

# Certified Penetration Testing Engineer

## KEY DATA

**Course Title:** CPTEngineer

**Duration:** 5 days

**Language:** English

**Class Format Options:**

Instructor-led classroom  
Live Online Training  
CBT - Pre-recorded Videos

**Prerequisites:**

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

**Student Materials:**

- Student Workbook
- Student Lab Guide
- Software/Tools (3 DVDs)

**Certification Exam:**

CPTe – Certified Pen Testing Engineer™ (Thompson Prometric – Globally)

OSCP – Offensive Security Certified Professional

**Certification Track:**

CPTe - Certified Pen Testing Engineer™

CPTC - Certified Pen Testing Consultant™

CDFE - Certified Digital Forensics Examiner™

## COURSE BENEFITS

Certified Penetration Testing Engineer graduates will obtain real world security knowledge enabling them to recognize vulnerabilities, exploit system weaknesses, and safeguard organizations against threats. Graduates will learn the art of Ethical Hacking with a professional edge (Penetration Testing).

## COURSE OVERVIEW

CPTEngineer's foundation is built firmly upon proven, hands-on, Penetration Testing methodologies utilized by our international group of vulnerability consultants. Mile2 trainers keep abreast of their field by practicing what they teach. They believe that, during training, an equal emphasis should be placed on both theoretical and real world experience if the student is going to succeed in mastering the necessary skills to become a CPTEngineer..

The CPTEngineer presents information based on the 5 Key Elements of Pen Testing: Information Gathering, Scanning, Enumeration, Exploitation and Reporting. System vulnerabilities will be discovered using these tried and true steps alongside the use of the latest hacking techniques.

This course also enhances the business skills needed by today's students. It will enable them to identify protection opportunities, justify testing activities, and optimize security controls needed by businesses attempting to reduce risks.

mile2 goes far beyond simply teaching students to "Hack". Mere hacking was the norm for classes that were available before mile2's introduced a new methodology in teaching this advanced skill.



*Also available as:*

## LIVE VIRTUAL TRAINING

**Attend live classes from anywhere in the world!**

- Our Live Online classes make use of industry standard meeting and collaboration technologies. Students use simple web based tools to view slides, the instructors desktop, and videos all while holding live audio (and chat ) discussions with the instructor.
- During lab time, each remote student has a dedicated high spec remote PC. Students have full desktop access as if they were sitting in-front a PC in the actual computer lab.
- The instructor monitors each student's PC as they perform the labs remotely. The instructor can access the remote student's system to demonstrate and assist in the event questions arise.
- Public and private text chat allows for increased interactivity between students and instructor during class in a way that prevents interruptions to other students.



Our course was developed around principles and behaviors used by malicious hackers. The course is taught with this in mind while keeping the focus on professional penetration testing and ensuring the security of information assets.

### UPON COMPLETION

Upon proper completion of the course, CPTEngineer students will be able to confidently sit for the CPTEngineer certification exam (recommended). Students will enjoy an in-depth course that is continuously updated to maintain and incorporate changes in the security environment. This course offers up-to-date proprietary labs that have been researched and developed by leading security professionals from around the world.

### COURSE DETAILS

**Module 0: Course Overview**

**Module 1: Business and Technical Logistics of Pen Testing**

**Module 2: Financial Sector Regulations**

**Module 3: Information Gathering**

**Module 4: Detecting Live Systems**

**Module 5: Enumeration**

**Module 6: Vulnerability Assessments**

**Module 7: Malware, Trojans and BackDoors**

**Module 8: Windows Hacking**

**Module 9: Hacking UNIX/Linux**

**Module 10: Advanced Exploitation Techniques**

**Module 11: Pen Testing Wireless Networks**

**Module 12: Networks, Sniffing and IDS**

**Module 13: Injecting the Database**

**Module 14: Attacking Web Technologies**

**Module 15: Report Writing**

**Appendix 1: The Basics**

**Appendix 2: Linux Fundamentals**

**Appendix 3: Access Controls**

**Appendix 4: Protocols**

**Appendix 5: Cryptography**

**Appendix 6: Economics and Law**

### OBJECTIVE OF LABORATORY SCENARIOS

This is an intensive hands-on class. Students may spend 20 hours or more performing labs that walk them through a real world Pen Testing model. Labs begin with simple activities and move on to more complex procedures. During labs, students move through a detailed Lab Guide containing screen shots, commands to be typed, and steps students should take. Students will make use of scores of traditional and cutting edge Pen Testing tools (GUI and command line, Windows and Linux) as they make their way through mile2's time-tested methodology. (See Outline below for tool titles) Customers can be confident that as new methods arise in the security world, our labs are updated to reflect them.

