



[Back to Product Page](#)

## Pen. Testing Foundations Course

**3 Sessions -**

11 Hours of Interactive Training

The Pen Testing Foundations training course is the 1st step in the CPTEngineer series which is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. The latest vulnerabilities will be discovered using these tried and true techniques. Expert Duane Anderson will walk you through business skills needed to identify protection opportunities, justify testing activities and optimize security appropriate to the business needs in order to reduce business risk. This course is part one of five training series that will help prepare you to pass the CPTEngineer Certification Exam, formerly known as CPTS.

### Benefits

- Obtain real world security knowledge with the latest Pen Testing Tools and methods
- Recognize vulnerabilities for both Windows and Linux systems
- Learn the art of ethical hacking with a professional edge

## Session 1

### Section A: Pen. Testing Foundations

- Introduction
- Course Overview
- Course Objectives
- The CPTS Exam
- Prerequisites
- Penetration Testing Defined
- Benefits of Pen. Testing
- Data Breach Insurance
- CSI Computer Crime Survey
- Attack Costs
- Vulnerable Institutions
- Internal Threats

### Section B: The Evolving Threat

- Curiosity and Personal Fame Threats
- Scanning Threats
- Security Vulnerability Life Cycle
- Zombies
- Shadowserver.org Stats
- Entropy
- Graphs
- Botnet Locations
- Botnets Defined
- Understanding Botnet Growth

### Section C: Methodologies and Keeping Informed

### Section F: Digital Access/Footprinting

- Digital Access
- Footprinting Defined
- KartOO
- KartOO Website
- Maltego
- Views in Maltego
- Finding Email Addresses
- Firefox Add-On Examples
- FireCAT v1.5
- Firefox Add-Ons

### Section G: Google Hacking and Other Online Tools

- Footprinting Tools
- Google Hijacking Tips
- Illegal vs. Unethical
- Johnny's Website
- Google Hacking Database
- Google Searches
- Kickstart File
- SensePost
- Wayback Machine
- Blogs, Forums, and Newsgroups

### Section H: DNS and Routing Information Gathering

- Domain Name Registration
- WHOIS
- dirk-loss.de/onlinetools
- dnsstuff.com
- CentralOps.net

## About The Author

Duane Anderson, for the last two decades, has been working in the IT Security Training and Consulting Arena. He has worked with US and foreign military branches, U.S. government agencies, banking and regulated industries and fortune 500 companies. Duane has contributed to mile2's security curriculum with Certified Penetration Testing Engineer, Certified Digital Forensics Examiner and Certified Wireless Security Engineer. In addition, he has coordinated and executed IT counter-hacking & security courses for the US Marine Corps, US Army, US Air Force, U.S. Treasury, Sprint, IBM, Washington Mutual and Service Canada. Duane brings a vast wealth of experience and holds the following professional qualifications -- Security+, CPTS, CPTE, CDFE, CEH and Mile2 Certified Instructor.

- Pen. Testing Types
- Hacking Life Cycle
- Methodology for Pen. Testing
- Additional Methodologies
- Methodology Files
- ISSAF (OISSG)
- The OSSTMM Model
- Hacker vs. Pen. Tester
- Website Review
- Dark Reading
- Talisker
- ARBOR Network's Website
- CIOview Player
- Seven Management Errors
- DNS Databases
- Using Nslookup
- Traceroute Operations
- Visual Mapping
- Opus One

## Section I: More Footprinting Tools

- People Search Engines
- Company Information Registration
- Domains By Proxy
- Footprinting Countermeasure Process

## Section D: Configuring a Testing Environment

- VMware Setup
- XP Pentester
- Snapshot Manager
- Inside the VMware
- Toolbar/Views
- Setup Considerations
- BackTrack
- Hardware Association
- Additional Features
- Power On to BIOS
- Cloning the Virtual Machine
- Virtual Appliances
- Virtual Appliance Marketplace

## **Section E: Physical and Social Access**

- Gathered Information
- Physical Access
- Social Access
- Social Engineering Techniques
- Social Websites
- IM and Chat

## **Session 2**

### **Section A: Port Scanning and Dealing with Results**

- Port Scanning
- Sources on TCP/IP
- Organizing Results
- Leo Meta-Text Editor
- FreeMind
- IHMC CmapTools
- Leo
- FreeMind Tool
- CmapTools

### **Section B: Nmap and Its Many Uses**

- Popular Port Scanning Tools
- Nmap
- TCP Connect Scans
- Half-Open Scans
- Firewalled Ports
- IronGeek
- Nmap Service Version Detection
- Additional Nmap Scans
- Saving Nmap Results
- Nmap UDP Scans
- Nmap Idle Scans

