



[Back to Product Page](#)

CPTEngineer Certification Series

0 Sessions -

24 Hours of Interactive Training

The CPTEngineer Certification training is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. Learn to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats. Upon completion of this series you will be prepared to pass the CPTEngineer Certification Exam, formerly known as CPTS.

Benefits

- Prevent your systems from exploitation
- Learn the art of ethical hacking with a professional edge
- Pass the CPTEngineer Certification Exam

Advanced Exploitation Revealed Course Session 1

Section A: The Nature of Exploits

- Exploits
- Format Strings
- Race Conditions
- Memory Organization
- Buffer Overflow
- Buffers and Stacks
- Stack Function
- How a Buffer Overflow Works
- Heap Overflow
- Heap Spraying
- Prevention

Section B: Exploit Development and the Tools

- Exploit Development
- Shellcode Development
- Metasploit
- Meterpreter
- Fuzzers
- Milw0rm
- SAINTexploit
- CORE IMPACT
- Tool Comparison

Section C: Metasploit at Work

- Update Metasploit
- Metasploit Demo

Section D: SAINT and CORE IMPACT at Work

- SAINTexploit Demo
- Exploits
- SAINTwriter
- CORE IMPACT Demo
- Results
- Analyzing the Results

Section E: Documentation and Risk Analysis

- Documentation Assets
- The Report
- Supporting Documentation
- Analyzing Risk
- Report Results Matrix
- Findings Matrix

Section F: Report Content and Delivery

- Delivering the Report
- Stating Fact
- Recommendations
- Executive Summary
- Technical Reports
- Scope of Testing
- Summary Recommendations
- Summary Observations
- Detailed Findings
- Strategic/Tactical Directives
- Statement of Responsibility

- Exploit List
- Payloads
- Command Line Metasploit
- RPC DCOM Exploit
- Metasploit Web Interface
- Restart
- Input Options
- Client Side Attack
- msf Exploit
- Verifying the Exploit
- Pressing the Exploit

Pen. Testing Foundations Course 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

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

- Threats
- Security Vulnerability Life Cycle
- Zombies
- Shadowserver.org Stats
- Entropy
- Graphs
- Botnet Locations
- Botnets Defined
- Understanding Botnet Growth
- 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
- DNS Databases
- Using Nslookup
- Traceroute Operations
- Visual Mapping
- Opus One

Section C: Methodologies and Keeping Informed

- 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

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

Pen. Testing Foundations Course 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

Section E: Banner Grabbing and DNS Enumeration

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

- 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 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

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

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

- Fuzzy Logic
- P0f, AMAP and Fragrouter
- Scanning Countermeasures

Pen. Testing Foundations Course Session 3

Section A: Cracking Windows Passwords

- Password Cracking
- LM Hash Encryption
- NT Hash 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 F: Accounts, Groups, Permissions, and Logs

- Accounts and Groups
- Passwords/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 C: ADS and Steganography

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

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 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

Section E: UNIX/Linux File System and Processes

- UNIX and Linux
- File System Structure
- The Kernel
- Processes
- Starting and Stopping Processes

- Start/Stop Example

Pen. Testing Websites and Databases Course Session 1

Section A: The Essence of SQL Injection

- Databases
- Vulnerabilities / Common Attacks
- SQL Injections
- Impacts of SQL Injection
- Business Impacts of SQL Injection
- Using SQL Injection
- SQL Injection Enumeration
- Extended Stored Procedures
- Lee Lawson Video

Section B: Direct Attacks and Protection

- Direct Attacks
- Attacking Database Servers
- Obtaining Sensitive Information
- Hacking Tools
- Oracle Security Tips
- Metasploit
- Metasploit Demo
- Finding and Fixing SQL Injections
- Hardening Databases

Section C: SQL Injection in Action

Section E: Most Common Attacks Illustrated

- Vertical Privilege Escalation
- XSS: Cross-Site Scripting
- Business Impacts of XSS
- Finding/Fixing XSS
- Injection Flaws
- Unvalidated Input
- Unvalidated Input Illustrated
- Business Impacts of Unvalidated Input
- Finding/Fixing Unvalidated Input
- Attacks Against IIS
- Unicode

Section F: Tools of the Trade Part I

- N-Stalker
- NTOSpider
- Free Web Assessment Tools
- N-Stalker Demo
- HTTrack
- Wikto

Section G: Tools of the Trade Part II

- Injection Attack
- Injection Attack Demo
- Joel Helkason Video

Section D: Attack Methods

- Web Server Market Share
- Common Web App Threats
- Progression of the Professional Hacker
- Anatomy of a Web Application Attack
- A Generic Web Application System
- Query Strings
- URL Mappings to Web Application Systems
- Penetration Methodologies

- Paros Proxy
- Paros Proxy Demo
- Burp Proxy
- Dictionary Maker/ Cookies
- Acunetix Web Scanner
- Eclipse for Code Review
- OWASP WebScarab
- Samurai Web Testing

Pen. Testing Wired and Wireless Networks Course Session 1

Section A: Sniffers

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

Section B: ARP

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

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
- 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

- 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
- coWPATty
- Exploiting Cisco LEAP

Section H: Tools in Action

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

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

- 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

Penetration Vulnerabilities Uncovered Course 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 B: VA Tools and Results

- Nessus
- SAINT

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 F: Malware Countermeasures

- Countermeasure Tools

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

Section C: Vulnerability Assessments at Work

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

Section D: Malware and Its Many Uses

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

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

Section G: Malware in Pen. Testing

- Pivot an Attack
- Additional Netcat
Uses
- Banner Grabbing
- DCOM Exploit
- Uploading a File
- Testing the
Connection
- Transferring Files
via Netcat
- Verifying the
Transfer

Listener

- Netcat Demo