## DETAILED COURSE OUTLINE

### Module 0 - Course Overview

- 0.1 Introduction
- 0.2 Courseware Materials
- 0.3 Course Overview – Appendix Items
- 0.4 Course Overview
- 0.5 Course Objectives
- 0.6 Exam Information
- 0.7 Learning Aids
- 0.8 Labs
- 0.9 Class Prerequisites
- 0.10 Student Facilities
- 0.11 Explanation Concerning Documentation

### Module 1 – Business and Technical Logistics of Pen Testing

- 1.1 Overview
- 1.2 What is a Penetration Test?
- 1.3 Benefits of a Penetration Test
- 1.4 Data Breach Insurance
- 1.5 CSI Computer Crime Survey
- 1.6 Hacking Examples and Associated Costs
- 1.7 Statistics on Internal Breaches
- 1.8 Stat
- 1.9 Trend at the End of 2008
- 1.10 The Evolving Threat
- 1.11 Security Vulnerability Life Cycle
- 1.12 Exploit Timeline
- 1.13 Zombies and Botnets
- 1.14 How are Botnet's Growing?
- 1.15 Types of Penetration Testing
- 1.16 "Hacking-Life-Cycle"
- 1.17 Penetration Testing Methodology
- 1.18 Other Penetration Testing Methodologies
- 1.19 Hacker vs. Penetration Tester
- 1.20 It is not always about the Tools!
- 1.21 Website Reviews
- 1.22 CIOview and SecurityNOW! SX
- 1.23 Seven Management Errors
- 1.24 What does the future hold?
- 1.25 Review
- 1.26 Lab 1 – Getting Set Up
  - 1.26.1 Exercise 1 – Discovering your class share
  - 1.26.2 Exercise 2 – Discovering your student DVD's
  - 1.26.3 Exercise 3 – VM Image Preparation
  - 1.26.4 Exercise 4 – Naming and Subnet Assignments
  - 1.26.5 Exercise 5 – PDF Penetration Testing
- Methodology Review

### Module 2 – Financial Sector Regulations

- 2.1 Overview
- 2.2 IT Governance Best Practices

- 2.3 IT Risk Management
- 2.4 Types of Risks
- 2.5 Approaches to Risk Management
- 2.6 Information Security Risk Evaluation
- 2.7 Improving Security Posture
- 2.8 Risk Evaluation Activities
- 2.9 Risk Assessment
- 2.10 Information Gathering
- 2.11 Data Classification
- 2.12 Threats and Vulnerabilities
- 2.13 Analytical Methods
- 2.14 Evaluate Controls
- 2.15 Risk Ratings
- 2.16 Important Risk Assessment Practices
- 2.17 Compliance
- 2.18 Many Regulations
- 2.19 Basel II
- 2.20 Gramm-Leach-Bliley Act 1999
- 2.21 Federal Financial Examination Institution Council
- 2.22 Sarbanes-Oxley Act (SOX 404) 2002
- 2.23 ISO 27002
- 2.24 PCI-DSS
- 2.25 Total Cost of Compliance
- 2.26 What does this mean to the tech?
- 2.27 Review
- 2.28 Lab 2 – Linux Fundamentals
  - 2.28.1 Exercise 1 – ifconfig
  - 2.28.2 Exercise 2 – Mounting a USB Thumb Drive
  - 2.28.3 Exercise 3 – Mount a Windows Partition
  - 2.28.4 Exercise 4 – VNC Server
  - 2.28.5 Exercise 5 – Preinstalled Tools in BackTrack3

### Module 3 – Information Gathering

- 3.1 Overview
- 3.2 What information does the Hacker want?
- 3.3 Methods of Obtaining Information
- 3.4 Physical Access
- 3.5 Social Engineering
- 3.6 Social Engineering via MySpa
- 3.7 Social Engineering via Facebook
- 3.8 Other Social Networks from around the world!
- 3.9 Identity Theft and MySpace
- 3.10 Instant Messengers and Chats
- 3.11 Digital Access
- 3.12 Passive vs Active Reconnaissance
- 3.13 Footprinting Defined
- 3.14 KartOO
- 3.15 Maltego
- 3.16 Firecat – Firefox Catalog of Auditing Extensions
- 3.17 Footprinting Tools
- 3.18 Johnny.ihackstuff.com

- 3.19 Google Hacking
- 3.20 SPUD
- 3.21 Wikto for Google Hacking
- 3.22 Blogs, Forums and Newsgroups
- 3.23 The Wayback Machine
- 3.24 Domain Name Registration
- 3.25 WHOIS
- 3.26 Dirx-loss – Online Tools
- 3.27 Dnsstuff
- 3.28 Central Ops
- 3.29 DNS Database Record Types
- 3.30 Nslookup
- 3.31 Dig
- 3.32 Traceroute
- 3.33 VisualRoute
- 3.34 Opus One Traceroute Tools
- 3.35 People Search Engines
- 3.36 EDGAR
- 3.37 Company House
- 3.38 Reputation Authority
- 3.39 Intelius – Background Check
- 3.40 Netcraft
- 3.41 Countermeasures
- 3.42 Review
- 3.43 Lab 3 – Information Gathering
  - 3.43.1 Exercise 1 – Google Queries
  - 3.43.2 Exercise 2 – Footprinting Tools
  - 3.43.3 Exercise 3 – Getting Everything You Need with Maltego
  - 3.43.4 Exercise 4 – Preparing Fi
  - 3.43.5 Exercise 5 – Turn in your Documentation

