

# Certified Penetration Testing Engineer

## KEY DATA

**Course Title:** Certified Penetration Testing Engineer

**Duration:** 5 days

**Language:** English

**Class Format Options:**

- Instructor-led classroom
- Live Online Training
- CBT - Pre-recorded Videos

**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 Lab Guide
- Prep Guide

**Certification Exam:**

C)PTE – Certified Pen Testing Engineer™ (taken through mile2's MACS online testing system)

**CPEs: 40**

**Who Should Attend:**

- Pen Testers
- Ethical Hackers
- Network Auditors
- Cyber Security Professionals
- Vulnerability Assessors
- Cyber Security Managers
- IS Managers

## COURSE OVERVIEW

The vendor neutral **Certified Penetration Testing Engineer** certification course is built firmly upon proven, hands-on, Penetration Testing methodologies utilized by our international group of Penetration Testing consultants.

The C)PTE 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 course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls to reduce risk associated to working with the internet. The student will be using the latest tools, such as **Saint, Metasploit** through **Kali Linux** and **Microsoft PowerShell**.

Mile2 goes far beyond simply teaching you to "Hack". The C)PTE was developed around principles and behaviors used to combat malicious hackers and focuses on professional penetration testing rather than "ethical hacking".

Besides utilizing ethical hacking methodologies, the student should be prepared to learn penetration testing methodologies using advanced persistent threat techniques. In this course, you will go through a complete penetration test from A-Z! **You'll learn to create your own assessment report and apply your knowledge immediately in the work force.**

With this in mind, the C)PTE certification course is a complete up-grade to the EC-Council CEH! The C)PTE exam is taken any time/anywhere on-line through mile2's MACS system, making the exam experience easy and mobile. Student does not need to take the C)PTE course to attempt the C)PTE exam.

## Pen Testing Hacking Career



## All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Guide
- Exam
- Cyber Range Lab



## ACCREDITATIONS



# NICCS™

NATIONAL INITIATIVE FOR  
CYBERSECURITY CAREERS AND STUDIES



is ACCREDITED by the NSA CNSS 4011-4016  
Is MAPPED to NIST/Homeland Security NICCS's Cyber Security Workforce Framework  
is APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

The Certified Penetration Testing Engineer course is accredited by the NSA CNSSI-4013: National Information Assurance Training.

## UPON COMPLETION

Upon completion, **Certified Penetration Testing Engineer** students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the C)PTE exam.

## EXAM INFORMATION

The **Certified Penetration Testing Engineer** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is \$400 USD and must be purchased from Mile2.com.



## COURSE DETAILS

- Module 0: Course Overview
- Module 1: Business & Technical Logistics of Pen Testing
- Module 2: Linux Fundamentals
- Module 3: Information Gathering
- Module 4: Detecting Live Systems
- Module 5: Enumeration
- Module 6: Vulnerability Assessments
- Module 7: Malware Goes Undercover
- Module 8: Windows Hacking
- Module 9: Hacking UNIX/Linux

- Module 10: Advanced Exploitation Techniques
  - Module 11: Pen Testing Wireless Networks
  - Module 12: Networks, Sniffing and IDS
  - Module 13: Injecting the Database
  - Module 14: Attacking Web Technologies
  - Module 15: Project Documentation
  - Module 16: Securing Windows w/ Powershell\*
  - Module 17: Pen Testing with Powershell\*
- \*(Module 16 & 17) will be introduced in August courses



## DETAILED HANDS-ON LABORATORY OUTLINE

### Module 1 Lab – Getting Set Up

- Exercise 1 – Naming and subnet assignments
- Exercise 2 – Discovering your class share
- Exercise 3 – VM Image Preparation
- Exercise 4 – Discovering the Student Materials
- Exercise 5 – PDF Penetration Testing Methodology's review

### Module 2 Lab – Linux Fundamentals

- Exercise 1 – ifconfig
- Exercise 2 – Mounting a USB Thumb Drive
- Exercise 3 – Mount a Windows partition
- Exercise 4 – VNC Server
- Exercise 5 – Preinstalled tools in Kali Linux

### Module 3 Lab – Information Gathering

- Exercise 1 – Google Queries
- Exercise 2 – Footprinting Tools
- Exercise 3 – Getting everything you need with Maltego
- Exercise 4 – Using Firefox for Pen Testing
- Exercise 5 – Documentation of the assigned tasks

