

Ethical Hacking & Penetration Testing



KEY DATA

Course Name:

CPTe - Certified Pen Testing Engineer &
EHE - Ethical Hacking Engineer

Duration: 5 days

Language: English

Format:

Instructor-led
Live Virtual Training
CBT - Pre-recorded

Prerequisites:

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

Student Materials:

- Student Workbook
- Student Reference Manual
- Software/Tools, 3xDVDs

Certification Exam:

EHE – Ethical Hacking Engineer™
CPTS – Certified Pen Testing Engineer™
OSCP – Offensive Security Certified Professional

Certification Track:

CPTS - Certified Pen Testing Specialist™
CPTe - Certified Pen Testing Expert™

BENEFITS OF CPTS COURSE

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

COURSE OVERVIEW

EHPT is built upon proven hands-on Penetration Testing methodologies as utilized by our international group of vulnerability consultants. Mile2 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 EHPT presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. The latest vulnerabilities will be discovered using these tried and true techniques. 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 you to “Hack” -- the norm with the classes that have been available until now. Our course is developed based on principles and methods used by malicious hackers, but its focus is professional penetration testing and securing information assets.

Also available as:

LIVE VIRTUAL TRAINING

Attend live class from anywhere in the world!

- Live Presentations with Powerful functionality that delivers easy viewing of slides and other documents, shared Internet access, virtual whiteboard, and a media center all through an easy-to-use toolbar.
- Application, file, and desktop sharing enables you to view live demonstrations.
- Dedicated high spec remote PC per student with full access as if you are sitting in-front of the PC in the classroom.
- Instructor views each students session when you perform your hands on labs, the instructor can access your remote system to demonstrate and assist while you sit back to absorb the classroom style mentoring you expect.
- Public and private text chat allows for increased interactivity between students and instructor



UPON COMPLETION

Upon completion, EHPT students will be able to confidently undertake the CPTe examination (recommended) or the Ethical Hacking Engineer examination or the Offensive Security Certified Professional exam. 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.

COURSE DETAILS

The Basics:

Module 1: Business and Technical Logistics of Penetration Testing

Module 2: Financial Sector Regulations

Module 6: Cryptography

Element 1: Information Gathering

Module 3: Information Gathering

Element 2: Scanning

Module 4: Detecting Live Systems

Element 3: Enumeration

Module 5: Reconnaissance -- Enumeration

Module 7: Vulnerability Assessments

Element 4: Exploitation

Module 8: Malware – Software Goes Undercover

Module 9: Hacking Windows

Module 10: Hacking Unix/Linux

Module 11: Advanced Vulnerability and Exploitation Techniques

Module 12: Attacking Wireless Networks

Module 13: Attacking Bluetooth, RFID and Other Mobile Devices

Module 14: Networks, Firewalls, Sniffing and IDS

Module 15: Injecting the Database

Module 16: Attacking Web Technologies

Element 5: Reporting

Module 17: The Essence of Reporting

OBJECTIVE OF LABORATORY SCENARIOS

This is an intensive hands-on class; you will spend 20 hours or more performing labs; 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 Penetration Testing

- Definition of a Penetration Test
- Benefits of a Penetration Test
- Data Breach Insurance
- What does a hack cost you!
- Recent Issues
- 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
- What to expect for Attacks!
- Website Review
- Module 1 Labs – Getting Set Up
 - Discovering your class share
 - Discovering your student DVD's
 - VM Image Preparation
 - Naming and subnet assignments
 - PDF Penetration Testing Methodology's review

Module 2: Financial Sector Regulations

- IT Governance Best Practices
- 4 Major Components of IT Risk Management
- Types of Risks
- Risk Evaluation
- Improving Security Posture
- Risk Evaluation Activities
- Risk Assessment
- Information Gathering
- Data Classification
- Threats and Vulnerabilities
- Analytical Methods

- Evaluate Controls
- Risk Ratings
- Important Risk Assessment Practices
- Basel II
- GLBA
- FFIEC
- SOX
 - IT Applications and Security
 - Internal Controls
 - IT Issues
- ISO 17799
 - Control Components
- PCI DSS
 - Dirty Dozen
 - Change Control and Auditing
- Total Cost of Compliance
- What does this mean to the tech?
- Module 2 Labs – Linux Fundamentals
 - Install VMware Tools
 - Ifconfig
 - Mounting a USB Thumb Drive
 - Mount a Windows partition
 - VNC Server
 - Preinstalled tools in BackTrack3

Module 3: 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
- Maltego
- Firecat
- Firefox Fully Loaded
- Footprinting Tools
- Google and Query Operators
- Johnny.lhackstuff.com.
- SPUD
- 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
- Client Email Reputation
- Intelius info and Background Check Tool
- Web Server Info Tool: Netcraft
- Countermeasure: Domainsbyproxy.com
- Footprinting Countermeasures
- Review White Papers/Templates
- Module 3 Labs – Information Gathering
 - Google Queries
 - Footprinting Tools
 - Preparing Firefox for Pen Testing
 - Turn in your documentation
- Packet Crafting and Advanced Scanning Methods
- OS Fingerprinting
- OS Fingerprinting: Xprobe2
- Xprobe Practice
- Fuzzy Logic
- Tool: P0f – Passive OS Finger Printing Utility
- Tool Practice: Amap
- Tool Fragrouter: Fragmenting Probe Packets
- Countermeasures: Scanning
- Scanning Tools Summary
- Module 4 Lab – Reconnaissance Scanning
 - LEO Setup
 - Look@LAN
 - Zenmap
 - Zenmap in BackTrack3
 - NMAP Command Line
 - Hping2
 - Unicornscan
 - Turn in your documentation

