

NETWORKING AND SECURITY

Revised 12/18/2011

/training/etc

The Art of Knowledge.

This Page Intentionally Left Blank

Table of Contents

A+ Essentials.....	1
Network+ Certification.....	2
Security+ Certification.....	3
Systems Security Certified Practitioner (SSCP) Certification.....	4
Certified Ethical Hacker.....	5
Wireless LAN Administration.....	7
Wireless LAN Security.....	8
CISSP.....	9
ISSEP.....	10
Cyber Security: Malicious Code Analysis.....	11
ECSA/LPT Certification Bootcamp.....	12
Certified Network Defense Architect (CNDA).....	13
Computer Hacking Forensics Investigator (CHFI).....	14
Security Certified Program: Tactical Perimeter Defense.....	16
Security Certified Program: Strategic Infrastructure Security.....	17
Security Certified Program: Advanced Security Implementation.....	18
Security Certified Program: Enterprise Security Solutions.....	19

This Page Intentionally Left Blank

Course Description:

In this course, students will install, upgrade, repair, configure, optimize, troubleshoot, and perform preventative maintenance on basic personal computer hardware and operating systems.

Who Should Attend:

The target student is anyone with basic computer user skills who is interested in obtaining a job as an IT professional or PC technician. Possible job environments include mobile or corporate settings with a high level of face-to-face client interaction, remote-based work environments where client interaction, client training, operating systems, and connectivity issues are emphasized, or settings with limited customer interaction where hardware activities are emphasized. In addition, this course will help prepare students to achieve a CompTIA A+ Certification.

Prerequisites:

Students taking this course should have the following skills: End-user skills with Windows-based personal computers, including the ability to: Browse and search for information on the Internet. Start up and shut down the computer. Log on to a computer and computer network. Run programs. Move, copy, delete, and rename files in Windows Explorer. Basic knowledge of computing concepts, including: The difference between hardware and software. The functions of software components, such as the operating system, applications, and file systems. The function of a computer network.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify the components of standard desktop personal computers.
- Identify fundamental components and functions of personal computer operating systems.
- Identify best practices followed by professional personal computer technicians.
- Install and configure computer components.
- Install and configure system components.
- Maintain and troubleshoot peripheral components.
- Troubleshoot system components.
- Install and configure operating systems.
- Maintain and troubleshoot installations of Microsoft Windows.
- Identify network technologies.
- Install and manage network connections.
- Support laptops and portable computing devices.
- Support printers and scanners.
- Identify personal computer security concepts.
- Support personal computer security.

Course Outline:**Lesson 1: Personal Computer Components**

Personal Computer Components
System Unit Components
Storage Devices
Personal Computer Connection Methods

Lesson 2: Operating System Fundamentals

Personal Computer Operating Systems
Windows User Interface Components
Windows File System Management
Windows System Management Tools

Lesson 3: PC Technician Professional Best Practices

Tools of the Trade
Electrical Safety
Environmental Safety and Materials Handling
Perform Preventative Maintenance
Diagnostics and Troubleshooting
Professionalism and Communication

Lesson 4: Installing and Configuring Peripheral Components

Install and Configure Display Devices
Install and Configure Input Devices
Install and Configure Adapter Cards
Install and Configure Multimedia Devices

Lesson 5: Installing and Configuring System Components

Install and Configure Storage Devices
Install and Configure Power Supplies
Install and Configure Memory
Install and Configure CPUs
Install and Configure System Boards

Lesson 6: Maintaining and Troubleshooting Peripheral Components

Troubleshoot Display Devices
Maintain and Troubleshoot Input Devices
Troubleshoot Adapter Cards

Troubleshoot Multimedia Devices

Lesson 7: Troubleshooting System Components

Troubleshoot Storage Devices
Troubleshoot Power Supplies
Troubleshoot Memory
Troubleshoot CPUs
Troubleshoot System Boards

Lesson 8: Installing and Configuring Operating Systems

Install Microsoft Windows
Upgrade Windows
Add Devices to Windows
Optimize Windows

Lesson 9: Maintaining and Troubleshooting Microsoft Windows

Operating System Utilities
Maintain Microsoft Windows
Troubleshoot Microsoft Windows
Recover Microsoft Windows

