Certified Penetration Testing Engineer (CPTE)

This course is designed to take an individual with knowledge of the basic security auditing toolset to the next and higher level. Many courses teach "how to hack"; the CPTC course teaches "the business of penetration testing". The course delivers advanced and cutting edge techniques for auditing a broad range of security controls (including Physical and User Security) with "hands-on" laboratories designed by real world security auditors. The CPTC course also delivers the "business side" of penetration testing, including RFPs, Authorization, Security Policy Review, and Compliance & Documentation skills required.

The CPTC courseware is constantly updated (with updates available to past students) to reflect the most current security issues and known exploits; this is the way of the Certified Penetration Testing Consultant.

Each day ends with a Capture the Flag Competition to ensure that participants retain the daily objectives.

Course Number: CPTEngineer (Formerly CPTS)
Duration: 120 hours
Data structure
Languages: English
Format: Instructor-led Live Virtual Training CBT - Pre-recorded
Prerequisites:

- A minimum of 12 months experience in networking technologies
- A minimum of 24 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:

1. Student Workbook
2. Student Reference Manual
3. Software/Tools, 3xDVD(s)

Certification Exam: CPTENGINEER Certified Pen Testing Engineer (Thompson Prometric Globally)
CEH   Certified Ethical Hacker
OSCP   Offensive Security Certified Professional

WEBCOM Technologies
South Extension: C-23, South Ext. - I, New Delhi – 110049, 011-24611138/39
Pitam Pura: C-574, Saraswati Vihar, Pitam Pura, New Delhi, 9250928432
Connaught Place: K-59, Opp. PVR Plaza, 9250928433

Certification Track: CPTE - Certified Pen Testing Engineer^{TM}

CPTC - Certified Pen Testing Consultant^{TM}

CDFE - Certified Digital Forensics Examiner^{TM}

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.

BENEFITS OF THIS COURSE

Certified Penetration Testing Engineer graduates would have obtained real world security knowledge that will enable them to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats. Graduates will learn the art of Ethical Hacking, but with a professional edge (Penetration Testing).

COURSE OVERVIEW

CCPTEngineer'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.

WEBCOM Technologies

South Extension: C-23, South Ext. - I, New Delhi – 110049, 011-24611138/39

Pitam Pura: C-574, Saraswati Vihar, Pitam Pura, New Delhi, 9250928432

Connaught Place: K-59, Opp. PVR Plaza, 9250928433

WEBCOM
(A 12 year old / ISO 9000-2001 Company)

With the Association of

CYBER
INTELLIGENT | CIS
SECURITY

Certification by

mile2
Information Assurance Training

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

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

MODULES

- **MODULE 0: Course Overview**
- **MODULE 1: Business and Technical Logistics of Penetration 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**

MODULE 0: Course Overview

- Introduction
- Courseware Materials
- Course Overview Appendix Items
- Course Overview
- Course Objectives
- Exam Information
- Learning Aids
- Labs
- Class Prerequisites
- Student Facilities
- Explanation Concerning Documentation

MODULE 1: Business and Technical Logistics of Penetration Testing

- Overview
- What is a Penetration Test?
- Benefits of a Penetration Test
- Data Breach Insurance
- CSI Computer Crime Survey
- Hacking Examples and Associated Costs
- Statistics on Internal Breaches
- Stat
- Trend at the End of 2008
- The Evolving Threat
- Security Vulnerability Life Cycle
- Exploit Timeline
- Zombies and Botnets
- How are Botnet's Growing?
- Types of Penetration Testing
- Hacking-Life-Cycle
- Penetration Testing Methodology
- Other Penetration Testing Methodologies
- Hacker vs. Penetration Tester
- It is not always about the Tools!
- Website Reviews
- CIOview and SecurityNOW! SX
- Seven Management Errors
- What does the future hold?
- Review
- Lab 1 Getting Set Up