### Module 4 Lab – Detecting Live Systems

- Exercise 1 – Look@LAN
- Exercise 2 – Zenmap
- Exercise 3 – Zenmap in Kali Linux
- Exercise 4 – NMAP Command Line
- Exercise 5 – Hping2/3
- Exercise 6 – Unicornscan
- Exercise 7 – Documentation of the assigned tasks

### Module 5 Lab – Reconnaissance

- Exercise 1 – Banner Grabbing
- Exercise 2 – Zone Transfers
- Exercise 3 – SNMP Enumeration
- Exercise 4 – LDAP Enumeration
- Exercise 5 – Null Sessions
- Exercise 6 – SMB Enumeration
- Exercise 7 – SMTP Enumeration
- Exercise 8 – Documentation of the assigned tasks

### Module 6 Lab – Vulnerability Assessment

- Exercise 1 – Run Nessus for Windows
- Exercise 2 – Run Saint
- Exercise 3 – Documentation of the assigned tasks

### Module 7 Lab – Malware

- Exercise 1 – Netcat (Basics of Backdoor Tools)
- Exercise 2 – Exploiting and Pivoting our Attack
- Exercise 3 – Creating a Trojan
- Exercise 4 – Documentation of the assigned tasks

### Module 8 Lab – Windows Hacking

- Exercise 1 – Cracking a Windows Password with Linux
- Exercise 2 – Cracking a Windows Password with Cain
- Exercise 3 – Covering your tracks via Audit Logs
- Exercise 4 – Alternate Data Streams
- Exercise 5 – Stegonagraphy
- Exercise 6 – Understanding Rootkits
- Exercise 7- Windows 7 Client Side Exploit (Browser)
- Exercise 8- Windows 2008 SMBv2 Exploit
- Exercise 9 – Documentation of the assigned tasks

### Module 9 Lab – Hacking UNIX/Linux

- Exercise 1 – Setup and Recon – Do you remember how?
- Exercise 2 – Making use of a poorly configured service
- Exercise 3 – Cracking a Linux password
- Exercise 4 – Creating a backdoor and covering our tracks
- Exercise 5 – Documentation of the assigned tasks

### Module 10 Lab – Advanced Vulnerability and Exploitation Techniques

- Exercise 1 – Metasploit Command Line
- Exercise 2 – Metasploit Web Interface
- Exercise 3 – Exploit-DB.com
- Exercise 4 – Saint
- Exercise 5 – Documentation

### Module 11 Lab – Attacking Wireless Networks

- Exercise 1 – War Driving Lab
- Exercise 2 – WEP Cracking Lab (classroom only)
- Exercise 3 – Documentation

### Module 12 Lab – Networks, Sniffing and IDS

- Exercise 1 – Capture FTP Traffic
- Exercise 2 – ARP Cache Poisoning Basics
- Exercise 3 – ARP Cache Poisoning – RDP
- Exercise 4 – Documentation

### Module 13 Lab – Database Hacking

- Exercise 1 – Hacme Bank – Login Bypass

Exercise 2 – Hacme Bank – Verbose Table Modification  
Exercise 3 – Hacme Books – Denial of Service  
Exercise 4 – Hacme Books – Data Tampering  
Exercise 5 – Documentation of the assigned tasks

### **Module 14 Lab – Hacking Web Applications**

Exercise 1 – Input Manipulation  
Exercise 2 – Shoveling a Shell  
Exercise 3 – Hacme Bank – Horizontal Privilege Escalation  
Exercise 4 – Hacme Bank – Vertical Privilege Escalation  
Exercise 5 – Hacme Bank – Cross Site Scripting  
Exercise 6 – Documentation of the assigned tasks

### **Module 15 Lab – Cryptography**

Exercise 1 – Caesar Encryption  
Exercise 2 – RC4 Encryption  
Exercise 3 – IPSec Deployment  
Post-Class Lab – CORE IMPACT  
Exercise 1 – CORE IMPACT

### **Module 16 & 17 Lab – Powershell\***

Lab 1 – Setting up Powershell  
Lab 2 – Securing Windows w/ Powershell  
Lab 3 – Pen testing w/ Powershell

### **FINAL LAB: FULL PENETRATION TESTING LAB - 4 Hour Session**

## **DETAILED COURSE OUTLINE**

### **Module 0: Course Introduction**

Courseware Materials  
Course Overview  
Course Objectives  
CPTe Exam Information

Learning Aids  
Labs  
Class Prerequisites  
Student Facilities

### **Module 1: Business and Technical Logistics of Penetration Testing**

Overview  
What is a Penetration Test?  
Benefits of a Penetration Test  
Data Breach Insurance  
CSI Computer Crime Survey  
Recent Attacks & Security Breaches  
What does a Hack cost you?  
Internet Crime Complaint Center  
The Evolving Threat  
Security Vulnerability Life Cycle  
Exploit Timeline  
Zombie Definition  
What is a Botnet?  
How is a Botnet Formed?