Lesson 10: Network Technologies

Network Concepts
Network Communications
Network Connectivity
Internet Technologies

Lesson 11: Installing and Managing Network Connections

Create Network Connections
Install and Configure Web Browsers
Maintain and Troubleshoot Network Connections

Lesson 12: Supporting Laptops and Portable Computing Devices

Laptop and Portable Computing Device Components
Install and Configure Laptops and Portable Computing Devices
Maintain and Troubleshoot Laptops and Portable Computing Devices

Lesson 13: Supporting Printers and Scanners

Printer and Scanner Technologies
Printer and Scanner Components
Printer and Scanner Processes
Install and Configure Printers and Scanners
Maintain and Troubleshoot Printers and Scanners

Lesson 14: Personal Computer Security Concepts

Security Fundamentals
Security Protection Measures
Data and Physical Security
Wireless Security
Social Engineering

Lesson 15: Supporting Personal Computer Security

Install and Configure Security Measures
Maintain and Troubleshoot Security Measures

Course Description:

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network. This course will help prepare students for the CompTIA Network+ 2009 certification exam. It should be noted that a course alone cannot prepare students for any CompTIA exam. It is important that students have the recommended work experience in IT networking prior to taking the exam. For the CompTIA Network+ 2009 certification, CompTIA recommends students have 9 to 12 months of experience in the IT support industry. If you are taking this course with the exam voucher, it is for exam N10-0005.

Who Should Attend:

This course is geared toward technicians with nine to 12 months of experience in the IT industry who wish to earn their Network+ certification.

Prerequisites:

An introductory course in a Windows operating system, or equivalent skills and knowledge, is required. CompTIA A+ certification, or the equivalent skills and knowledge, is helpful but not required.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.
- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.
- Identify major issues, models, tools, and techniques in network troubleshooting.

Course Outline:**Network basics**

Network concepts
Network architectures
The OSI model

Wired computer-to-computer connections

Wired network connections
Network interface cards and modems

Network-to-network connections

Network-to-network connection components
LAN wiring
LAN wiring tests

Wired internetworking devices

Basic internetworking devices
Specialized internetworking devices

Wired communication standards

The TCP/IP protocol suite
TCP/IP
DHCP servers

Wireless networking

Wireless network devices
Wireless networking standards
Wireless configuration

Security threats and mitigation

Security threats
Threat mitigation

Security practices

Operating systems
Devices

Network access control

Authentication
Public key cryptography
Remote access
Wireless security

Monitoring

Monitoring resources
Event Viewer

Troubleshooting

Troubleshooting basics

Troubleshooting the network
Troubleshooting scenarios

Appendix A: Certification exam objectives map

Comprehensive exam objectives

Appendix B: CompTIA Network+ Acronyms

Acronym list

Course Description:

This course will prepare students to pass the current CompTIA Security+ SY0-301 certification exam. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field. Comes with CertBlaster exam prep software (download).

Who Should Attend:

This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as NetWare, Macintosh, UNIX/Linux, and OS/2, who wants to: further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

Prerequisites:

Students should have CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP. Although not required, students might find it helpful to obtain foundational information from introductory operating system administration courses.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.
- Enforce an organizational security policy.
- Monitor the security infrastructure.

Course Outline:**Mitigating threats**

System maintenance
Application security
Physical security
Malware
Social engineering

Cryptography

Symmetric cryptography
Public key cryptography

Authentication

: Authentication factors and requirements
Authentication systems
Authentication system vulnerabilities

User- and role-based security

Baseline security policies
Resource access

Peripheral security

File and disk encryption
Peripheral and component security
Mobile device security

Public key infrastructure

Public key cryptography
Implementing public key infrastructure
Web server security with PKI

Application and messaging security

Application security
E-mail security
Social networking and messaging

Ports and protocols

TCP/IP basics
Protocol-based attacks

Network security

Network devices
Secure network topologies
Secure networking
Virtualization and cloud computing

Wireless security

Wireless network security
Mobile device security

Remote access security

Remote access
Virtual private networks

Vulnerability testing and monitoring

Risk and vulnerability assessment
Auditing and logging
Intrusion detection and prevention systems
Incident response

Organizational security

Organizational policies
Education and training
Disposal and destruction

Business continuity

Business continuity planning
Disaster recovery
Environmental controls

Course Description:

Looking to move up in the information security field? If you have at least one year of security experience, you qualify for the Systems Security Certified Practitioner (SSCP) certification, which offers junior security professionals a way to validate their experience and demonstrate competence with (ISC)2®'s seven domains.