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: Unicornscan
- Tool: Hping2
- Tool: Auto Scan

Module 5: Reconnaissance – Enumeration

- Overview of Enumeration
- Web Server Banner
- Banner Grabbing with Telnet
- SuperScan 4 Tool: Banner Grabbing
- HTTPPrint
- SMTP Banner
- DNS Enumeration Methods
- Backtrack DNS Enumeration
- Zone Transfers
- Countermeasure: DNS Zone Transfer
- SNMP Insecurity
- SNMP Enumeration
- SNMP Enumeration Countermeasures
- Active Directory Enumeration
- LDAPminer
- AD Enumeration Countermeasures
- Null Session
- Syntax for a Null Session
- Viewing Shares
- Tool: DumpSec
- Tool: Enumeration with Cain and Abel
- NAT Dictionary Attack Tool
- THC-Hydra
- Injecting the Able Service
- Null Session Countermeasures
- Enumeration Tools Summary

- Module 5 Lab – Enumeration
 - Banner Grabbing
 - Zone Transfers
 - SNMP Enumeration
 - LDAP Enumeration
 - Null Sessions
 - SMB Enumeration
 - SMTP Enumeration
 - Turn in your documentation

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
- SSL/TLS
- SSH
- PKI ~ Public Key Infrastructure Models
- PKI-Enabled Applications
- MD5 Hash Collisions Create Rouge CA
- Quantum Cryptography
- Attack Vectors – Password Cracking
- Module 6 Lab – Cryptography
 - Caesar Encryption
 - RC4 Encryption
 - IPSec Deployment

Module 7: Vulnerability Assessments

- Vulnerability Assessments Introduction
- Testing Overview
- Staying Abreast: Security Alerts
- Vulnerability Scanners
- Nessus
- Saint
- Retina

- Qualys Guard
- LANguard
- Analyzing the Scan Results
- Microsoft Baseline Analyzer
- Dealing with the Assessment Results
- Patch Management
- Patching with LANguard Network Security Scanner
- Module 7 Lab – Vulnerability Assessment
 - Install and Run Nessus for Windows
 - Install and Run Saint for Linux
 - Turn in your documentation

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
- BPMTK
- Malware Countermeasures
- Gargoyle Investigator
- Spy Sweeper Enterprise
- Port Monitoring Software
- File Protection Software
- Windows File Protection
- Windows Software Restriction Policies
- Hardware-based Malware Detectors
- Countermeasure: User Education
- Module 8 Lab – Malware
 - Netcat (Basics of Backdoor Tools)
 - Exploiting and Pivoting our Attack
 - Creating a Trojan

- Turn in your documentation

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 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
- Breaking HD Encryption
- 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
- Janus
- StealthSurfer II Privacy Stick
- Tor: Anonymous Internet Access
- Encrypted Tunnel Notes
- Rootkits
- Rootkit Countermeasures
- Module 9 Lab – Hacking Windows
 - Cracking a Windows Password with Linux
 - Cracking a Windows Password with Cain
 - Covering your tracks via Audit Logs

- Alternate Data Streams
- Steganography
- Understanding Rootkits
- Turn in your documentation

Module 10: Hacking Unix/Linux

- Introduction and Background
- File System Structure
- The Kernel
- Processes
 - Starting and Stopping
 - Interacting with Processes
- Account and Groups
- passwd and shadow files
- Permissions
 - Octal Equivalents
 - SetUID
- Trust Relationships
- Logs and Auditing
- Network Services
- Remote Access Attacks
- Brute-Force Attacks
- Brute-Force Countermeasures
- X-Window System
- X Insecurities Countermeasures
- NFS
- NFS in Action
- NFS Countermeasures
- Passwords and Encryption
- Password Cracking Tools
 - Crack
 - John the Ripper
- Salting
- Symlink
- Symlink Countermeasures
- Race Conditions
- Core File Manipulation
- Shared Libraries
- Kernel Flaws
- File and Directory Attacks
- SUID Files Countermeasures
- World-Writeable File Countermeasures
- Clearing the Log Files
- Rootkits
- Rootkit Countermeasures
- Module 10 Lab – Hacking UNIX/Linux
 - Attacking NFS
 - Cracking an MD5 Password

- Clearing the Logs
- Using THC-Hydra
- Rootkits in UNIX/Linux

Module 11: Advanced Vulnerability & Exploitation Techniques

- How Do Exploits Work?
- Memory Organization
- Buffer Overflows
- Stack Function
- Stages of Exploit Development
- Prevention
- The Metasploit Project
- SaintExploit
- Core Impact
- Module 10 Lab –Advanced Vulnerability and Exploitation Techniques
 - Metasploit Command Line
 - Metasploit Web Interface
 - Milw0rm
 - Saint
 - Core Impact
 - Turn in your Documentation