#### Module 4 – Detecting Live Systems

- 4.1 Overview
- 4.2 Introduction to Port Scanning
- 4.3 Port Scan Tips
- 4.4 Expected Results
- 4.5 Organizing the Results
- 4.6 Leo Meta-Text Editor
- 4.7 Free Mind
- 4.8 IHMC CmapTools
- 4.9 Popular Port Scanning Tools
- 4.10 Online Ping
- 4.11 NMAP - Ping
- 4.12 ICMP Disabled?
- 4.13 NMAP TCP Connect Scan
- 4.14 TCP Connect Port Scan
- 4.15 NMAP Half-Open Scan
- 4.16 Half-Open Scan
- 4.17 Firewalled Ports
- 4.18 Iron Geek – Hacking Illustrated
- 4.19 NMAP Service Version Detection
- 4.20 Addition NMAP Scans

- 4.21 Saving NMAP Results
- 4.22 NMAP UDP Scans
- 4.23 UDP Port Scan
- 4.24 NMAP Idle Scan
- 4.25 Superscan
- 4.26 Look@LAN
- 4.27 Unicornscan
- 4.28 Hping2
- 4.29 AutoScan
- 4.30 Xprobe2
- 4.31 What is Fuzzy Logic?
- 4.32 P0f
- 4.33 AMAP
- 4.34 Fragrouter
- 4.35 Countermeasures
- 4.36 Review
- 4.37 Lab 4 – Scanning
  - 4.37.1 Exercise 1 – Leo
  - 4.37.2 Exercise 2 – Look@LAN
  - 4.37.3 Exercise 3 – Zenmap
  - 4.37.4 Exercise 4 – Zenmap in BT3
  - 4.37.5 Exercise 5 – NMAP Command Line
  - 4.37.6 Exercise 6 – Hping2
  - 4.37.7 Exercise 7 – Unicornscan
  - 4.37.8 Exercise 8 – Turn in your

#### Module 5 - Enumeration

- 5.1 Overview
- 5.2 Banner Grabbing with Telnet
- 5.3 Banner Grabbing with Sup
- 5.4 HTTPPrint
- 5.5 SMTP Server Banner Grabbing
- 5.6 DNS Enumeration
- 5.7 Zone Transfers
- 5.8 Backtrack DNS Enumeration
- 5.9 Countermeasure: DNS Zone Transfer
- 5.10 SNMP Insecurity
- 5.11 SNMP Enumeration Tools
- 5.12 SNMP Countermeasures
- 5.13 Active Directory Enumeration
- 5.14 LDAPMiner
- 5.15 Active Directory Countermeasures
- 5.16 Null Sessions
- 5.17 Syntax for Null Sessions
- 5.18 Viewing Shares
- 5.19 Null Session Tools
- 5.20 Cain and Abel
- 5.21 NAT Dictionary Attack Tool
- 5.22 THC-Hydra
- 5.23 Injecting the Abel Service
- 5.24 Null Session Countermeasures
- 5.25 Tools Summary
- 5.26 Review

- 5.27 Lab 5 – Enumeration
- 5.27.1 Exercise 1 – Banner Grabbi
- 5.27.2 Exercise 2 – Zone Transfers
- 5.27.3 Exercise 3 – SNMP Enumeration
- 5.27.4 Exercise 4 – LDAP Enumeration
- 5.27.5 Exercise 5 – Null Sessions
- 5.27.6 Exercise 6 – SMB Enumeration
- 5.27.7 Exercise 7 – SMTP Enumeration
- 5.27.8 Exercise 8 – Maltego
- 5.27.9 Exercise 9 – Turn in Your Documentation

### Module 6 – Vulnerability Assessments

- 6.1 Overview
- 6.2 Vulnerabilities in Net
- 6.3 Vulnerabilities in Networks
- 6.4 Vulnerability Assessment Introduction
- 6.5 Testing Overview
- 6.6 Staying Abreast: Security Alerts
- 6.7 Vulnerability Scanners
- 6.8 Nessus
- 6.9 Saint
- 6.10 Retina
- 6.11 Qualys Guard
- 6.12 GFI LANguard
- 6.13 Scanner Comparison
- 6.14 Microsoft Baseline Analyzer
- 6.15 Dealing with the Results
- 6.16 Patch Management
- 6.17 Shavlik HFNetChkPro
- 6.18 Patching with GFI LANguard
- 6.19 Review
- 6.20 Lab 6 – Vulnerability Assessment
- 6.20.1 Exercise 1 – Running Nessus in Windows
- 6.20.2 Exercise 2 – Running Saint in Linux
- 6.20.3 Exercise 3 – Turn in your Documentation