Exercise 1 Discovering your class share

Exercise 2 Discovering your student DVD's

Exercise 3 VM Image Preparations

Exercise 4   Naming and Subnet Assignments

Exercise 5 PDF Penetration Testing Methodology Review

MODULE 2: Financial Sector Regulations

* Overview
* IT Governance Best Practices
* IT Risk Management
* Types of Risks
* Approaches to Risk Management
* Information Security Risk Evaluation
* Improving Security Posture
* Risk Evaluation Activities
* Risk Assessment
* Information Gathering
* Data Classification
* Threats and Vulnerabilities
* Analytical Methods
* Evaluate Controls
* Risk Ratings
* Important Risk Assessment Practices
* Compliance
* Many Regulations
* Basel II
* Gramm-Leach-Bliley Act 1999
* Federal Financial Examination Institution Council
* Sarbanes-Oxley Act (SOX 404) 2002
* ISO 27002
* PCI-DSS
* Total Cost of Compliance
* What does this mean to the tech?
* Review
* Lab 2 Linux Fundamentals

Exercise 1 ifconfig

Exercise 2 Mounting a USB Thumb Drive

Exercise 3 Mount a Windows Partition

Exercise 4 VNC Server

Exercise 5 Preinstalled Tools in BackTrack3

MODULE 3: Information Gathering

- Overview
- What information does the Hacker want?
- Methods of Obtaining Information
- Physical Access
- Social Engineering
- Social Engineering via MySpa
- Social Engineering via Facebook
- Other Social Networks from around the world!
- Identity Theft and MySpace
- Instant Messengers and Chats
- Digital Access
- Passive vs Active Reconnaissance
- Footprinting Defined
- KartOO
- Maltego
- Firecat Firefox Catalog of Auditing Extensions
- Footprinting Tools
- Johnny.ihackstuff.com
- Google Hacking
- SPUD
- Wikto for Google Hacking
- Blogs, Forums and Newsgroups
- The Wayback Machine
- Domain Name Registration
- WHOIS
- Dirk-loss Online Tools
- Dnsstuff
- Central Ops
- DNS Database Record Types
- Nslookup
- Dig
- Traceroute

WEBC☉M
(A 12 year old / ISO 9000-2001 Company)

With the Association of   Certification by

CYBER
INTELLIGENT | CIS
SECURITY

mile2
Information Assurance Training

- VisualRoute
- Opus One Traceroute Tools
- People Search Engines
- EDGAR
- Company House
- Reputation Authority
- Intelius Background Check
- Netcraft
- Countermeasures
- Review
- Lab 3 Information Gathering

  Exercise 1 Google Queries

  Exercise 2 Footprinting Tools

  Exercise 3 Getting Everything You Need with Maltego

  Exercise 4 Preparing Fi

  Exercise 5 Turn in your Documentation

MODULE 4: Detecting Live Systems

- Overview
- Introduction to Port Scanning
- Port Scan Tips
- Expected Results
- Organizing the Results
- Leo Meta-Text Editor
- Free Mind
- IHMC CmapTools
- Popular Port Scanning Tools
- Online Ping
- NMAP - Ping
- ICMP Disabled
- NMAP TCP Connect Scan
- TCP Connect Port Scan
- NMAP Half-Open Scan
- Half-Open Scan
- Firewalled Ports
- Iron Geek Hacking Illustrated
- NMAP Service Version Detection
- Addition NMAP Scans

WEBCOM
(A 12 year old / ISO 9000-2001 Company)

With the Association of

Certification by

CYBER
INTELLIGENT | CIS
SECURITY

mile2
Information Assurance Training

- Saving NMAP Results
- NMAP UDP Scans
- UDP Port Scan
- NMAP Idle Scan
- Superscan
- Look@LAN
- Unicornscan
- Hping2
- AutoScan
- Xprobe2
- What is Fuzzy Logic?
- P0f
- AMAP
- Fragrouter
- Countermeasures
- Review
- Lab 4 Scanning