Botnet Statistics  
How are Botnet's Growing?  
Types of Penetration Testing  
Hacking Methodology  
Methodology for Penetration Testing  
Penetration Testing Methodologies  
Hacker vs. Penetration Tester  
Not Just Tools  
Website Review  
Tool: SecurityNOW! SX  
Seven Management Errors  
Review

### **Module 2: Linux Fundamentals**

Overview  
Linux History: Linus + Minix = Linux  
The GNU Operating System  
Linux Introduction  
Linux GUI Desktops  
Linux Shell  
Linux Bash Shell  
Recommended Linux Book

Password & Shadow File Formats  
User Account Management  
Instructor Demonstration  
Changing a user account password



## Module 3: Information Gathering

Overview  
What Information is gathered by the Hacker?  
Organizing Collected Information  
Leo meta-text editor  
Free Mind: Mind mapping  
IHMC CmapTools  
Methods of Obtaining Information  
Physical Access  
Social Access  
Social Engineering Techniques  
Social Networks  
Instant Messengers and Chats  
Digital Access  
Passive vs. Active Reconnaissance  
Footprinting defined  
Maltego  
Maltego GUI  
FireCAT  
Footprinting tools  
Google Hacking  
Google and Query Operators  
SiteDigger

Job Postings Blogs & Forums  
Google Groups / USENET  
Internet Archive: The WayBack Machine  
Domain Name Registration  
WHOIS  
WHOIS Output  
DNS Databases  
Using Nslookup  
Dig for Unix / Linux  
Traceroute Operation  
Traceroute (cont.)  
3D Traceroute  
Opus online traceroute  
People Search Engines  
Intelius info and Background Check Tool  
EDGAR For USA Company Info  
Company House For British Company Info  
Client Email Reputation  
Web Server Info Tool: Netcraft  
Footprinting Countermeasures  
DOMAINSBYPROXY.COM  
Review

## Module 4: Detecting Live System

Overview  
Introduction to Port Scanning  
Port Scan Tips  
Expected Results  
Popular Port Scanning Tools  
Stealth Online Ping  
NMAP: Is the Host online  
ICMP Disabled?  
NMAP TCP Connect Scan  
TCP Connect Port Scan  
Tool Practice : TCP half-open & Ping Scan  
Half-open Scan  
Firewalled Ports  
NMAP Service Version Detection  
Additional NMAP Scans  
Saving NMAP results  
NMAP UDP Scans

UDP Port Scan  
Advanced Technique  
Tool: Superscan  
Tool: Look@LAN  
Tool: Hping2/3  
Tool: Hping2/3  
More Hping2/3  
Tool: Auto Scan  
OS Fingerprinting: Xprobe2  
Xprobe2 Options  
Xprobe2 -v -T21-500 192.168.XXX.XXX  
Tool: P0f  
Tool Practice: Amap  
Tool: Fragrouter: Fragmenting Probe Packets  
Countermeasures: Scanning  
Review

## Module 5: Enumeration

Enumeration Overview  
Web Server Banners  
Practice: Banner Grabbing with Telnet  
SuperScan 4 Tool: Banner Grabbing  
Sc HTTPPrint  
SMTP Server Banner  
DNS Enumeration  
Zone Transfers from Windows 2000 DNS  
Backtrack DNS Enumeration  
Countermeasure: DNS Zone Transfers  
SNMP Insecurity  
SNMP Enumeration Tools  
SNMP Enumeration Countermeasures

Active Directory Enumeration  
LDAPMiner  
AD Enumeration countermeasures  
Null sessions  
Syntax for a Null Session  
Viewing Shares  
Tool: DumpSec  
Tool: Enumeration with Cain and Abel  
NAT Dictionary Attack Tool  
THC-Hydra  
Injecting Abel Service  
Null Session Countermeasures  
Review

