Cyber Security Training & Consulting

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

CERTIFIED PENETRATION TESTING ENGINEER

KEY DATA

Course Title: C)PTE

Duration: 5 days

CPE Credits: 40

Class Format Options:

Instructor-led classroom
Live Virtual Training
Computer Based Training

Who Should Attend:

IT Auditors
System Administrators
IS Managers

Prerequisites:

A minimum of 12 months experience in networking technologies

Sound knowledge of TCP/IP

Network+, Security+

Basic Knowledge of Linux

Provided Materials:

Student Workbook
Student Reference Manual
Student Lab Guide
Software/Tools (DVDs)

Certification Exam:

C)PTE - Certified Penetration Testing Engineer

Certification Track:

C)PTE - Certified Penetration Testing Engineer

C)PTC - Certified Penetration Testing Consultant

C)DFE - Certified Digital Forensics Examiner

COURSE OVERVIEW

The Certified Penetration Testing Engineer course trains students on the 5 key elements of penetration testing: information gathering, scanning, enumeration, exploitation and reporting. Ethical hacking is the art of using these penetration testing techniques to identify and repair the latest vulnerabilities in a system to make sure it is secure. Malicious hackers use these same techniques to find the same vulnerabilities except they exploit the vulnerabilities giving them access to the businesses' network. Once inside, hackers can access private information, such as usernames, passwords, credit card numbers, and social security numbers of clients and employees. It's very likely this data will be held for ransom or sold off on a black market. Hackers are constantly looking for new companies they can exploit; when they come across yours, will they be able to gain access? Certified Penetration Testing Engineers are the solution to prevent this from happening to businesses they serve.

This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk.

The C)PTE'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; we believe that an equal emphasis on theoretical and real world experience is essential for effective knowledge transfer to you, the student.

UPON COMPLETION

Students will:

- Have knowledge to perform penetration test
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)PTE Exam.

ACCREDITATION

Accreditor:

The United States of America National Security Agency's Committee of National Security Systems

Accreditation:

For CNSS Standard CNSSI-4013: National Information Assurance Training Standard for System Administrators

Also available as:

LIVE VIRTUAL TRAINING

Attend live classes from anywhere in the world!

Visit Mile2.com for more information

gs GENERAL SECURITY pt PENETRATION TESTING ws WIRELESS SECURITY sc SECURE CODING vbp VIRTUALIZATION BEST PRACTICES cf COMPUTER FORENSICS dr DISASTER RECOVERY ias INFORMATION ASSURANCE SERVICES

mile2 SECURITY TRAINING PARTNER

EXAM INFORMATION

The Certified Penetration Testing Engineer exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $300 USD and must be purchased from the store on Mile2.com.

COURSE CONTENT

Module 0: Course Overview
Module 1: Logistics of Pen Testing
Module 2: Linux Fundamentals
Module 3: Information Gathering
Module 4: Detecting Live Systems
Module 5: Enumeration
Module 6: Vulnerability Assessments
Module 7: Malware Goes Undercover
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: Project Documentation

Lab 1: Getting Set Up
Lab 2: Linux Fundamentals
Lab 3: Information Gathering
Lab 4: Detecting Live Systems
Lab 5: Reconnaissance
Lab 6: Vulnerability Assessment
Lab 7: Malware
Lab 8: Windows Hacking
Lab 9: UNIX/Linux Hacking
Lab 10: Advanced Vulnerability and Exploitation
Lab 11: Attacking Wireless Networks
Lab 12: Network Sniffing and IDS
Lab 13: Database Hacking
Lab 14: Hacking Web Applications
Lab A5: Cryptography
Post Class Lab: Core Impact

DETAILED LAB DESCRIPTION

Module 1 Lab – Getting Set UP

Naming and subnet assignments
Discovering your class share
VM Image Preparation
Discovering the Student Materials
PDF Penetration Testing Methodology

Module 2 Lab – Linux Fundamentals

Ifconfig
Mounting a USB Thumb Drive
Mount a Windows partition
VNC Server
Preinstalled tools in BackTrack 5