> Exercise 1 Leo
>
> Exercise 2 Look@LAN
>
> Exercise 3 Zenmap
>
> Exercise 4 Zenmap in BT3
>
> Exercise 5 NMAP Command Line
>
> Exercise 6 Hping2
>
> Exercise 7 Unicornscan
>
> Exercise 8 Turn in your

MODULE 5: Enumeration

- Overview
- Banner Grabbing with Telnet
- Banner Grabbing with Sup
- HTTPrint
- SMTP Server Banner Grabbing
- DNS Enumeration
- Zone Transfers
- Backtrack DNS Enumeration

- Countermeasure: DNS Zone Transfer
- SNMP Insecurity
- SNMP Enumeration Tools
- SNMP Countermeasures
- Active Directory Enumeration
- LDAPMiner
- Active Directory Countermeasures
- Null Sessions
- Syntax for Null Sessions
- Viewing Shares
- Null Session Tools
- Cain and Abel
- NAT Dictionary Attack Tool
- THC-Hydra
- Injecting the Abel Service
- Null Session Countermeasures
- Tools Summary
- Review
- Lab 5 Enumeration

    Exercise 1 Banner Grabbi

    Exercise 2 Zone Transfers

    Exercise 3 SNMP Enumeration

    Exercise 4   LDAP Enumeration

    Exercise 5   Null Sessions

    Exercise 6   SMB Enumeration

    Exercise 7   SMTP Enumeration

    Exercise 8   Maltego

    Exercise 9   Turn in Your Documentation

MODULE 6:Vulnerability Assessments

- Overview
- Vulnerabilities in Net
- Vulnerabilities in Networks
- Vulnerability Assessment Introduction

WEBCOM Technologies
South Extension: C-23, South Ext. - I, New Delhi – 110049, 011-24611138/39
Pitam Pura: C-574, Saraswati Vihar, Pitam Pura, New Delhi, 9250928432
Connaught Place: K-59, Opp. PVR Plaza, 9250928433

- Testing Overview
- Staying Abreast: Security Alerts
- Vulnerability Scanners
- Nessus
- Saint
- Retina
- Qualys Guard
- GFI LANguard
- Scanner Comparison
- Microsoft Baseline Analyzer
- Dealing with the Results
- Patch Management
- Shavlik HFNetChkPro
- Patching with GFI LANguard
- Review
- Lab 6 Vulnerability Assessment

  Exercise 1 Running Nessus in Windows

  Exercise 2 Running Saint in Linux

  Exercise 3 Turn in your Documentation

MODULE 7:Malware, Trojans and BackDoors

- Overview
- Distributing Malware
- Malware Capabilities
- Auto-Starting Malware
- Countermeasure to Auto
- Netcat
- Netcat Commands
- Executable Wrappers
- Historically Wrapped Trojans
- Restorator
- EXE Icon
- Infectious CD-ROM Technique
- Trojan Examples
- Avoiding Detection
- BPMTK
- Malware Countermeasures
- Gargoyle Investigator
- Spy Sweeper Enterprise
- Port Monitoring Software

- File Protection Software
- Windows File Protection
- Windows Software Restriction Policies
- Company Surveillance Software
- Hardware-Based Malware Detectors
- Countermeasure
- Review
- Lab 7 Malware

Exercise 1 Netcat and its uses

Exercise 2 Exploiting and Pivoting our Attack

Exercise 3 Creating a Trojan

Exercise 4 Turn in your Documentation

MODULE 8:Windows Hacking

- Overview
- Types of Password Attacks
- Keystroke Loggers
- Password Guessing
- Password Cracking
- LM Hash Encryption
- NT Hash Encryption
- Syskey
- Cracking Techniques
- Rainbow Tables
- Creating Rainbow Tables
- Free Rainbow Tables
- Hash Insertion Attack
- Password Sniffing
- Windows Authentication Protocols
- Breaking Kerberos
- Monitoring Logs
- Hard Disk Security
- Breaking Hard Disk Encryption
- Tokens and Smart Cards
- Covering your Tracks
- Disabling Auditing
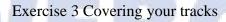- Clearing the Event Log
- Alternate Data Streams
- ADS Countermeasures

