Methodologies<br>• Assessment Tool: Stealth HTTP Scanner<br>• HTTrack Tool: Copying the website offline<br>• Httprint Tool: Web Server Software ID<br>• Wikto Web Assessment Tool<br>• Tool: Paros Proxy<br>• Tool: Burp Proxy<br>• Attacks against IIS<br>• ISAPI DLL Source disclosures<br>• ISAPI.DLL Exploit<br>• IIS Directory Traversal<br>• Unicode<br>• IIS Logs<br>• What is Cross Side Scripting (XSS?<br>• XSS Countermeasures<br>• Tool: Brutus<br>• Dictionary Maker<br>• Query String<br>• Cookies<br>• Top Ten Web Vulnerabilities<br>• Putting all this to the Test<br>• Case Study and Lab |

TIP Communication. 01 (52) 55 – 57 31 88 06. Todos los Derechos Reservados. 2008.