Who Should Attend:

This course is for those in an organization who are fairly new to the field of information security or that do not have security as their primary job responsibility.

Prerequisites:

Students should have systems administration experience, familiarity with TCP/IP, and an understanding of UNIX, Linux, and Windows. This course also requires intermediate-level knowledge of security concepts.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Understand Access Controls
- Perform Security Operations and Administration
- Perform Analysis and Monitoring
- Understand Cryptography
- Understand and manage Networks and Telecommunications
- Identify and react to Malicious Code/Malware
- Identify Risk, Response, and Recovery

Course Outline:**Testing-Taking Tips and Study Techniques**

Preparation for the SSCP Exam
Submitting Required Paperwork
Resources and Study Aids
Passing the Exam the First Time

Security Operations and Administration

Change Control/Configuration Management
Dual Control, Separation of Duties, Rotation of Duties
Vulnerability Assessment and Pen-Testing

Access Controls

AAA
Authentication Methods (Types 1, 2, & 3)
Authorization - DAC, RBAC, MAC
Accounting - Logging, Monitoring, Auditing
Central/Decentralized and Hybrid Management
Single Sign-On - Kerberos, Radius, Diameter, TACACS
Vulnerabilities - Emanations, Impersonation, Rouge Infrastructure, Social Engineering

Cryptography

Intro/History
Symmetric
Asymmetric
Hashing
Cryptosystems - SSL, S/MIME, PGP
PKI
Cryptanalysis

Malicious Code and Malware

Layering, Data Hiding, and Abstraction
Database Security
AI
OOD
Mobil Code
Malware Architecture Problems - Covert Channels + TOC/TOU, Object Reuse
Network Vulnerabilities

Networks and Telecommunications

OSI/DoD TCP/IP Models
TCP/UDP/ICMP/IP
Ethernet
Devices - Routers/Switches/Hubs
Firewalls
Wireless
WAN Technologies - X.25/Frame Relay/PPP/ISDN/DSL/Cable
Voice - PBX/Cell Phones/VOIP
IPSec

Risk, Response, and Recovery

CIA
Roles and Responsibilities - RACI
Asset Management
Taxonomy - Information Classification
Risk Management
Policies, Procedures, Standards, Guidelines, Baselines
Knowledge Transfer - Awareness, Training, Education

BIA Policy
BIA Roles and Teams
Data Backups, Vaulting, Journaling, Shadowing
Alternate Sites
Emergency Response
Required notifications
BIA Tests

Analysis and Monitoring

Ethics - Due Care/Due diligence
Intellectual Property
Incident Response
Forensics
Evidence
Laws - HIPAA, GLB, SOX

Review and Q&A Session

Final Review and Test Prep

Course Description:

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5--day class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Who Should Attend:

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites:

Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent. Not anyone can be a student - the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Understand how intruders escalate privileges.
- Understand Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Understand Ethical Hacking.

Course Outline:**Module 01: Introduction to Ethical Hacking**

Internet Crime Current Report: IC3
Data Breach Investigations Report
Types of Data Stolen From the Organizations
Essential Terminologies
Elements of Information Security
Authenticity and Non-Repudiation
The Security, Functionality, and Usability Triangle
Security Challenges
Effects of Hacking
Who is a Hacker?
Hacker Classes
Hacktivism
What Does a Hacker Do?
Phase 1 - Reconnaissance
Phase 2 - Scanning
Phase 3 - Gaining Access
Phase 4 - Maintaining Access
Phase 5 - Covering Tracks
Types of Attacks on a System
Why Ethical Hacking is Necessary?
Defense in Depth
Scope and Limitations of Ethical Hacking
Who Do Ethical Hackers Do?
Skills of an Ethical Hacker
Vulnerability Research
Vulnerability Research Websites
What is Penetration Testing?
Why Penetration Testing?
Penetration Testing Methodology