- Stream Explorer
- Steganography
- Steganography Tools
- Shredding Files Left Behind
- Leaving No Local Trace
- Anonymizers
- StealthSurfer II Privacy Stick
- TOR
- Janus VM
- Encrypted Tunnel Notes
- Rootkits
- Windows Rootkit Countermeasures
- Review
- Lab 8 Hacking Windows

> Exercise 1 Cracking a Windows Password with Linux

> Exercise 2 Cracking a Windows Password with Cain and Abel

> Exercise 3 Covering your tracks

> Exercise 4 Alternate Data Streams

> Exercise 5 Steganography

> Exercise 6 Understanding Rootkits

> Exercise 7 Turn in your Documentation

MODULE 9: Hacking UNIX/Linux

- Overview
- Introduction
- Linux Introduction
- File System Structure
- Kernel
- Processes
- Starting and Stopping Processes
- Interacting with Processes
- Accounts and Groups
- Password and Shadow File Formats
- More on Accounts and Groups
- Linux and UNIX Permissions
- Set UID Programs

- Trust Relationships
- Logs and Auditing
- Common Network Services
- Remote Access Attacks
- Brute-Force Attacks
- Brute-Force Countermeasures
- X Window System
- X Insecurities Countermeasures
- Network File System
- NFS in Action
- NFS Countermeasure
- Passwords and Encryption
- Password Cracking Tools
- Salting
- Symbolic Link
- Symlink Countermeasure
- Core File Manipulation
- Shared Libraries
- Kernel Flaws
- File and Directory Permissions
- SUID Files Countermeasure
- File and Directory Permissions
- World-Writable Files Countermeasure
- Clearing the Log Files
- Rootkits ? User and Kernel
- Rootkit Countermeasure
- 40 Review
- Lab 10 Hacking UNIX/Linux

    Exercise 1 Setup and Recon

    Exercise 2 Making use of a poorly configured service.

    Exercise 3 Cracking a Linux Password

    Exercise 4 Creating a simple backdoor and covering your tracks.

    Exercise 5 Turn in your Documentation

MODULE 10:Advanced Exploitation Techniques

- Overview
- How Do Exploits Work?
- Format String

WEBCOM Technologies
South Extension: C-23, South Ext. - I, New Delhi – 110049, 011-24611138/39
Pitam Pura: C-574, Saraswati Vihar, Pitam Pura, New Delhi, 9250928432
Connaught Place: K-59, Opp. PVR Plaza, 9250928433

- Race Conditions
- Memory Organization
- Buffer Overflows
- Buffer Overflow Illustration
- How Stacks Work
- Stack Function Illustrated
- Buffer Overflow Illustration #2
- Heap Overflows
- Heap Spraying
- Prevention
- Secure Code Reviews
- Review Process
- Know the Vulnerabilities
- Know the Business Risks
- When to Conduct the Review
- Who should be Involved
- What to Look For
- Fixing the Issues
- Automated Tools
- Stages of Exploit Development
- Shellcode Development
- Metasploit
- Metasploit - Mete
- Fuzzers
- SaintExploit
- Core Impact
- Tools Comparison
- Review
- Lab 10 ? Advanced Exploitation Techniques

       Exercise 1 Metasploit Command Line

       Exercise 2 Metasploit Web Interface

       Exercise 3 Milw0rm

       Exercise 4 SaintExploit

       Exercise 5 Core Impact

       Exercise 6 Turn in your Documentation

MODULE 11:Pen Testing Wireless Networks

WEBC⊕M
(A 12 year old / ISO 9000-2001 Company)