Module 3 Lab – Information Gathering

Google Queries
Footprinting Tools
Getting everything you need with Maltego
Using Firefox for Pen Testing
Documentation of the assigned tasks

Module 4 Lab – Detecting Live Systems

Look@LAN
Zenmap
Zenmap in BackTrack 5
NMAP Command Line
Hping2
Unicornscan
Documentation of the assigned tasks

Module 5 Lab – Reconnaissance

Banner Grabbing
Zone Transfers
SNMP Enumeration
LDAP Enumeration
Null Sessions
SMB Enumeration
SMTP Enumeration
Documentation of the assigned tasks

Module 6 Lab – Vulnerability Assessment

Run Nessus for Windows
Run Saint
Documentation of the assigned tasks

Module 7 Lab – Malware

Netcat (Basics of Backdoor Tools)
Exploiting and Pivoting our Attack
Creating a Trojan
Documentation of the assigned tasks

Module 8 Lab – Windows Hacking

Cracking a Windows Password with Linux
Covering your tracks via Audit Logs
Stegonagraphy
Understanding Rootkits
Cracking a Windows Password with Cain
Windows 7 Client Side Exploit (Browser)
Windows 2008 SMBv2 Exploit
Documentation of the assigned tasks

Module 9 Lab – Hacking UNIX/Linux

Setup and Recon – Do you remember how?
Making use of a poorly configured service
Cracking a Linux password
Creating a backdoor and covering our tracks
Documentation of the assigned tasks

Module 10 Lab – Advanced Vulnerability and Exploitation Techniques

Metasploit Command Line
Metasploit Web Interface
Exploit-DB.com
Saint
Documentation

Module 11 Lab – Attacking Wireless Networks

War Driving Lab
WEP Cracking Lab (classroom only)
Documentation

Module 12 Lab – Networks, Sniffing and IDS

Capture FTP Traffic
ARP Cache Poisoning Basics
ARP Cache Poisoning - RDP
Documentation

Module 13 Lab – Database Hacking

Hacme Bank – Login Bypass
Hacme Bank – Verbose Table Modification
Hacme Books – Denial of Service
Hacme Books – Data Tampering
Documentation of the assigned tasks

Module 14 Lab – Hacking Web Applications

Input Manipulation
Shoveling a Shell
Hacme Bank – Horizontal Privilege Escalation
Hacme Bank – Vertical Privilege Escalation
Hacme Bank – Cross Site Scripting
Documentation of the assigned tasks

A5 Lab – Cryptography

Caesar Encryption
RC4 Encryption
IPSec Deployment

Post-Class Lab – CORE IMPACT

CORE IMPACT Exercise

DETAILED MODULE AND APPENDIX DESCRIPTION

Module 0: Course Introduction

Courseware Materials
Course Overview
Course Objectives
CPTEngineer Exam Information
Learning Aids
Labs
Class Prerequisites
Student Facilities

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
Recent Attacks & Security Breaches
What does a Hack cost you?
Internet Crime Complaint Center
The Evolving Threat
Security Vulnerability Life Cycle
Exploit Timeline
Zombie Definition
What is a Botnet?
How is a Botnet Formed?
Botnet Statistics
How are Botnet's Growing?
Types of Penetration Testing
Hacking Methodology
Methodology for Penetration Testing
Hacker vs. Penetration Tester
Not Just Tools
Website Review
Tool: SecurityNOW! SX
Seven Management Errors
Review

Module 2: Linux Fundamentals

Overview
Linux History: Linus + Minix = Linux
The GNU Operating System
Linux Introduction
Linux GUI Desktops
Linux Shell
Linux Bash Shell
Recommended Linux Book
Password & Shadow File Formats
User Account Management
Instructor Demonstration
Changing a user account password
Configuring Network Interfaces with Linux
Mounting Drives with Linux
Tarballs and Zips
Compiling Programs in Linux
Why Use Live Linux Boot CDs
Typical Linux Operating Systems
Most Popular: BackTrack
Review