### Module 7 – Malware, Trojans and BackDoors

- 7.1 Overview
- 7.2 Distributing Malware
- 7.3 Malware Capabilities
- 7.4 Auto-Starting Malware
- 7.5 Countermeasure to Auto
- 7.6 Netcat
- 7.7 Netcat Commands
- 7.8 Executable Wrappers
- 7.9 Historically Wrapped Trojans
- 7.10 Restorator
- 7.11 EXE Icon
- 7.12 Infectious CD-ROM Technique
- 7.13 Trojan Examples
- 7.14 Avoiding Detection
- 7.15 BPMTK
- 7.16 Malware Countermeasures

- 7.17 Gargoyle Investigator
- 7.18 Spy Sweeper Enterprise
- 7.19 Port Monitoring Software
- 7.20 File Protection Software
- 7.21 Windows File Protection
- 7.22 Windows Software Restriction Policies
- 7.23 Company Surveillance Software
- 7.24 Hardware-Based Malware Detectors
- 7.25 Countermeasure –
- 7.26 Review
- 7.27 Lab 7 – Malware –
- 7.27.1 Exercise 1 – Netcat and its uses
- 7.27.2 Exercise 2 – Exploiting and Pivoting our Attack
- 7.27.3 Exercise 3 – Creating a Trojan
- 7.27.4 Exercise 4 – Turn in your Documentation

### Module 8 – Windows Hacking

- 8.1 Overview
- 8.2 Types of Password Attacks
- 8.3 Keystroke Loggers
- 8.4 Password Guessing
- 8.5 Password Cracking
- 8.6 LM Hash Encryption
- 8.7 NT Hash Encryption
- 8.8 Syskey
- 8.9 Cracking Techniques
- 8.10 Rainbow Tables
- 8.11 Creating Rainbow Tables
- 8.12 Free Rainbow Tables
- 8.13 Hash Insertion Attack
- 8.14 Password Sniffing
- 8.15 Windows Authentication Protocols
- 8.16 Breaking Kerberos
- 8.17 Monitoring Logs
- 8.18 Hard Disk Security
- 8.19 Breaking Hard Disk Encryption
- 8.20 Tokens and Smart Cards
- 8.21 Covering your Tracks
- 8.22 Disabling Auditing
- 8.23 Clearing the Event Log
- 8.24 Alternate Data Streams
- 8.25 ADS Countermeasures
- 8.26 Stream Explorer
- 8.27 Steganography
- 8.28 Steganography Tools
- 8.29 Shredding Files Left Behind
- 8.30 Leaving No Local Trace
- 8.31 Anonymizers
- 8.32 StealthSurfer II Privacy Stick
- 8.33 TOR
- 8.34 Janus VM
- 8.35 Encrypted Tunnel Notes
- 8.36 Rootkits

- 8.37 Windows Rootkit Countermeasures
- 8.38 Review
- 8.39 Lab 8 – Hacking Windows
- 8.39.1 Exercise 1 – Cracking a Windows Password with Linux
- 8.39.2 Exercise 2 – Cracking a Windows Password with Cain and Abel
- 8.39.3 Exercise 3 – Covering your tracks
- 8.39.4 Exercise 4 – Alternate Data Streams
- 8.39.5 Exercise 5 – Steganography
- 8.39.6 Exercise 6 – Understanding Rootkits
- 8.39.7 Exercise 7 – Turn in your Documentation

### Module 9 – Hacking UNIX/Linux

- 9.1 Overview
- 9.2 Introduction
- 9.3 Linux Introduction
- 9.4 File System Structure
- 9.5 Kernel
- 9.6 Processes
- 9.7 Starting and Stopping Processes
- 9.8 Interacting with Processes
- 9.9 Accounts and Groups
- 9.10 Password and Shadow File Formats
- 9.11 More on Accounts and Groups
- 9.12 Linux and UNIX Permissions
- 9.13 Set UID Programs
- 9.14 Trust Relationships
- 9.15 Logs and Auditing
- 9.16 Common Network Services
- 9.17 Remote Access Attacks
- 9.18 Brute-Force Attacks
- 9.19 Brute-Force Countermeasures
- 9.20 X Window System
- 9.21 X Insecurities Countermeasures
- 9.22 Network File System
- 9.23 NFS in Action
- 9.24 NFS Countermeasure
- 9.25 Passwords and Encryption
- 9.26 Password Cracking Tools
- 9.27 Salting
- 9.28 Symbolic Link
- 9.29 Symlink Countermeasure
- 9.30 Core File Manipulation
- 9.31 Shared Libraries
- 9.32 Kernel Flaws
- 9.33 File and Directory Permissions
- 9.34 SUID Files Countermeasure
- 9.35 File and Directory Permissions
- 9.36 World-Writable Files Countermeasure
- 9.37 Clearing the Log Files
- 9.38 Rootkits – User and Kernel
- 9.39 Rootkit Countermeasure