## Module 6: Vulnerability Assessments

Overview  
Vulnerabilities in Network Services  
Vulnerabilities in Networks  
Vulnerability Assessment Def  
Vulnerability Assessment Intro  
Testing Overview  
Staying Abreast: Security Alerts  
Vulnerability Research Sites  
Vulnerability Scanners  
Nessus  
Nessus Report

SAINT – Sample Report  
Tool: Retina  
Qualys Guard  
<http://www.qualys.com/products/overview/>  
Tool: LANguard  
Microsoft Baseline Analyzer  
MBSA Scan Report  
Dealing with Assessment Results  
Patch Management  
Other Patch Management Options

## Module 7: Malware Goes Undercover

Overview  
Distributing Malware  
Malware Capabilities  
Countermeasure: Monitoring Autostart Methods  
Tool: Netcat  
Netcat Switches  
Netcat as a Listener  
Executable Wrappers  
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  
BPMTK  
Malware Countermeasures  
Gargoyle Investigator  
Spy Sweeper Enterprise  
CM Tool: Port Monitoring Software  
CM Tools: File Protection Software  
CM Tool: Windows File Protection  
CM Tool: Windows Software  
Restriction Policies  
CM Tool: Hardware Malware Detectors  
Countermeasure: User Education

## Module 8: Windows Hacking

### Overview

Password Guessing  
LM/NTLM Hashes  
LM Hash Encryption  
NT Hash Generation  
Syskey Encryption  
Cracking Techniques  
Precomputation Detail  
Creating Rainbow Tables  
Free Rainbow Tables  
NTPASSWD:Hash Insertion Attack  
Password Sniffing  
Windows Authentication Protocols  
Hacking Tool: Kerbsniff & KerbCrack  
Countermeasure: Monitoring Logs  
Hard Disk Security  
Breaking HD Encryption  
Tokens & Smart Cards

Password Cracking  
USB Tokens  
Covering Tracks Overview  
Disabling Auditing  
Clearing and Event log  
Hiding Files with NTFS Alternate Data Stream  
NTFS Streams countermeasures  
What is Steganography?  
Steganography Tools  
Shedding Files Left Behind  
Leaving No Local Trace  
Tor: Anonymous Internet Access  
How Tor Works  
TOR + OpenVPN= Janus VM  
Encrypted Tunnel Notes:  
Hacking Tool: RootKit  
Windows RootKit Countermeasures

## Module 9: Hacking UNIX/Linux

### Overview

Introduction  
File System Structure  
Kernel  
Processes  
Starting and Stopping Processes  
Interacting with Processes  
Command Assistance  
Interacting with Processes  
Accounts and Groups  
Password & Shadow File Formats  
Accounts and Groups  
Linux and UNIX Permissions  
Set UID Programs  
Trust Relationships  
Logs and Auditing  
Common Network Services  
Remote Access Attacks  
Brute-Force Attacks  
Brute-Force Countermeasures

X Window System  
X Insecurities Countermeasures  
Network File System (NFS)  
NFS Countermeasures  
Passwords and Encryption  
Password Cracking Tools  
Salting  
Symbolic Link  
Symlink Countermeasure  
Core File Manipulation  
Shared Libraries  
Kernel Flaws  
File and Directory Permissions  
SUID Files Countermeasure  
File and Directory Permissions  
World-Writable Files Countermeasure  
Clearing the Log Files  
Rootkits  
Rootkit Countermeasures  
Review

## Module 10: Advanced Exploitation Techniques

### Overview

How Do Exploits Work?  
Format String  
Race Conditions  
Memory Organization

Buffer OverFlows  
Buffer Overflow Definition  
Overflow Illustration

How Buffers and Stacks  
Are  
Supposed to Work  
Stack Function  
How a Buffer Overflow Works  
Buffer Overflows  
Heap Overflows  
Heap Spraying  
Prevention  
Security Code Reviews  
Stages of Exploit Development  
Shellcode Development

The Metasploit Project  
The Metasploit Framework  
Meterpreter  
Fuzzers  
SaintExploit at a Glance  
SaintExploit Interface  
Core Impact Overview  
Review