Module 02: Footprinting and Reconnaissance

Footprinting Terminologies
What is Footprinting?
Objectives of Footprinting
Footprinting Threats
Finding a Company's URL
Locate Internal URLs
Public and Restricted Websites
Search for Company's Information
Footprinting Through Search Engines
Collect Location Information
People Search
Gather Information from Financial Services
Footprinting Through Job Sites
Monitoring Target Using Alerts
Competitive Intelligence Gathering
WHOIS Lookup
Extracting DNS Information
Locate the Network Range
Traceroute
Mirroring Entire Website
Extract Website Information from <http://www.archive.org>
Monitoring Web Updates Using Website Watcher

Tracking Email Communications
Footprint Using Google Hacking Techniques
What a Hacker Can Do With Google Hacking?
Google Advance Search Operators
Google Hacking Tool: Google Hacking Database (GHD)
Google Hacking Tools
Additional Footprinting Tools
Footprinting Countermeasures
Footprinting Pen Testing

Module 03: Scanning Networks

Network Scanning
Types of Scanning
Checking for Live Systems - ICMP Scanning
Ping Sweep
Three-Way Handshake
TCP Communication Flags
Hping2 / Hping3
Hping Commands
Scanning Techniques
Scanning: IDS Evasion Techniques
IP Fragmentation Tools
Scanning Tool: Nmap
Scanning Tool: NetScan Tools Pro
Scanning Tools
Do Not Scan These IP Addresses (Unless you want to get into trouble)

Module 04: Enumeration

What is Enumeration?
Techniques for Enumeration
Netbios Enumeration
Enumerating User Accounts
Enumerate Systems Using Default Passwords
SNMP (Simple Network Management Protocol) Enumeration
UNIX/Linux Enumeration
LDAP Enumeration
NTP Enumeration
SMTP Enumeration
DNS Zone Transfer Enumeration
Using nslookup
Enumeration Countermeasures
Enumeration Pen Testing

Module 05: System Hacking

Information at Hand Before System Hacking Stage
System Hacking: Goals
CEH Hacking Methodology (CHM)
Password Cracking
Microsoft Authentication
How Hash Passwords are Stored in Windows SAM?
What is LAN Manager Hash?
Kerberos Authentication

Salting
PWdump7 and Fgdump
L0phtCrack
Optcrack
Cain & Abel
RainbowCrack
Password Cracking Tools
LM Hash Backward Compatibility
How to Defend against Password Cracking?

Privilege Escalation
Active@ Password Changer
Privilege Escalation Tools
How to Defend against Privilege Escalation?
Executing Applications
Alchemy Remote Executor
RemoteExec
Execute This!
Keylogger
Types of Keystroke Loggers
Acoustic/CAM Keylogger
Keyloggers
Spyware
How to Defend against Keyloggers?
How to Defend against Spyware?
Rootkits
Types of Rootkits
How Rootkit Works?
Rootkit: Fx
Detecting Rootkits
How to Defend against Rootkits?
Anti-Rootkit: RootkitRevealer and McAfee Rootkit Detective

NTFS Data Stream
What is Steganography?
Types of Steganography
Image Steganography
Document Steganography: wbStego
Video Steganography: Our Secret
Audio Steganography: Mp3stegz
Folder Steganography: Invisible Secrets 4
Spam/Email Steganography: Spam Mirror
Natural Text Steganography: Sams Big G Play Maker
Steganalysis
Steganography Detection Tool: Stegdetect
Why Cover Tracks?
Ways to Clear Online Tracks
Disabling Auditing: Auditpol
Covering Tracks Tool: Window Washer
Covering Tracks Tool: Tracks Eraser Pro
System Hacking Penetration Testing

Module 06: Trojans and Backdoors

What is a Trojan?

