



Certified Penetration Testing Engineer

Duration: 5 Days

Language: English

Course Delivery: Classroom

COURSE BENEFITS

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.

Examination

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

Course Outline

Module 0: Course Introduction

Courseware Materials

Course Overview

Course Objectives

C)PTE 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?

Module 2: Linux Fundamentals

Overview
Linux History: Linux + 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

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

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

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

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

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

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

Client Email Reputation
Web Server Info Tool: Netcraft
Footprinting Countermeasures
DOMAINSBYPROXY.COM
Review

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: POF
Tool Practice: Amap
Tool: Fragrouter: Fragmenting Probe Packets
Countermeasures: Scanning
Review

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

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

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

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

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

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

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: 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



أكاديمية اتصالات
etisalat academy
Skills | Solutions | Results

Report Table of Contents
Summary of Security Weaknesses Identified
Scope of Testing

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