



A Certified Penetration Testing Expert is a security professional with the ability to plan, manage and perform a penetration test. The designation “Expert” is related to the depth and breadth of understanding required to manage a project involving multiple team members, manage the client’s expectations and deliver an audit of security controls that is thorough, well documented and ethically sound.

This course is designed to take an individual with knowledge of the basic security auditing toolset to the next level. Many courses teach “how to hack”; the CPTE course teaches “the business of penetration testing”. The course delivers advanced and cutting edge techniques for auditing a broad range of security controls (including Physical and User Security) with “hands-on” laboratories designed by real world security auditors.

### **Student Materials :**

1. Student Workbook
2. Student Reference Manual
3. Software/Tools; 2x DVDs

### **Course Benefits**

The CPTE course provides attendees with the unique opportunity to perform all stages of an actual penetration test within a controlled classroom environment. Hands-on laboratories have been researched and developed by leading security professionals from around the world and are continuously updated. The CPTE will cover much more in-depth attacks, techniques, technologies and countermeasures than foundation Penetration Testing and Ethical Hacking courses such as CPTS, CEH and OSPT. Participants of the CPTE course will have the ability to complete laboratories in all of the following areas:

- Perform a penetration test and submit a deliverable report
- Capture and replay unencrypted VoIP traffic
- Find and exploit databases with SQL Injection vulnerabilities
- Manipulate prices on e-commerce websites
- Obtain and transfer information via Bluetooth enabled telephones
- Tools and resources for picking simple and complex locks
- Techniques for Wireless Site Surveying and Cracking WEP/WPA keys

Additionally, attendees will be qualified to confidently undertake the upcoming CPTE practical examination.

## PREREQUISITES

### Prerequisites:

- CPTS, CEH, GIAC, or equivalent knowledge
- A minimum of 24 months experience in Networking Technologies
- Sound knowledge of TCP/IP
- Computer Hardware knowledge
- Experience as a Support Professional or Consultant

## COURSE CONTENTS

### What's Included:

#### Module 1: Intro and Pen Test Overview

- Authorization
- Defining Boundaries
- Objectives and Scope of the Pen Test
- Plan of Attack
- Gathering Information

#### Module 2: Refresher -- The Attack Stage

- Reconnaissance
- Information Gathering
- Scanning
- Enumeration
- Vulnerability Assessments
- Exploiting Systems
- Back Doors/Root Kits
- Covering Tracks
- Wireless Attacks

To ensure that students gain as much as possible from the CPTe course, we start with a refresher on all tools and techniques covered in 'foundation' hacking courses such as CPTS, CEH and OSPT. The subjects covered include information gathering, scanning, enumeration, vulnerability assessments, exploiting systems, packet interception/analysis and wireless detection techniques. Some of the tools the student will use include Sam Spade, SmartWhois, nmap, hping2, xprobe2, RPCclient, LophtCrack, Cain & Abel, Metasploit, Ethereal, Netstumbler, Wellenreiter etc. Each day ends with a Capture the Flag Competition to ensure that participants retain the daily objectives.

#### Module 3: Core Impact -- Initial Pen Test

This lesson will instruct in the use of Core Technologies, market leading commercial penetration testing application. This tool will allow the penetration tester to quickly build up a security snapshot of the target network. From here, the tester will then move onto more advanced manual methods to complete the test. The hands on laboratory will allow the student to use Core Impact to perform a Rapid Pen Test.

#### Module 4: External/DMZ

The first point of contact with a target network will predominantly be through the De-Militarized Zone. This whole section is dedicated to the exploits that apply to this part of the Attack Surface. It is sub-sectioned into:

- DNS/Mail/Web/VPN Servers
- Database Mining-SQL Injection

Database Mining is the process of attacking a database server through the front end. In this section, we open up a network through a SQL server web interface running on a web server inside the DMZ.

Laboratory: Students will be thrust into an online banking environment and will successfully exploit the database front-end to bypass authorization, elevate account privileges, transfer money and manipulate cookies by employing an advanced 'SQL Injection' technique known as 'Blind SQL Injection'. Other attack methods will include VPN IPSEC PSK cracking, circumventing DNS, Mail and Web servers using the latest techniques.

## Module 5: Wireless Site Surveying

During this module, the students will learn all about the current security mechanisms employed to secure wireless networks, WEP/WPA/WPA2 and 802.11x. After talking about the security of these networks, we cover the attacks to bypass all of the security.

Laboratory: Most corporate wireless networks are now protected with encryption such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA). The auditing of these networks requires the tester to attempt to break that encryption. This is exactly what the student will do! We use advanced techniques to break WEP encryption by re-injecting encrypted packets back onto the network and cracking the key in as little as 10 minutes. The tool set the student will become expert with includes kismet, airodump, aireplay, aircrack and cowpatty.

## Module 6: Attacking Bluetooth Devices

As more and more Bluetooth devices appear on the corporate network, the professional penetration tester has to enhance his/her skills to encompass this technology. PDAs, cell phones and other BT devices are all vulnerable to attacks. The hands-on laboratory will teach the students the practical skills required to discover BT devices and retrieve personal information from cell phones and even make phone calls on somebody else's bill! The tool set includes BTscanner, ghattotooth, redfang and bluesnarfer.

## Module 7: Programming 101

This module is not designed as a 'learn programming in one easy step' as that is not possible. We focus our students' efforts on checking code obtained from underground websites so that it will compile correctly and perform the actions it is meant to. We cannot use a new tool on a client network without first ensuring it is safe.

## Module 8: Internal Pen Testing

Once inside the external defenses, the penetration tester has a whole different set of techniques and tools to use. This module is dedicated to internal testing. It is sub-sectioned into:

- Database Servers
- Network Attacks
- Password Retrieval and Cracking

Having a direct connection to a database server will allow many more attack vectors such as database discovery, enumeration and direct exploits like buffer overflows. We cover the market leading database Laboratory: ARP Cache Poisoning, SSH/SSL Man-In-The-Middle Attacks, Voice Over IP interception and DNS Poisoning, Protocol Analysis, Password Cracking (Dictionary/Brute Force/Hybrid/Rainbow Tables), Buffer Overflow/Heap Overflow/Stack Overflow Exploits are just some of the attacks in this module, all of which will enable the penetration tester to expose the weaknesses of the network.

## Module 9: Physical Security

Physical access to a client's building can offer the penetration tester a whole host of powerful attack vectors. This module will teach the student how to gain access by picking the door locks and padlocks securing the building. Yes, you read correctly! By the end of the hands on laboratory, the student will be able to open most common types of pin tumbler door locks and 90% of padlocks available on the market. Most 'Ethical Hacking' courses talk about the theory of physical access, the CPTC covers the practical art of physical access.

## Module 10: After the Pen Test

Laboratory: Presentation of the Penetration Test Report

1. Most lessons have hands-on laboratories.
2. Laboratories will change continuously, adapting to changes in the security industry.
3. Mile2 consultants working in the security field will be dynamically implementing new scenarios that are over and above the base laboratories used in student workbooks.
4. Please note that this is not a class that will explain the very intricacies of each and every tool. The software is mostly open source and underground software which leaves us with no guarantee of compatibility.
5. Mile2 consultants constantly test most of the tools used in this class; however, we may use a tool that is not tested in the environment we have at our partner's site.
6. We will be using a large array of Operating Systems that are set-up to be used in different ways, perhaps to attack or to use as a hacker box.

VMware is used very often in the class. It would be helpful if you download a trial version prior to the class.