Module 3: Information Gathering

Overview
What Information is gathered by the Hacker?
Organizing Collected Information
Leo meta-text editor
Free Mind: Mind mapping
IHMC CmapTools
Methods of Obtaining Information
Physical Access
Social Access
Social Engineering Techniques
Social Networks
Instant Messengers and Chats
Digital Access
Passive vs. Active Reconnaissance
Footprinting defined
Maltego
Maltego GUI
FireCAT
Footprinting tools
Google Hacking
Google and Query Operators
Blogs & Forums
Google Groups / USENET
Internet Archive: The WayBack Machine
Domain Name Registration
WHOIS
WHOIS Output
DNS Databases
Using Nslookup
Dig for Unix / Linux
Traceroute Operation
Traceroute (cont.)
3D Traceroute
Opus online traceroute
People Search Engines
Intelius info and Background Check Tool
EDGAR For USA Company Info
Company House For British Company Info
Client Email Reputation
Web Server Info Tool: Netcraft
Footprinting Countermeasures
DOMAINSBYPROXY.COM

SiteDigger
Job Postings
Review

Module 4: Detecting Live System

Overview
Introduction to Port Scanning
Port Scan Tips
Expected Results
Popular Port Scanning Tools
Stealth Online Ping
NMAP: Is the Host online
ICMP Disabled?
NMAP TCP Connect Scan
TCP Connect Port Scan
Tool Practice : TCP half-open & Ping Scan
Half-open Scan
Firewalled Ports
NMAP Service Version Detection
Additional NMAP Scans
Saving NMAP results
NMAP UDP Scans
UDP Port Scan
Advanced Technique
Tool: Superscan
Tool: Look@LAN
Tool: Hping2
Tool: Hping2
More Hping2
Tool: Auto Scan
OS Fingerprinting: Xprobe2
Xprobe2 Options
Xprobe2 –v –T21-500 192.168.XXX.XXX
Tool: P0f
Tool Practice: Amap
Tool: Fragrouter: Fragmenting Probe Packets
Countermeasures: Scanning
Review

Module 5: Enumeration

Enumeration Overview
Web Server Banners
Practice: Banner Grabbing with Telnet
SuperScan 4 Tool: Banner Grabbing
Sc
HTTPrint
SMTP Server Banner
DNS Enumeration
Zone Transfers from Windows 2000 DNS
Backtrack DNS Enumeration
Countermeasure: DNS Zone Transfers
SNMP Insecurity
SNMP Enumeration Tools
SNMP Enumeration Countermeasures
Active Directory Enumeration
LDAPMiner
AD Enumeration countermeasures
Null sessions
Syntax for a Null Session
Viewing Shares
Tool: DumpSec
Tool: Enumeration with Cain and Abel
NAT Dictionary Attack Tool
THC-Hydra
Injecting Abel Service
Null Session Countermeasures
Review

Module 6: Vulnerability Assessments

Overview
Vulnerabilities in Network Services
Vulnerabilities in Networks
Vulnerability Assessment Def
Vulnerability Assessment Intro
Testing Overview
Staying Abreast: Security Alerts
Vulnerability Research Sites
Vulnerability Scanners
Nessus
Nessus Report
SAINT – Sample Report
Tool: Retina
Qualys Guard
http://www.qualys.com/products/overview/
Tool: LANguard
Microsoft Baseline Analyzer
MBSA Scan Report
Dealing with Assessment Results
Patch Management
Other Patch Management Options

Module 7: Malware Goes Undercover

Overview
Distributing Malware
Malware Capabilities
Countermeasure: Monitoring Autostart Methods
Tool: Netcat
Netcat Switches
Netcat as a Listener
Executable Wrappers
Benign EXE's Historically Wrapped with Trojans
Tool: Restorator
Tool: Exe Icon
The Infectious CD-Rom Technique
Trojan: Backdoor.Zombam.B
Trojan: JPEG GDI+
All in One Remote Exploit
Advanced Trojans: Avoiding Detection
BPMTK
Malware Countermeasures
Gargoyle Investigator
Spy Sweeper Enterprise
CM Tool: Port Monitoring Software
CM Tools: File Protection Software
CM Tool: Windows File Protection
CM Tool: Windows Software Restriction Policies
CM Tool: Hardware Malware Detectors
Countermeasure: User Education