## Module 11: Pen Testing Wireless Networks

Overview  
Standards Comparison  
SSID (Service Set Identity)  
MAC Filtering  
Wired Equivalent Privacy  
Weak IV Packets  
WEP Weaknesses  
XOR – Encryption Basics  
How WPA improves on WEP  
TKIP  
The WPA MIC Vulnerability  
802.11i - WPA2  
WPA and WPA2 Mode Types  
WPA-PSK Encryption  
LEAP  
LEAP Weaknesses  
NetStumbler  
Tool: Kismet  
Tool: Aircrack-ng Suite  
Tool: Airodump-ng  
Tool: Aireplay  
DOS: Deauth/disassociate attack  
Tool: Aircrack-ng  
Attacking WEP  
Attacking WPA  
coWPAtty  
Exploiting Cisco LEAP  
asleep  
WiFiZoo  
Wesside-ng  
Typical Wired/Wireless Network  
802.1X: EAP Types  
EAP Advantages/Disadvantages  
EAP/TLS Deployment  
New Age Protection  
Aruba – Wireless Intrusion Detection and Prevention  
RAPIDS Rogue AP Detection Module  
Review

## Module 12: Networks, Sniffing, IDS

Overview  
Example Packet Sniffers  
Tool: Pcap & WinPcap  
Tool: Wireshark  
TCP Stream Re-assembling  
Tool: Packetizer  
tcpdump & windump  
Tool: OmniPeek  
Sniffer Detection Using Cain & Abel  
Active Sniffing Methods  
Switch Table Flooding  
ARP Cache Poisoning  
ARP Normal Operation  
ARP Cache Poisoning Tool  
Countermeasures  
Tool: Cain and Abel  
Ettercap  
Linux Tool Set: Dsniff Suite  
Dsniff Operation  
MailSnarf, MsgSnarf, FileSnarf  
What is DNS spoofing?  
Tools: DNS Spoofing  
Session Hijacking  
Breaking SSL Traffic  
Tool: Breaking SSL Traffic  
Tool: Cain and Abel  
Voice over IP (VoIP)  
Intercepting VoIP



### Intercepting RDP

- Cracking RDP Encryption
- Routing Protocols Analysis
- Countermeasures for Sniffing
- Countermeasures for Sniffing
- Evading The Firewall and IDS
- Evasive Techniques

- Firewall – Normal Operation
- Evasive Technique -Example
- Evading With Encrypted Tunnels
- Newer Firewall Capabilities
- 'New Age' Protection
- Networking Device – Bastion Host
- Spyware Prevention System (SPS)
- Intrusion 'SecureHost' Overview
- Intrusion Prevention Overview
- Review

## Module 13: Injecting the Database

- Overview
- Vulnerabilities & Common Attacks
- SQL Injection
- Impacts of SQL Injection
- Why SQL "Injection"?
- SQL Injection: Enumeration
- SQL Extended Stored Procedures
- Direct Attacks
- SQL Connection Properties
- Attacking Database Servers

- Obtaining Sensitive Information
- Hacking Tool: SQLScan
- Hacking Tool: osql.exe
- Hacking Tool: Query Analyzers
- Hacking Tool: SQLExec
- www.petefinnegan.com
- Hacking Tool: Metasploit
- Finding & Fixing SQL Injection
- Hardening Databases
- Review

## Module 14: Attacking Web Technologies

- Overview
- Web Server Market Share
- Common Web Application Threats
- Progression of a Professional Hacker
- Anatomy of a Web Application Attack
- Web Applications Components
- Web Application Penetration Methodologies
- URL Mappings to Web Applications
- Query String
- Changing URL Login Parameters
- Cross-Site Scripting (XSS)
- Injection Flaws
- Unvalidated Input
- Unvalidated Input Illustrated
- Impacts of Unvalidated Input
- Finding & Fixing Un-validated Input
- Attacks against IIS

- Unicode
- IIS Directory Traversal
- IIS Logs
- Other Unicode Exploitations
- N-Stalker Scanner 2009
- NTOSpider
- HTTrack Website Copier
- Wikto Web Assessment Tool
- SiteDigger v3.0
- Paros Proxy
- Burp Proxy
- Brutus
- Dictionary Maker
- Cookies
- Acunetix Web Scanner
- Samurai Web Testing Framework

## Module 15: Project Documentation

- Overview
- Additional Items
- The Report
- Report Criteria:
- Supporting Documentation
- Analyzing Risk
- Report Results Matrix
- Findings Matrix

- Delivering the Report
- Stating Fact
- Recommendations
- Executive Summary
- Technical Report
- Report Table of Contents
- Summary of Security Weaknesses Identified
- Scope of Testing



- Summary
- Recommendations
- Summary Observations
- Detailed Findings
- Strategic and Tactical Directives
- Statement of Responsibility / Appendices