With the Association of

CYBER
INTELLIGENT | CIS
SECURITY

Certification by

mile2
Information Assurance Training

- Overview
- Standards Comparison
- SSID
- MAC Filtering
- WEP
- Weak IV Packets
- XOR Basics
- WEP Weaknesses
- How WPA Improves on WEP
- TKIP
- The WPA MIC Vulnerability
- WPA2
- WPA and WPA2 Modes
- WPA-PSK Encryption
- LEAP
- LEAP Weaknesses
- NetStumbler
- KNSGEM
- Vistumbler
- Kismet
- OmniPeek Personal
- Aircrack-ng Suite
- Airodump-ng
- Aireplay-ng
- DoS Attack
- Aircrack-ng
- Aircrack for Windows
- Attacking WEP
- Attacking WPA
- coWPAtty
- Exploiting Cisco LEAP
- asleap
- WiFiZoo
- Wesside-ng
- www.wirelessdefence.org
- Typical Network Blueprint
- EAP Types
- EAP Advantages/Disadvantages
- EAP/TLS Deployment
- Aruba Products
- Airwave RAPIDS Rogue Detection Module
- Review
- Lab 11 Pen Testing Wireless Networks

Exercise 1 War Driving

Exercise 2 WEP Cracking

Exercise 3 Turn in your Documentation

MODULE 12:Networks, Sniffing and IDS

- Overview
- Packet Sniffers
- Pcap and WinPcap
- Wireshark
- TCP Stream Re-assembling
- Packetyzer
- tcpdump and windump
- Omnipeek
- Cain and Abel
- Active Sniffing Methods
- Switch Table Flooding
- ARP Cache Poisoning
- ARP Normal Operation
- ARP Cache Poisoning in Action
- ARP Cache Poisoning with Linux
- Countermeasures
- Using Cain and Abel for ARP Cache Poisoning
- Ettercap
- Dsniff Suite
- Dsniff in Action
- MailSnarf, MsgSnarf and FileSnarf
- What is DNS Spoofing?
- DNS Spoofing
- Session Hijacking
- Breaking SSL
- Capturing VoIP
- Intercepting VoIP
- Intercepting RDP
- Routing Protocols Analysis
- Countermeasures for Sniffing
- Evading the Firewall and IDS
- Fragmentation
- Evading with Encryption
- Newer Firewall Capabilities
- New Age Protection
- Bastion Host

- Spyware Prevention System
- Intrusion SecureHost Overview
- IPS Overview
- Review
- Lab 12 Networks, Sniffing and IDS

    Exercise 1 Capture FTP Traffic

    Exercise 2 ARP Cache Poisoning Basics

    Exercise 3 ARP Cache Poisoning

    Exercise 4 Turn in your Documentation

MODULE 13:Injecting the Database

- Overview
- Vulnerabilities and Common Attacks
- SQL Injection
- Business Impacts of SQL Injection
- Why SQL Injection?
- Database Enumeration
- Extended Stored Proc
- Direct Attacks
- SQL Connection Properties
- Default Ports
- Obtaining Sensitive Info
- SQL Ping2
- osql.exe
- Query Analyzers
- SQLExec
- www.petefinnegan.com
- Metasploit
- Finding and Fixing SQL Injection
- Hardening Databases
- Review
- Lab 13 Attacking the Database