Overt and Covert Channels
Purpose of Trojans
What Do Trojan Creators Look For?
Indications of a Trojan Attack
Common Ports used by Trojans
How to Infect Systems Using a Trojan?
Wrappers
Different Ways a Trojan can Get into a System

How to Deploy a Trojan?
Evasion Anti-Virus Techniques
Types of Trojans
Destructive Trojans
Notification Trojans
Credit Card Trojans
Data Hiding Trojans (Encrypted Trojans)
BlackBerry Trojan: PhoneSnoop
MAC OS X Trojan: DNSChanger
MAC OS X Trojan: DNSChanger
Mac OS X Trojan: Hell Raiser
How to Detect Trojans?
Process Monitoring Tool: What's Running
Scanning for Suspicious Registry Entries
Registry Entry Monitoring Tools
Scanning for Suspicious Device Drivers
Scanning for Suspicious Windows Services
Scanning for Suspicious Startup Programs
Scanning for Suspicious Files and Folders
Scanning for Suspicious Network Activities

Module 07: Viruses and Worms

Trojan Countermeasures
Backdoor Countermeasures
Trojan Horse Construction Kit
Anti-Trojan Software: TrojanHunter
Anti-Trojan Software: Emissoft Anti-Malware
Anti-Trojan Softwares
Pen Testing for Trojans and Backdoors
Introduction to Viruses
Virus and Worm Statistics 2010
Stages of Virus Life
Working of Viruses: Infection Phase
Working of Viruses: Attack Phase
Why Do People Create Computer Viruses?
Indications of Virus Attack
How does a Computer get Infected by Viruses?
Virus Hoaxes
Virus Analysis:

Types of Viruses
Transient and Terminate and Stay Resident Viruses
Writing a Simple Virus Program
Computer Worms
How is a Worm Different from a Virus?
Example of Worm Infection: Conficker Worm

Worm Analysis:
What is Sheep Dip Computer?
Anti-Virus Sensors Systems
Malware Analysis Procedure
String Extracting Tool: Bintext
Compression and Decompression Tool: UPX
Process Monitoring Tools: Process Monitor
Log Packet Content Monitoring Tools: NetResident
Debugging Tool: Ollydbg
Virus Analysis Tool: IDA Pro
Online Malware Testing:
Online Malware Analysis Services
Virus Detection Methods
Virus and Worms Countermeasures
Compression Antivirus: Immunet Protect
Anti-virus Tools
Penetration Testing for Virus

Module 08: Sniffers

Lawful Intercept
Wiretapping
Sniffing Threats
How a Sniffer Works?
Hacker Attacking a Switch
Types of Sniffing: Active Sniffing
Protocols Vulnerable to Sniffing
Tie to Data Link Layer in OSI Model
Hardware Protocol Analyzers
SPAN Port
MAC Flooding
How DHCP Works?
What is Address Resolution Protocol (ARP)?
Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
MAC Spoofing/Duplicating
DNS Poisoning Techniques
Sniffing Tool: WireShark
Sniffing Tool: CACE Pilot
Sniffing Tool: Tcplump/Windowump
Discovery Tool: NetworkView
Discovery Tool: The Dude Sniffer
Password Sniffing Tool: Ace Packet Sniffing Tool: Capsa Network Analyzer
OmniPeek Network Analyzer
Network Packet Analyzer: Observer

Certified Ethical Hacker

Session Capture Sniffer: NetWitness
Email Message Sniffer: Big-Mother
TCP/IP Packet Crafter: Packet Builder
Additional Sniffing Tools
How an Attacker Hacks the Network
Using Sniffers?
How to Defend Against Sniffing?
Sniffing Prevention Techniques
How to Detect Sniffing?
Promiscuous Detection Tool:
PromyUI
Promiscuous Detection Tool:
PromiScan

Module 09: Social Engineering

What is Social Engineering?
Behaviors Vulnerable to Attacks
Why is Social Engineering Effective?
Warning Signs of an Attack
Phases in a Social Engineering Attack
Impact on the Organization
Command Injection Attacks
Common Targets of Social Engineering
Types of Social Engineering
Insider Attack
Common Intrusion Tactics and Strategies for Prevention
Social Engineering Through Impersonation on Social Networking Sites
Risks of Social Networking to Corporate Networks
Identity Theft Statistics 2010
Real Steven Gets Huge Credit Card Statement
Identity Theft - Serious Problem
Social Engineering Countermeasures: Policies
How to Detect Phishing Emails?
Identity Theft Countermeasures
Social Engineering Pen Testing