Module 8: Windows Hacking

Overview
Password Guessing
Password Cracking LM/NTLM Hashes
LM Hash Encryption
NT Hash Generation
Syskey Encryption
Cracking Techniques
Precomputation Detail
Creating Rainbow Tables
Free Rainbow Tables
NTPASSWD:Hash Insertion Attack
Password Sniffing
Windows Authentication Protocols
Hacking Tool: Kerbsniff & KerbCrack
Countermeasure: Monitoring Logs
Hard Disk Security
Breaking HD Encryption
Tokens & Smart Cards
USB Tokens
Covering Tracks Overview
Disabling Auditing
Clearing and Event log
Hiding Files with NTFS Alternate Data Stream
NTFS Streams countermeasures
What is Steganography?
Steganography Tools
Shedding Files Left Behind
Leaving No Local Trace
Tor: Anonymous Internet Access
How Tor Works
TOR + OpenVPN= Janus VM
Encrypted Tunnel Notes:
Hacking Tool: RootKit
Windows RootKit Countermeasures

Module 9: Hacking UNIX/Linux

Overview
Introduction
File System Structure
Kernel
Processes
Starting and Stopping Processes
Interacting with Processes
Command Assistance
Interacting with Processes
Accounts and Groups
Password & Shadow File Formats
Accounts and Groups
Linux and UNIX Permissions
X Window System
X Insecurities Countermeasures
Network File System (NFS)
NFS Countermeasures
Passwords and Encryption
Password Cracking Tools
Salting
Symbolic Link
Symlink Countermeasure
Core File Manipulation
Shared Libraries
Kernel Flaws
File and Directory Permissions

Set UID Programs
Trust Relationships
Logs and Auditing
Common Network Services
Remote Access Attacks
Brute-Force Attacks
Brute-Force Countermeasures
SUID Files Countermeasure
File and Directory Permissions
World-Writable Files Countermeasure
Clearing the Log Files
Rootkits
Rootkit Countermeasures
Review

Module 10: Advanced Exploitation Techniques

Overview
How Do Exploits Work?
Format String
Race Conditions
Memory Organization
Buffer OverFlows
Buffer Overflow Definition
Overflow Illustration
How Buffers and Stacks Are Supposed to Work
Stack Function
How a Buffer Overflow Works
Buffer Overflows
Heap Overflows
Heap Spraying
Prevention
Security Code Reviews
Stages of Exploit Development
Stages of Exploit Development
Shellcode Development
The Metasploit Project
The Metasploit Framework
Meterpreter
Fuzzers
SaintExploit at a Glance
SaintExploit Interface
Core Impact Overview
Review

Module 11: Pen Testing Wireless Networks

Overview
Standards Comparison
SSID (Service Set Identity)
MAC Filtering
Wired Equivalent Privacy
Weak IV Packets
WEP Weaknesses
XOR – Encryption Basics
How WPA improves on WEP
TKIP
The WPA MIC Vulnerability
802.11i - WPA2
WPA and WPA2 Mode Types
WPA-PSK Encryption
LEAP
LEAP Weaknesses
NetStumbler
Tool: Kismet
Tool: Aircrack-ng Suite
Tool: Airodump-ng
Tool: Aireplay
DOS: Deauth/disassociate attack
Tool: Aircrack-ng
Attacking WEP
Attacking WPA
coWPAtty
Exploiting Cisco LEAP
asleap
WiFiZoo
Wesside-ng
Typical Wired/Wireless Network
802.1X: EAP Types
EAP Advantages/Disadvantages
EAP/TLS Deployment
New Age Protection
Aruba – Wireless Intrusion Detection and Prevention
RAPIDS Rogue AP Detection Module
Review