- 9.40 Review
- 9.41 Lab 10 – Hacking UNIX/Linux
- 9.41.1 Exercise 1 – Setup and Recon
- 9.41.2 Exercise 2 – Making use of a poorly configured service.
- 9.41.3 Exercise 3 – Cracking a Linux Password
- 9.41.4 Exercise 4 – Creating a simple backdoor and covering your tracks.
- 9.41.5 Exercise 5 – Turn in your Documentation

### Module 10 – Advanced Exploitation Techniques

- 10.1 Overview
- 10.2 How Do Exploits Work?
- 10.3 Format String
- 10.4 Race Conditions
- 10.5 Memory Organization
- 10.6 Buffer Overflows
- 10.7 Buffer Overflow Illustration
- 10.8 How Stacks Work
- 10.9 Stack Function Illustrated
- 10.10 Buffer Overflow Illustration #2
- 10.11 Heap Overflows
- 10.12 Heap Spraying
- 10.13 Prevention
- 10.14 Secure Code Reviews
- 10.15 Review Process
- 10.16 Know the Vulnerabilities
- 10.17 Know the Business Risks
- 10.18 When to Conduct the Review
- 10.19 Who should be Involved
- 10.20 What to Look For
- 10.21 Fixing the Issues
- 10.22 Automated Tools
- 10.23 Stages of Exploit Development
- 10.24 Shellcode Development
- 10.25 Metasploit
- 10.26 Metasploit - Mete
- 10.27 Fuzzers
- 10.28 SaintExploit
- 10.29 Core Impact
- 10.30 Tools Comparison
- 10.31 Review
- 10.32 Lab 10 – Advanced Exploitation Techniques
- 10.32.1 Exercise 1 – Metasploit Command Line
- 10.32.2 Exercise 2 – Metasploit Web Interface
- 10.32.3 Exercise 3 – Milw0rm
- 10.32.4 Exercise 4 – SaintExploit
- 10.32.5 Exercise 5 – Core Impact
- 10.32.6 Exercise 6 – Turn in your Documentation

### Module 11 – Pen Testing Wireless Networks

- 11.1 Overview
- 11.2 Standards Comparison

- 11.3 SSID
- 11.4 MAC Filtering
- 11.5 WEP
- 11.6 Weak IV Packets
- 11.7 XOR Basics
- 11.8 WEP Weaknesses
- 11.9 How WPA Improves on WEP
- 11.10 TKIP
- 11.11 The WPA MIC Vulnerability
- 11.12 WPA2
- 11.13 WPA and WPA2 Modes
- 11.14 WPA-PSK Encryption
- 11.15 LEAP
- 11.16 LEAP Weaknesses
- 11.17 NetStumbler
- 11.18 KNSGEM
- 11.19 Vistumbler
- 11.20 Kismet
- 11.21 OmniPeek Personal
- 11.22 Aircrack-ng Suite
- 11.23 Airodump-ng
- 11.24 Aireplay-ng
- 11.25 DoS Attack
- 11.26 Aircrack-ng
- 11.27 Aircrack for Windows
- 11.28 Attacking WEP
- 11.29 Attacking WPA
- 11.30 coWPAtty
- 11.31 Exploiting Cisco LEAP
- 11.32 asleep
- 11.33 WiFiZoo
- 11.34 Wesside-ng
- 11.35 www.wirelessdefence.org
- 11.36 Typical Network Blueprint
- 11.37 EAP Types
- 11.38 EAP Advantages/Disadvantages
- 11.39 EAP/TLS Deployment
- 11.40 Aruba Products
- 11.41 Airwave – RAPIDS Rogue Detection Module
- 11.42 Review
- 11.43 Lab 11 – Pen Testing Wireless Networks
  - 11.43.1 Exercise 1 – War Driving
  - 11.43.2 Exercise 2 – WEP Cracking
  - 11.43.3 Exercise 3 – Turn in your Documentation

### **Module 12 – Networks, Sniffing and IDS**

- 12.1 Overview
- 12.2 Packet Sniffers
- 12.3 Pcap and WinPcap
- 12.4 Wireshark
- 12.5 TCP Stream Re-assembling
- 12.6 Packetizer
- 12.7 tcpdump and windump

