C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

Certified Penetration Testing Engineer

KEY DATA

Course Title: Certified Penetration Testing Engineer

Duration: 5 days

Language: English

Class Format Options:

- Instructor-led classroom

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:

CPTE – Certified Pen Testing Engineer™

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 CPTE certification course is a complete up-grade to the EC-Council CEH!

Pen Testing Hacking Career

C)VA™ Certified Vulnerability Assessor

C)PEH™ CERTIFIED PROFESSIONAL ETHICAL HACKER

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER *

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

All Combos Include:

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

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS — SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION — FIDELITY BRAVERY INTEGRITY

mile2 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** will take 2 hours and consist of 100 multiple choice questions.

macs Assessment & Certification System

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

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

DETAILED HANDS-ON LABORATORY OUTLINE

Lab 1 – Introduction to Pen Testing Setup
Section 1 – Recording IPs and Logging into the VMs
Section 2 – Research

Lab 2 – Linux Fundamentals
Section 1 – Command Line Tips & Tricks
Section 2 - Linux Networking for Beginners
Section 3 – Using FTP during a pentest

Lab 3 – Using tools for reporting
Section 1 – Setting up and using magictree

Lab 4 – Information Gathering
Section 1 – Google Queries
Section 2 – Searching Pastebin
Section 3 – Automated Vulnerabilities Search using Search Diggity
Section 4 – Maltego
Section 5 – People Search Using the Spokeo Online Tool
Section 6 – Recon with Firefox
Section 7 – Documentation

Lab 5 – Detecting Live Systems - Scanning Techniques
Section 1 – Finding a target using Ping utility
Section 2 – Footprinting a Target Using nslookup Tool
Section 3 – Scanning a Target Using nmap Tools
Section 4 – Scanning a Target Using Zenmap Tools
Section 5 – Scanning a Target Using hping3 Utility
Section 6 – Make use of the telnet utility to perform banner grabbing
Section 7 – Documentation

Lab 6 – Enumeration
Section 1 – OS Detection with Zenmap
Section 2 – Enumerating a local system with Hyena
Section 3 – Enumerating services with nmap
Section 4 – DNS Zone Transfer
Section 5 – LDAP Enumeration

Lab 7 – Vulnerability Assessments
Section 1 – Vulnerability Assessment with SAINT
Section 2 – Vulnerability Assessment with OpenVAS

Lab 8 – Software Goes Undercover
Section 1 – Creating a Virus

Lab 9 – System Hacking – Windows Hacking
Section 1 – System Monitoring and Surveillance
Section 2 – Hiding Files using NTFS Streams
Section 3 – Find Hidden ADS Files
Section 4 – Hiding Files with Stealth Tools
Section 5 – Extracting SAM Hashes for Password cracking
Section 6 – Creating Rainbow Tables
Section 7 – Password Cracking
Section 8 – Mimikatz

Lab 10 – System Hacking – Linux/Unix Hacking
Section 1 – Taking Advantage of Misconfigured Services
Section 2 – Cracking a Linux Password
Section 3 – Setting up a Backdoor

Lab 11 – Advanced Vulnerability and Exploitation Techniques
Section 1 – Metasploitable Fundamentals
Section 2 – Metasploit port and vulnerability scanning
Section 3 – Client-side attack with Metasploit
Section 4 – Armitage

Lab 12 – Network Sniffing/IDS
Section 1 – Sniffing Passwords with Wireshark
Section 2 – Performing MitM with Cain
Section 3 – Performing MitM with sslstrip

Lab 13 – Attacking Databases
Section 1 – Attacking MySQL Database
Section 2 – Manual SQL Injection

Lab 14 – Attacking Web Applications
Section 1 – Attacking with XSS
Section 2 – Attacking with CSRF

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

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
Configuring Network Interfaces with Linux
Mounting Drives with Linux
Tarballs and Zips
Compiling Programs in Linux
Why Use Live Linux Boot CDs
Typical Linux Operating Systems

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
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 HTTPrint
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
asleap
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: Packetyzer
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

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
Summary
Recommendations
Summary Observations
Detailed Findings
Strategic and Tactical Directives
Statement of Responsibility / Appendices
Recommendations
Executive Summary
Technical Report
Report Table of Contents
Summary of Security Weaknesses Identified
Scope of Testing