



[Back to Product Page](#)

Penetration Vulnerabilities Uncovered Course

1 Sessions -

3 Hours of Interactive Training

The Penetration Vulnerabilities training course is the 2nd step in the CPTEngineer series which is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. In this course expert Duane Anderson will help you understand the techniques necessary to effectively assess your system and network vulnerabilities. In this course you will learn the different tools used to assess system vulnerability and you will learn how and when to use them in the work place. This course is part two of five training series that will help prepare you to pass the CPTEngineer Certification Exam, formerly known as CPTS.

Benefits

- Learn effective malware countermeasures
- Identify and resolve network hardware vulnerabilities
- Implement effective tools for tracking security alerts

Session 1

Section A: Vulnerability Assessments

- Network Service Vulnerabilities
- Network Hardware Vulnerabilities
- When to Apply Vulnerability Assessments
- Vulnerability Assessment Tools
- Security Alerts
- Secunia
- National Vulnerability Database
- Vulnerability Scanners

Section E: Historical Look at Malware

- Executable Wrappers
- eLiTeWrap
- Verify the Wrap
- Zenmap Scan
- Troubleshooting
- Fport
- Delivery Examples
- Restorator
- Exelcon
- Infectious CD-ROM
- Trojan Horses
- Advanced Trojan Horses
- BPMTK

Section B: VA Tools and Results

- Nessus
- SAINT
- Retina
- QualysGuard
- GFI LANguard
- Tool Comparisons
- Microsoft Security Assessment Tool
- Penetration vs. Vulnerability
- Patch Management

Section F: Malware Countermeasures

- Countermeasure Tools
- Gargoyle Investigator
- Spy Sweeper
- Port Monitoring Software
- File Protection Software
- Windows Software Restriction Policies
- Company Surveillance Software
- Hardware-Based Detectors
- User Education

Section C: Vulnerability Assessments at Work

- Using Nessus
- Nessus 4
- Adding Networks/ Policies
- Nessus Options
- Credentials
- Plugin Selection

Section G: Malware in Pen. Testing

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.

- Network/Advanced
- Scans/Results
- Results Continued
- Other Reporting Templates/Files
- Exporting Reports
- SAINT Functions
- Sessions
- Scanning
- Data: Report/Analysis
- Produce Full Report
- SAINT Options
- GFI LANGuard Basics
- Deploying Updates
- NULL Session
- Pivot an Attack
- Additional Netcat Uses
- Banner Grabbing
- DCOM Exploit
- Uploading a File
- Testing the Connection
- Transferring Files via Netcat
- Verifying the Transfer

Section D: Malware and Its Many Uses

- Malware Distribution
- Malware Capabilities
- Auto Starting Malware
- Countermeasures
- HijackThis
- Netcat
- Generic Hash Demo
- Netcat as a Listener
- Netcat Demo