- 12.8 Omnippeek
- 12.9 Cain and Abel
- 12.10 Active Sniffing Methods
- 12.11 Switch Table Flooding
- 12.12 ARP Cache Poisoning
- 12.13 ARP Normal Operation
- 12.14 ARP Cache Poisoning in Action
- 12.15 ARP Cache Poisoning with Linux
- 12.16 Countermeasures
- 12.17 Using Cain and Abel for ARP Cache Poisoning
- 12.18 Ettercap
- 12.19 Dsniff Suite
- 12.20 Dsniff in Action
- 12.21 MailSnarf, MsgSnarf and FileSnarf
- 12.22 What is DNS Spoofing?
- 12.23 DNS Spoofing
- 12.24 Session Hijacking
- 12.25 Breaking SSL
- 12.26 Capturing VoIP
- 12.27 Intercepting VoIP
- 12.28 Intercepting RDP
- 12.29 Routing Protocols Analysis
- 12.30 Countermeasures for Sniffing
- 12.31 Evading the Firewall and IDS
- 12.32 Fragmentation
- 12.33 Evading with Encryption
- 12.34 Newer Firewall Capabilities
- 12.35 New Age Protection
- 12.36 Bastion Host
- 12.37 Spyware Prevention System
- 12.38 Intrusion ‘SecureHost’ Overview
- 12.39 IPS Overview
- 12.40 Review
- 12.41 Lab 12 – Networks, Sniffing and IDS
  - 12.41.1 Exercise 1 – Capture FTP Traffic
  - 12.41.2 Exercise 2 – ARP Cache Poisoning Basics
  - 12.41.3 Exercise 3 – ARP Cache Poisoning
  - 12.41.4 Exercise 4 – Turn in your Documentation

### **Module 13 – Injecting the Database**

- 13.1 Overview
- 13.2 Vulnerabilities and Common Attacks
- 13.3 SQL Injection
- 13.4 Business Impacts of SQL Injection
- 13.5 Why SQL Injection?
- 13.6 Database Enumeration
- 13.7 Extended Stored Proc
- 13.8 Direct Attacks
- 13.9 SQL Connection Properties
- 13.10 Default Ports
- 13.11 Obtaining Sensitive Info
- 13.12 SQL Ping2
- 13.13 osql.exe

- 13.14 Query Analyzers
- 13.15 SQLExec
- 13.16 www.petefinnegan.com
- 13.17 Metasploit
- 13.18 Finding and Fixing SQL Injection
- 13.19 Hardening Databases
- 13.20 Review
- 13.21 Lab 13 – Attacking the Database
  - 13.21.1 Exercise 1 – Login Bypass
  - 13.21.2 Exercise 2 – Verbose Table Modific
  - 13.21.3 Exercise 3 – Denial of Service
  - 13.21.4 Exercise 4 – Data Tampering
  - 13.21.5 Exercise 5 – Turn in your Documentation

#### Module 14 – Attacking Web Technologies

- 14.1 Overview
- 14.2 Web Server Market Share
- 14.3 OWASP Top 10
- 14.4 Progression of the Professional Hacker
- 14.5 The Anatomy of a Web Application Attack
- 14.6 Components of a Web Application System
- 14.7 Query String
- 14.8 URL Mappings
- 14.9 Information Gathering
- 14.10 Changing URL Login Parameters
- 14.11 URL Login - Horizontal Attack
- 14.12 URL Login – Vertical Escalation
- 14.13 Cross-Site Scripting
- 14.14 Stored XSS Illustrated
- 14.15 Reflected XSS Illustrated
- 14.16 Business Impacts of XSS
- 14.17 Finding and Fixing XSS
- 14.18 Injection Flaws
- 14.19 Unvalidated Input
- 14.20 Unvalidated Input Illustrated
- 14.21 Business Impacts of Unvalidated Input
- 14.22 Finding and Fixing Unvalidated Input
- 14.23 Attacks against IIS
- 14.24 IIS Directory Traversal
- 14.25 Unicode
- 14.26 IIS Logs
- 14.27 N-Stalker
- 14.28 NTO Spider
- 14.29 HTTrack Website Copier
- 14.30 Wikto
- 14.31 Burp Proxy
- 14.32 Brutus
- 14.33 Dictionary Maker
- 14.34 Cookies
- 14.35 Acunetix Web Scanner
- 14.36 Eclipse for Code Review
- 14.37 WebScarab
- 14.38 Samurai

- 14.39 OWASP Web Application Penetration Checklist
- 14.40 Review
- 14.41 Lab 14 – Attacking Web Technologies
  - 14.41.1 Exercise 1 – Input Manipulation
  - 14.41.2 Exercise 2 – Shovelling a Shell
  - 14.41.3 Exercise 3 – Horizontal Privilege Escalation
  - 14.41.4 Exercise 4 – Vertical Privilege Escalation
  - 14.41.5 Exercise 5 – Cross Site Scripting
  - 14.41.6 Exercise 6 – Turn in your Documentation