Module 12: Networks, Sniffing, IDS

Overview
Example Packet Sniffers
Breaking SSL Traffic
Tool: Breaking SSL Traffic

Tool: Pcap & WinPcap
Tool: Wireshark
TCP Stream Re-assembling
Tool: Packetyzer
tcpdump & windump
Tool: OmniPeek
Sniffer Detection Using Cain & Abel
Active Sniffing Methods
Switch Table Flooding
ARP Cache Poisoning
ARP Normal Operation
ARP Cache Poisoning Tool
Countermeasures
Tool: Cain and Abel
Ettercap
Linux Tool Set: Dsniff Suite
Dsniff Operation
MailSnarf, MsgSnarf, FileSnarf
What is DNS spoofing?
Tools: DNS Spoofing
Session Hijacking
Tool: Cain and Abel
Voice over IP (VoIP)
Intercepting VoIP
Intercepting RDP
Cracking RDP Encryption
Routing Protocols Analysis
Countermeasures for Sniffing
Countermeasures for Sniffing
Evading The Firewall and IDS
Evasive Techniques
Firewall – Normal Operation
Evasive Technique -Example
Evading With Encrypted Tunnels
Newer Firewall Capabilities
'New Age' Protection
Networking Device – Bastion Host
Spyware Prevention System (SPS)
Intrusion 'SecureHost' Overview
Intrusion Prevention Overview
Review

Module 13: Injecting the Database

Overview
Vulnerabilities & Common Attacks
Why SQL "Injection"?
SQL Injection: Enumeration
SQL Extended Stored Procedures
Direct Attacks
SQL Connection Properties
Attacking Database Servers
Obtaining Sensitive Information
Hacking Tool: SQLScan
SQL Injection
Impacts of SQL Injection
Hacking Tool: osql.exe
Hacking Tool: Query Analyzers
Hacking Tool: SQLExec
www.petefinnegan.com
Hacking Tool: Metasploit
Finding & Fixing SQL Injection
Hardening Databases
Review

Module 14: Attacking Web Technologies

Overview
Web Server Market Share
Common Web Application Threats
Progression of a Professional Hacker
Anatomy of a Web Application Attack
Web Applications Components
Web Application Penetration Methodologies
URL Mappings to Web Applications
Query String
Changing URL Login Parameters
Cross-Site Scripting (XSS)
Injection Flaws
Unvalidated Input
Unvalidated Input Illustrated
Impacts of Unvalidated Input
Unicode
IIS Directory Traversal
IIS Logs
Other Unicode Exploitations
N-Stalker Scanner 2009
NTOSpider
HTTrack Website Copier
Wikto Web Assessment Tool
SiteDigger v3.0
Paros Proxy
Burp Proxy
Brutus
Dictionary Maker
Cookies
Acunetix Web Scanner

Finding & Fixing Un-validated Input
Attacks Against IIS
Samurai Web Testing Framework

Module 15: Project Documentation

Overview
Additional Items
The Report
Report Criteria:
Supporting Documentation
Analyzing Risk
Report Results Matrix
Findings Matrix
Delivering the Report
Stating Fact
Recommendations
Executive Summary
Technical Report
Report Table Of Contents
Summary Of Security Weaknesses Identified
Scope of Testing
Summary 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: Protecting Information!
CIA Triad in Detail
Approach Security Holistically
Security Definitions
Definitions Relationships
Method: Ping
The TCP/IP stack
Recommended Video: It's Showtime
Which services use which ports?
TCP 3-Way Handshake
TCP Flags
Malware
Types of Malware
Types of Malware Cont…
Types of Viruses
More Malware: Spyware
Trojan Horses
Back Doors
DDoS Issues
DDoS
Packet Sniffers
Passive Sniffing
Active Sniffing
Firewalls, IDS and IPS
Firewall – First line of defense
IDS – Second line of defense
IPS – Last line of defense?
Firewalls
Firewall Types: (1) Packet Filtering
Firewall Types: (2) Proxy Firewalls
Firewall Types – Circuit-Level Proxy Firewall
Type of Circuit-Level Proxy – SOCKS
Firewall Types – Application-Layer Proxy
Firewall Types: (3) Stateful
Firewall Types: (4) Dynamic Packet-Filtering
Firewall Types: (5) Kernel Proxies
Firewall Placement
Firewall Architecture Types – Screened Host
Multi- or Dual-Homed
Screened Subnet
Wi-Fi Network Types
Widely Deployed Standards
Standards Comparison
802.11n - MIMO
Overview of Database Server
Types of databases
Overview of Database Server
Review