    Exercise 1 Login Bypass

    Exercise 2 Verbose Table Modific

    Exercise 3 Denial of Service

Exercise 4 Data Tampering

Exercise 5 Turn in your Documentation

MODULE 14:Attacking Web Technologies

* Overview
* Web Server Market Share
* OWASP Top 10
* Progression of the Professional Hacker
* The Anatomy of a Web Application Attack
* Components of a Web Application System
* Query String
* URL Mappings
* Information Gathering
* Changing URL Login Parameters
* URL Login - Horizontal Attack
* URL Login Vertical Escalation
* Cross-Site Scripting
* Stored XSS Illustrated
* Reflected XSS Illustrated
* Business Impacts of XSS
* Finding and Fixing XSS
* Injection Flaws
* Unvalidated Input
* Unvalidated Input Illustrated
* Business Impacts of Unvalidated Input
* Finding and Fixing Unvalidated Input
* Attacks against IIS
* IIS Directory Traversal
* Unicode
* IIS Logs
* N-Stalker
* NTO Spider
* HTTrack Website Copier
* Wikto
* Burp Proxy
* Brutus
* Dictionary Maker
* Cookies
* Acunetix Web Scanner
* Eclipse for Code Review
* WebScarab
* Samurai

WEBC☻M
(A 12 year old / ISO 9000-2001 Company)

With the Association of

CYBER
INTELLIGENT | CIS
SECURITY

Certification by

mile 2¹
Information Assurance Training

- OWASP Web Application Penetration Checklist
- Review
- Lab 14 Attacking Web Technologies

    Exercise 1 Input Manipulation

    Exercise 2 Shovelling a Shell

    Exercise 3 Horizontal Privilege Escalation

    Exercise 4 Vertical Privilege Escalation

    Exercise 5 Cross Site Scripting

    Exercise 6 Turn in your Documentation

MODULE 15: Report Writing

- Overview
- Additional Items to Consider
- The Report
- Support Documentation
- Analyzing Risk
- Report Results Matrix
- Findings Matrix Examples
- Delivering the Report
- Stating the Fact
- Recommendations
- Executive Summary
- Technical Report
- Table of Contents
- Summary of Weaknesses Identified
- Scope of Testing
- Summary of Recommendations
- Summary Observations
- Detailed Findings
- Strategic and Tactical Directives
- Statement of Responsibility
- Appendices
- Review

Appendix 1 – The Basics

- Overview
- The Growth of Environments and Security
- Our Motivation
- The Goal
- CIA Triad in Detail
- Holistic Security
- Security Definitions
- Definitions Relationships
- TCP/IP Basics

  Ping

  TCP/IP Stack

  TCP/IP for Security Administrators

  Ports and Services

  TCP 3-Way Handshake

  TCP Flags

- Malware

  Types of Malware

  Types of Viruses

  Spyware

  Trojan Horse

  Back Doors

- Denial of Service

  DDoS Issues

Appendix2 – Linux Fundamentals

- Overview
- Linux History
- The GNU Operating System
- Linux Introduction
- Linux GUI Desktops
- Linux Shell
- Linux Bash Shell
- Books on Linux
- Password and Shadow File Formats
- User Account Management
- Changing your Password
- Configuring your Network Interface
- Mounting Drives
- Tarballs and Zips
- Compiling Programs
- Typical Linux Operating Systems
- Gentoo
- VLOS
- Why use Linux Boot CD's?
- FrozenTechs Complete Distro List
- Backtrack
- Review

WEBCOM
(A 12 year old / ISO 9000-2001 Company)

With the Association of

CYBER INTELLIGENT SECURITY | CIS

Certification by

mile2
Information Assurance Training

- Network Devices and Sniffers

  Packet Sniffers

  Passive Sniffing

  Active Sniffing

- Firewalls, IDS and IPS

  Firewall

  IDS

  IPS

  Firewall Types

  Packet Filterin

  Proxy Firewalls

  Circuit-Level Proxy Firewall

  SOCKS

  Application-Layer Proxy

  Stateful

  Dynamic Packet

  Kernel Proxies

  Firewall Placement

  Screened Host

  Multi- or Dual

  Screened Subnet

- Wireless Standards

    WiFi Network Types

    Widely Deployed Standards

    Standards Comparison

    802.11n MIMO

- Database Basics

    Overview of Database Server

    Types of Databases

    Components of the

- Review

Appendix3 – Linux Fundamentals

- Overview
- Role of Access Control
- Definitions
- Categories of Access Controls
- Physical Controls
- Logical Controls
- Soft Controls
- Security Roles
- Steps to Granting Access
- Access Criteria
- Physical Access Control Mechanisms
- Biometric System Types
- Synchronous Token
- Asynchronous Token
- Memory Cards
- Smart Cards
- Cryptographic Keys
- Logical Access Controls
- OS Access Controls