#### Module 15 – Report Writing

- 15.1 Overview
- 15.2 Additional Items to Consider
- 15.3 The Report
- 15.4 Support Documentation
- 15.5 Analyzing Risk
- 15.6 Report Results Matrix
- 15.7 Findings Matrix Examples
- 15.8 Delivering the Report
- 15.9 Stating the Fact
- 15.10 Recommendations
- 15.11 Executive Summary
- 15.12 Technical Report
- 15.13 Table of Contents
- 15.14 Summary of Weaknesses Identified
- 15.15 Scope of Testing
- 15.16 Summary of Recommendations
- 15.17 Summary Observations
- 15.18 Detailed Findings
- 15.19 Strategic and Tactical Directives
- 15.20 Statement of Responsibility
- 15.21 Appendices
- 15.22 Review

#### Appendix 1 – The Basics

- 16.1 Overview
- 16.2 The Growth of Environments and Security
- 16.3 Our Motivation
- 16.4 The Goal
- 16.5 CIA Triad in Detail
- 16.6 Holistic Security
- 16.7 Security Definitions
- 16.8 Definitions Relationships
- 16.9 TCP/IP Basics
  - 16.9.1 Ping
  - 16.9.2 TCP/IP Stack
  - 16.9.3 TCP/IP for Security Administrators
  - 16.9.4 Ports and Services
  - 16.9.5 TCP 3-Way Handshake
  - 16.9.6 TCP Flags
- 16.10 Malware
  - 16.10.1 Types of Malware
  - 16.10.2 Types of Viruses

- 16.10.3 Spyware
- 16.10.4 Trojan Horse
- 16.10.5 Back Doors
- 16.11 Denial of Service
- 16.11.1 DDoS Issues
- 16.12 Network Devices and Sniffers
- 16.12.1 Packet Sniffers
- 16.12.2 Passive Sniffing
- 16.12.3 Active Sniffing
- 16.13 Firewalls, IDS and IPS
- 16.13.1 Firewall
- 16.13.2 IDS
- 16.13.3 IPS
- 16.13.4 Firewall Types
- 16.13.5 Packet Filterin
- 16.13.6 Proxy Firewalls
- 16.13.7 Circuit-Level Proxy Firewall
- 16.13.8 SOCKS
- 16.13.9 Application-Layer Proxy
- 16.13.10 Stateful
- 16.13.11 Dynamic Packet
- 16.13.12 Kernel Proxies
- 16.13.13 Firewall Placement
- 16.13.14 Screened Host
- 16.13.15 Multi- or Dual
- 16.13.16 Screened Subnet
- 16.14 Wireless Standards
- 16.14.1 WiFi Network Types
- 16.14.2 Widely Deployed Standards
- 16.14.3 Standards Comparison
- 16.14.4 802.11n – MIMO
- 16.15 Database Basics
- 16.15.1 Overview of Database Server
- 16.15.2 Types of Databases
- 16.15.3 Components of the
- 16.16 Review

## Appendix 2 – Linux Fundamentals

- 17.1 Overview
- 17.2 Linux History
- 17.3 The GNU Operating System
- 17.4 Linux Introduction
- 17.5 Linux GUI Desktops
- 17.6 Linux Shell
- 17.7 Linux Bash Shell
- 17.8 Books on Linux
- 17.9 Password and Shadow File Formats
- 17.10 User Account Management
- 17.11 Changing your Password
- 17.12 Configuring your Network Interface
- 17.13 Mounting Drives
- 17.14 Tarballs and Zips
- 17.15 Compiling Programs

- 17.16 Typical Linux Operating Systems
- 17.17 Gentoo
- 17.18 VLOS
- 17.19 Why use Linux Boot CD's?
- 17.20 FrozenTech's Complete Distro List
- 17.21 Backtrack
- 17.22 Review

## Appendix 3 – Access Controls

- 18.1 Overview
- 18.2 Role of Access Control
- 18.3 Definitions
- 18.4 Categories of Access Controls
- 18.5 Physical Controls
- 18.6 Logical Controls
- 18.7 "Soft" Controls
- 18.8 Security Roles
- 18.9 Steps to Granting Access
- 18.10 Access Criteria
- 18.11 Physical Access Control Mechanisms
- 18.12 Biometric System Types
- 18.13 Synchronous Token
- 18.14 Asynchronous Token
- 18.15 Memory Cards
- 18.16 Smart Cards
- 18.17 Cryptographic Keys
- 18.18 Logical Access Controls
- 18.19 OS Access Controls
- 18.20 Review