Appendix 2: Financial Sector Regulations Pertaining to Pen Testing

Overview
IT Governance Best Practice
IT Risk Management
Types of Risks
Gramm-Leach-Bliley-Act 1999 Title V
Federal Financial Examination Institution Council -FF
Sarbanes-Oxley Act (SOX 404) 2002
IT Applications and Security

Information Security Risk Evaluation
Improving Security Posture
Risk Evaluation Activities
Risk Assessment
Information Gathering
Data Classification
Threats and Vulnerabilities
Analytical Methods
Evaluate ControlsRisk Ratings
Important Risk Assessment Practices
Compliance
Many Regulations
Basel II
Internal Control: SOX
SOX: Business or IT Issue?
IT Issue for SOX
ISO 27002
ISO 27002: Control Components
Background on PCI
Dirty Dozen
Change Control and Auditing
Total Cost of Compliance
What does this mean to the tech?
Review

Appendix 3: Access Controls

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 Device
Memory Cards
Smart Card
Cryptographic Keys
Logical Access Controls
OS Access Controls
Review

Appendix 4: Protocols

Protocols Overview
OSI – Application Layer
OSI – Presentation Layer
OSI – Session Layer
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 versus TCP
Protocols – ARP
Protocols – ICMP
Network Service – DNS
SSH Security Protocol
SSH
Protocols – SNMP
Protocols – SMTP
Review

Appendix 5: Cryptography

Overview
Introduction
Encryption
Cryptographic Definitions
Encryption Algorithm
Implementation
Symmetric Encryption
Symmetric Downfalls
Symmetric Algorithms
Common Hash Algorithms
Birthday Attack
Example of a Birthday Attack
Generic Hash Demo
Instructor Demonstration
Security Issues in Hashing
Hash Collisions
MD5 Collision Creates Rogue Certificate Authority
Hybrid Encryption

Crack Times
Asymmetric Encryption
Public Key Cryptography Advantages
Asymmetric Algorithm Disadvantages
Asymmetric Algorithm Examples
Key Exchange
Symmetric versus Asymmetric
Using the Algorithm Types Together
Instructor Demonstration
Hashing
Hashing Explained
Digital Signatures
SSL/TLS
SSL Connection Setup
SSL Hybrid Encryption
SSH
IPSec - Network Layer Protection
Public Key Infrastructure
Quantum Cryptography
Attack Vectors
Network Attacks
More Attacks (Cryptanalysis)

Appendix 6: Economics and Law

Security Incentives & Motivations
What motivates us to promote security?
Security Incentives & Motivations
What motivates others to attack security?
What is Your Weakest Link?
What Is the Value of an Asset?
Examples of non-obvious Vulnerabilities
Categorizing Risks
Some Examples of Types of Losses
Different Approaches to Analyzing Risks
Who Uses What Analysis Type?
Qualitative Analysis Steps
Quantitative Analysis
Routing Data Through Different Countries
Employee Privacy Issues
U.S. LAW
Common Laws – Civil
Common Laws – Criminal
Common Laws – Administrative
U.S. Federal Laws
Intellectual Property Laws
More Intellectual Property Laws
Software Licensing
Digital Millennium Copyright Act
Investigating
Computer Crime and Its Barriers
Countries Working Together
Security Principles for International Use
Can a Purely Quantitative Analysis Be Accomplished?
Comparing Cost and Benefit
Cost of a Countermeasure
Cyber Crime!
Not Just Fun and Games
Examples of Computer Crimes
Who Perpetrates These Crimes?
A Few Attack Types
Telephone Fraud
Identification Protection & Prosecution
Privacy of Sensitive Data
Privacy Issues – U.S. Laws as Examples
European Union Principles on Privacy
Bringing in Law Enforcement
Investigation of Any Crime
Role of Evidence in a Trial
Evidence Requirements
Chain of Custody
How Is Evidence Processed?
Evidence Types
Hearsay Rule Exception
Responding to an Incident
Preparing for a Crime Before It Happens
Incident Handling
Evidence Collection Topics
Computer Forensics