Module 12: Attacking Wireless Networks

- Wireless LAN Network Types
- Deployed Standards
- Standards Comparison
- 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
- LEAP
- LEAP Weaknesses
- Tool: NetStumbler
- Tool: KNSGEM
- Tool: Vistumbler
- Tool: Kismet

- Analysis Tool: OmniPeek Personal
- Tool: Aircrack-ng Suite
 - Airodump-ng
 - Aireplay-ng
 - Death/disassociate attack
 - Aircrack-ng
- Aircrack for Windows
- Attacking WEP
- Attacking WPS
- Tool:coWPAtty
- Exploiting Cisco LEAP
- Tool: asLEAP
- Wirelessdefence.org
- EAP Types
- EAP Advantages/Disadvantages
- EAP/TLS Deployment
- New Age Protection
- Lab 12 –Attacking Wireless Networks
 - Exercise 1 – War Driving Lab
 - Exercise 2 – WEP Cracking
 - Exercise 3 – Turn in your Documentation

Module 13: Attacking Bluetooth, RFID and other Mobile Devices

- GSM
 - Evesdropping in GSM
 - TIMSI Catchers
- RFID
 - RFID Systems
 - RFID Attacks
 - RFID Collisions
- Bluetooth
 - Bluetooth Attacks
 - Man-in-the-Middle
 - Blue-Spam
 - Blue-jacking
 - Weakness in Bluetooth Authentication
- Mobile Devices Mobile Platforms
 - Palm OS
 - iPhone OS X
 - Windows Mobile
 - Symbian
 - Linux
 - Android
 - BlackBerry
- BlackBerry Attacks

- PDA Attacks
- iPhone/iPod Attacks

Module 14: 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?
- Module 14 Lab – Networks, Sniffing and IDS
 - Exercise 1 – Capture FTP Traffic
 - Exercise 2 – ARP Cache Poisoning Basics
 - Exercise 3 – ARP Cache Poisoning - RDP
 - Exercise 4 – Turn in your Documentation

Module 15: 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
- Business Impacts of SQL Injection
- Why SQL “Injection
- SQL Connection Properties
- SQL Injection: Enumeration
- Extended Stored Procedures
- Shutting Down SQL Server
- Direct Attacks
- SQL Connection Properties
- Attacking Database Servers
- Obtaining Sensitive Information
- Hacking Tool: SQL Ping2
- Hacking Tool: osql.exe
- Hacking Tool: Query Analyzers
- Hacking Tool: SQLExec
- www.petefinnegan.com
- Hacking Tool: Metasploit
- Finding and Fixing SQL Injection
- Hardening Databases
- Module 15 Lab – Database Hacking
 - Exercise 1 – Hackme Bank – SQL Injection
 - Exercise 2 – Hackme Bank – Verbose Table Modification
 - Exercise 3 – Hackme Books Setup
 - Exercise 4 – Hackme Books – Denial of Service
 - Exercise 5 – Hackme Books – Data Tampering

- Exercise 6 – Documentation of the assigned tasks

Module 16: Attacking Web Technologies

- Common Web Application Threats
- OWASP Top 10
- 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
- Cross-Site Scripting (XSS)
- Stored XSS Illustrated
- Reflected XSS Illustrated
- Business Impacts of XSS
- Finding and Fixing XSS
- Injection Flaws
- Unvalidated Input
- Unvalidated Input Illustrated
- Business Impacts of Unvalidated Input
- Finding and Fixing Unvalidated Input
- Attacks against IIS
- IIS Directory Traversal
- Unicode
- IIS Logs
- Tool: N-Stalker
- Tool: NTOSpider
- Tool: HTTrack
- Tool: Wikto
- Tool: Paros Proxy
- Tool: Burp Proxy
- Tool: Brutus
- Dictionary Maker
- Query String

- Cookies
- Fuzzers
- Tool: Acunetix Web Scanner
- Tool: Eclipse for Code Review
- Tool: WebScarab
- Samurai Web Pen Testing Framework
- Putting all this to the Test
- Module 14 Lab – Hacking Web Applications
 - Exercise 1 – Input Manipulation
- Exercise 2 –Shoveling a Shell
- Exercise 3 – Hackme Bank – Horizontal Privilege Escalation
- Exercise 4 – Hackme Bank – Vertical Privilege Escalation
- Exercise 5 – Hackme Bank – Cross Site Scripting
- Exercise 6 – Documentation of the assigned tasks

Module 17: The Essence of Reporting

- The Report
- Report Criteria
- Analyzing Risk
- Report Results Matrix
- Findings Matrix
- Delivering the Report
- Stating the Facts
- Recommendations
- Executive Summary
- Technical Report
- Report Table of Contents
- Summary of Security Weaknesses
- Scope of the Project
- Summary Recommendations
- Summary Observations
- Detailed Findings
- Strategic and Technical Directives
- Statement of Responsibilities / Appendices