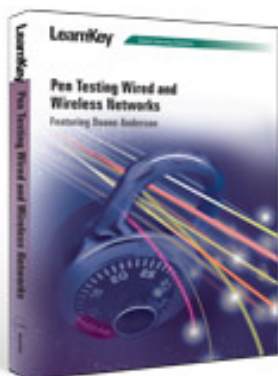


Pen. Testing Wired and Wireless Networks Course



[Back to Product Page](#)

Pen. Testing Wired and Wireless Networks Course

1 Sessions -

4 Hours of Interactive Training

Pen Testing Wired and Wireless Networks training course is the 3rd course in the CPTEngineer series which is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. In this course you will learn to use TCP packet sniffers to understand the methods that attackers use to gather sensitive encrypted data. This course is part three of five training series that will help prepare you to pass the CPTEngineer Certification Exam, formerly known as CPTS.

Benefits

- Learn and master War Driving and Auditing Tools
- WEP and WPA Wireless attack process uncovered
- Implement and configure wireless intrusion detection system

About The Author

Session 1

Section A: Sniffers

- Packet Sniffing
- Wireshark
- Following the TCP Stream
- Additional Wireshark Features
- Packetizer
- Command Line Protocol Analyzers
- The OmniPeek Series
- Cain & Abel
- Active Sniffing Methods

Section B: ARP Poisoning and Sniffing

- Switch Table Flooding
- ARP Cache Poisoning
- ARP Normal Operation
- Countermeasures
- Cache Poisoning Via Cain & Abel
- Ettercap
- Dsniff Suite

Section C: DNS Spoofing and Breaking SSL

- DNS Spoofing
- Session Hijacking
- Breaking SSL Traffic
- Cain & Abel Demo
- Testing on Hotmail
- Testing on Gmail
- Testing on Salesforce
- Testing on Mile2 Site

Section F: War Driving and Auditing Tools

- NetStumbler
- War Driving with KNSGEM
- Vistumbler
- Network Stumbler
- Separate by SSID
- Deriving Global Positioning
- Generating Reports in Google Earth
- Viewing Reports in Google Earth
- Stockholm_C
- Vistumbler Demo
- Kismet
- OmniPeek Personal
- OmniPeek Personal Demo

Section G: Breaking WEP and WPA

- Aircrack-ng Suite
- Aireplay
- Disassociate Attacks
- Aircrack
- Attacking WEP
- Attacking WPA
- coWPATy
- Exploiting Cisco LEAP

Section H: Tools in Action

- Tool Examples
- Aircrack-ng GUI
- BackTrack
- Kismet-Konsole

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.

- Ettercap in BackTrack

Section D: Evading Firewalls and IDS/IPS

- Voice over IP
- Intercepting VoIP
- Intercepting RDP
- Cracking RDP Encryption
- Countermeasures for Sniffing
- Evasive Techniques
- Evasive Techniques Example
- Evading With Encrypted Tunnel
- Newer Firewall Capabilities
- New Age Protection
- Bastion Host
- SpySnare
- Intrusion Prevention

Section E: Wireless Technologies

- Wireless Standards Comparison
- Service Set Identifier
- Wired Equivalent Privacy
- Weak IV Packets
- XOR Basics
- WEP Weaknesses
- WPA Improvements
- TKIP
- MIC Vulnerability
- 802.11i - WPA2
- Connecting to a Wireless Network
- LEAP

Section I: Other Tools and New Age Protection

- WifiZoo
- wesside-ng
- Wirelessdefence.org
- Aruba
- Detection and Prevention
- EAP
- EAP-TLS Deployment
- Wireless Intrusion Detection Systems