### **Section C: Active Reconnaissance at**

### **Section E: Banner Grabbing and DNS Enumeration**

- Enumeration
- Banner Grabbing
- HTTPPrint
- Telnetting via HTTPPrint
- SuperScan 4 with HTTPPrint
- HTTPPrint Report
- SMTP Banners and Nslookup
- DNS Enumeration in BackTrack 3
- DNS Enumeration
- Zone Transfer Countermeasures

### **Section F: SNMP and AD Enumeration**

- SNMP Insecurity
- SNMP Enumeration
- SNMP Countermeasures
- Look@LAN and SNMP
- SNMP Enumeration in BackTrack
- AD Enumeration
- LdapMiner
- AD Enumeration Countermeasures

## Work

- Nmap in Action
- Zenmap
- Intense Scan
- BackTrack Comparison
- System Scan/ Analysis
- Polite Command
- #5 Command
- Grepable Files
- XML Output
- nmapfe in BackTrack

## Section D: Other Active Reconnaissance Tools

- Unicornscan Overview
- How Unicornscan Works
- Unicornscan Simple
- Unicornscan SuperScan
- SuperScan Demo
- Look@LAN and Hping2
- Hping2 In-depth
- Hping2 Demo
- UDP Scans with Hping2
- Other UNIX/Linux Tools
- Fuzzy Logic
- P0f, AMAP and Fragrouter
- Scanning Countermeasures

## Session 3

### Section A: Cracking Windows Passwords

- Password Cracking
- LM Hash Encryption
- NT Hash

### Section G: Null Sessions

- Null Sessions Defined
- Null Session Tools
- Dictionary Attack Tools
- Injecting the Abel Service
- Null Session Countermeasures
- Cain and Abel Enumeration
- Enumeration on Windows 2003
- NAT Dictionary
- Hydra
- Abel Service

### Section F: Accounts, Groups, Permissions, and Logs

- Accounts and Groups
- Passwords/

- Generation
- Syskey Encryption
- Cracking Techniques
- Password Cracking with Cain
- Dictionary Attack
- Import Hash/Rainbow Tables
- Password Recovery Software (ElcomSoft)
- Winrtgen
- The Shmoo Group
- Creating and Using Rainbow Tables
- Hash Insertion Attacks
- Password Sniffing
- Windows Authentication Protocols

### **Section B: Event Logs, Encryption, and Smart Cards**

- Event Viewer
- Hard Disk Security
- Tokens and Smart Cards
- Disable Auditing
- Clearing and Event Logs
- Auditpol
- elsave

### **Section C: ADS and Steganography**

- Alternate Data Streams
- NTFS Countermeasures
- Create Alternate Data Stream
- Finding Alternate Data Streams
- Steganography
- Steganography Software
- Steganography Tools
- Shedding Files

- Shadow File Format
- passwd Information
- Example of Permissions
- Utilizing Accounts and Groups
- UNIX and Linux Permissions
- Permission Indicators
- Setting the UID
- Trust Relationships
- Logs and Auditing

### **Section G: Remote Access Attacks**

- Common Network Services
- Remote Attack Types
- Brute-Force Attacks
- X Window System
- X Window Countermeasures
- Network File System
- Password Encryption Methods
- Password Cracking Tools
- Salting

### **Section H: Local Attacks and Rootkits**

- Symbolic Links
- Core File Manipulations
- Shared Libraries
- Kernel Flaws
- File/Directory Permissions
- World-Readable / Writeable
- Clearing the Log Files
- UNIX/Linux Rootkits
- Rootkit Countermeasures

## **Section D: Anonymous Attacking Applications**

- Leaving No Trace
- SecurSurf
- StealthSurfer II
- Tor
- JanusVM
- Janus Tunneling
- Verification of Connection
- Example of Speed Reduction
- Tunnel Encryption
- Rootkits
- Windows Rootkit Countermeasures
- Rootkit.com
- Rootkit Operations
- Previous Existing Rootkit
- IceSword

## **Section E: UNIX/Linux File System and Processes**

- UNIX and Linux
- File System Structure
- The Kernel
- Processes
- Starting and Stopping Processes
- Start/Stop Example

## **Section I: Hacking an Ubuntu Server**

- Common Attack - Inconfigured Services
- Mount
- Copy Files to tmp
- Reading Data
- Creating a Backdoor
- Sudo Adduser
- Add User to Admin Group
- Destroying the Evidence
- wtmp File
- Altering the File
- Verifying the Illusion