## Appendix 4 – Protocols

- 19.1 Overview
- 19.2 OSI – Application Layer
- 19.3 OSI – Presentation Layer
- 19.4 OSI – Session Layer
- 19.5 OSI – Transport Layer
- 19.6 OSI – Network Layer
- 19.7 OSI – Data Link
- 19.8 OSI – Physical Layer
- 19.9 Protocols at Each OSI Model Layer
- 19.10 TCP/IP Suite
- 19.11 Port and Protocol Relationship
- 19.12 Conceptual Use of Ports
- 19.13 UDP vs TCP
- 19.14 ARP
- 19.15 ICMP
- 19.16 DNS
- 19.17 SSH
- 19.18 SNMP
- 19.19 SMTP
- 19.20 Review

## Appendix 5 – Cryptography

- 20.1 Overview
- 20.2 Introduction
- 20.3 Encryption
- 20.4 Cryptographic Definitions
- 20.5 The Science of Secret Communications
- 20.6 Encryption Algorithm
- 20.7 Implementation
- 20.8 Symmetric Encryption
- 20.9 Symmetric Downfalls
- 20.10 Symmetric Algorithms
- 20.11 Crack Times
- 20.12 Asymmetric Encryption
- 20.13 Asymmetric Advantages
- 20.14 Asymmetric Disadvantages
- 20.15 Asymmetric Algorithms
- 20.16 Key Exchange
- 20.17 Symmetric vs Asymmetric
- 20.18 Hybrid Encryption
- 20.19 Hashing
- 20.20 Common Hash Algorithms
- 20.21 Birthday Attack
- 20.22 Hash Demo
- 20.23 Security Issues in Hashing
- 20.24 Hash Collisions
- 20.25 MD5 Collision Creates Rogue Certificate Authority
- 20.26 More Hybrid Encryption
- 20.27 Digital Signatures
- 20.28 SSL/TLS
- 20.29 SSL Connection Setup
- 20.30 SSL Hybrid Encryption
- 20.31 SSH
- 20.32 IPSec
- 20.33 PKI
- 20.34 Quantum Cryptography
- 20.35 Attack Vectors
- 20.36 Network Attacks
- 20.37 More Attacks
- 20.38 Review
- 20.39 A5 Lab – Cryptography
  - 20.39.1 Exercise 1 – Caesar Encryption
  - 20.39.2 Exercise 2 – RC4 Encryption
  - 20.39.3 Exercise 3 – IPSec Deployment

**Appendix 6 – Economics and Law**

- 21.1 Overview
- 21.2 Security Incentives and Motives
- 21.3 What is Your Weakest Link?
- 21.4 What is the Value of an Asset?
- 21.5 Non-Obvious Vulnerabilities
- 21.6 Categorizing Risks
- 21.7 Types of Losses
- 21.8 Approaches to Analyzing Risk

- 21.9 Who Uses What Analysis Type?
- 21.10 Qualitative Analysis Method
- 21.11 Quantitative Analysis
- 21.12 Can a Purely Quantitative Method be accomplished?
- 21.13 Comparing Cost and Benefit
- 21.14 Cost of a Countermeasure
- 21.15 CyberCrime
- 21.16 Not Just Fun and Games
- 21.17 Example of Computer Crimes
- 21.18 Perpetrators
- 21.19 Attack Types
- 21.20 Telephone Fraud
- 21.21 Identification Protection and Prosecution
- 21.22 Privacy of Sensitive Data
- 21.23 Privacy Issues – US Laws and Examples
- 21.24 EU Principles on Privacy
- 21.25 Transborder Information Flow
- 21.26 Employee Privacy Issues
- 21.27 U.S. Law
- 21.28 Common Laws – Civil
- 21.29 Common Laws – Criminal
- 21.30 Common Laws – Administrative
- 21.31 U.S. Federal Laws
- 21.32 Intellectual Property Laws
- 21.33 Trademark and Patent
- 21.34 Software Licensing
- 21.35 Digital Millennium Copyright Act
- 21.36 Investigating
- 21.37 Computer Crime and its Barriers
- 21.38 Countries Working Together
- 21.39 Security Principles for International Use
- 21.40 Has a Crime Been Committed?
- 21.41 Bringing in Law Enforcement
- 21.42 Citizen vs Law Enforcement Investigation
- 21.43 Investigation of Any Crime
- 21.44 Role of Evidence in a Trial
- 21.45 Evidence Requirements
- 21.46 Chain of Custody
- 21.47 How Evidence is Processed
- 21.48 Evidence Types
- 21.49 Hearsay Rule Exception
- 21.50 Responding to an Incident
- 21.51 Preparing for a Crime before it happens!
- 21.52 Incident Handling
- 21.53 Evidence Collection Topics
- 21.54 Specialized Skill
- 21.55 Trying to Trap the Bad Guy
- 21.56 Companies Can be Found Liable!
- 21.57 Review