Appendix4 – Protocols

- Overview
- OSI Application Layer
- OSI Presentation Layer
- OSI Session Layer
- OSI Transport Layer
- OSI Network Layer
- OSI Data Link
- OSI Physical Layer
- Protocols at Each OSI Model Layer
- TCP/IP Suite
- Port and Protocol Relationship
- Conceptual Use of Ports
- UDP vs TCP
- ARP
- ICMP
- DNS
- SSH
- SNMP
- SMTP

- Review   - Review

Appendix5 – Cryptography

- Overview
- Introduction
- Encryption
- Cryptographic Definitions
- The Science of Secret Communications
- Encryption Algorithm
- Implementation
- Symmetric Encryption
- Symmetric Downfalls
- Symmetric Algorithms
- Crack Times
- Asymmetric Encryption
- Asymmetric Advantages
- Asymmetric Disadvantages
- Asymmetric Algorithms
- Key Exchange
- Symmetric vs Asymmetric
- Hybrid Encryption
- Hashing
- Common Hash Algorithms

- Birthday Attack
- Hash Demo
- Security Issues in Hashing
- Hash Collisions
- MD5 Collision Creates Rogue Certificate Authority
- More Hybrid Encryption
- Digital Signatures
- SSL/TLS
- SSL Connection Setup
- SSL Hybrid Encryption
- SSH
- IPSec
- PKI

Appendix6 – Economics and Law

- Overview
- Security Incentives and Motives
- What is Your Weakest Link?
- What is the Value of an Asset?
- Non-Obvious Vulnerabilities
- Categorizing Risks
- Types of Losses
- Approaches to Analyzing Risk
- Who Uses What Analysis Type?
- Qualitative Analysis Method
- Quantitative Analysis
- Can a Purely Quantitative Method be accomplished?
- Comparing Cost and Benefit
- Cost of a Countermeasure
- CyberCrime
- Not Just Fun and Games
- Example of Computer Crimes
- Perpetrators
- Attack Types
- Telephone Fraud
- Identification Protection and Prosecution
- Privacy of Sensitive Data
- Privacy Issues US Laws and Examples
- EU Principles on Privacy
- Transborder Information Flow
- Employee Privacy Issues
- U.S. Law
- Common Laws Civil
- Common Laws Criminal
- Common Laws Administrative
- U.S. Federal Laws
- Intellectual Property Laws
- Trademark and Patent

WEBCOM
(A 12 year old / ISO 9000-2001 Company)

With the Association of

CYBER INTELLIGENT SECURITY | CIS

Certification by

mile2
Information Assurance Training

- Quantum Cryptography
- Attack Vectors
- Network Attacks
- More Attacks
- Review
- A5 Lab – Cryptography

  Exercise 1 – Caesar Encryption

  Exercise 2 – RC4 Encryption

  Exercise 3 – IPSec Deployment

- Software Licensing
- Digital Millennium Copyright Act
- Investigating
- Computer Crime and its Barriers
- Countries Working Together
- Security Principles for International Use
- Has a Crime Been Committed?
- Bringing in Law Enforcement
- Citizen vs Law Enforcement Investigation
- Investigation of Any Crime
- Role of Evidence in a Trial
- Evidence Requirements
- Chain of Custody
- How Evidence is Processed
- Evidence Types
- Hearsay Rule Exception
- Responding to an Incident
- Preparing for a Crime before it happens!
- Incident Handling
- Evidence Collection Topics
- Specialized Skill
- Trying to Trap the Bad Guy
- Companies Can be Found Liable!
- Review