Module 10: Denial of Service

What is a Denial of Service Attack?
What is Distributed Denial of Service Attacks?
Symptoms of a DoS Attack
Cyber Criminals
Internet Chat Query (ICQ)
Internet Relay Chat (IRC)
DoS Attack Techniques
Botnet
WikiLeak Operation Payback
DoS Attack Tools
Detection Techniques
DoS/DDoS Countermeasure Strategies
DDoS Attack Countermeasures
Post-attack Forensics
Techniques to Defend against Botnets
DoS/DDoS Countermeasures
DoS/DDoS Protection at ISP Level
Enabling TCP Intercept on Cisco IOS Software
Advanced DDoS Protection:
IntelliGuard DDoS Protection System (DPS)
DoS/DDoS Protection Tool
Denial of Service (DoS) Attack Penetration Testing

Module 11: Session Hijacking

What is Session Hijacking?
Dangers Posed by Hijacking
Why Session Hijacking is Successful?
Key Session Hijacking Techniques
Brute Forcing
HTTP Referrer Attack
Spoofing vs. Hijacking
Session Hijacking Process
Packet Analysis of a Local Session Hijack
Types of Session Hijacking
Predictable Session Token
Man-in-the-Middle Attack
Man-in-the-Browser Attack
Client-side Attacks
Cross-site Script Attack
Session Fixation
Network Level Session Hijacking
The 3-Way Handshake
Sequence Numbers
TCP/IP Hijacking
IP Spoofing: Source Routed Packets
RST Hijacking
Blind Hijacking
Man-in-the-Middle Attack using Packet Sniffer
UDP Hijacking
Session Hijacking Tools
Countermeasures
Protecting against Session Hijacking
Methods to Prevent Session

Hijacking: To be Followed by Web Developers
Methods to Prevent Session Hijacking: To be Followed by Web Users
Defending against Session Hijack Attacks
Session Hijacking Remediation
IPSec
Session Hijacking Pen Testing

Module 12: Hijacking Webservers

Webserver Market Shares
Open Source Webserver Architecture
IIS Webserver Architecture
Website Defacement
Case Study
Why Web Servers are Compromised?
Impact of Webserver Attacks
Webserver Misconfiguration
Directory Traversal Attacks
HTTP Response Splitting Attack
Web Cache Poisoning Attack
HTTP Response Hijacking
SSH BruteForce Attack
Man-in-the-Middle Attack
Webserver Password Cracking
Web Application Attacks
Webserver Attack Methodology
Webserver Attack Tools
Web Password Cracking Tool
Countermeasures
How to Defend Against Web Server Attacks?
How to Defend against HTTP Response Splitting and Web Cache Poisoning?
Patches and Hotfixes
What is Patch Management?
Identifying Appropriate Sources for Updates and Patches
Installation of a Patch
Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)
Web Application Security Scanner: Sandcat
Web Server Security Scanner: Wikto
Webserver Malware Infection Monitoring Tool: HackAlert
Webserver Security Tools
Web Server Penetration Testing

Module 13: Hacking Web Applications

Web Application Security Statistics
Introduction to Web Applications
Web Application Components
How Web Applications Work?
Web Application Architecture
Web 2.0 Applications
Vulnerability Stack
Web Attack Vectors
Web Application Threats - 1
Web Application Threats - 2
Unvalidated Input
Parameter/Form Tampering
Directory Traversal
Security Misconfiguration
Injection Flaws
What is LDAP Injection?
How LDAP Injection Works?
Hidden Field Manipulation Attack
Cross-Site Scripting (XSS) Attacks
Web Application Denial-of-Service (DoS) Attack
Buffer Overflow Attacks
Cookie/Session Poisoning
Session Fixation Attack
Insufficient Transport Layer Protection
Improper Error Handling
Insecure Cryptographic Storage
Broken Authentication and Session Management
Unvalidated Redirects and Forwards
Web Services Architecture
Footprint Web Infrastructure
Web Spidering Using Burp Suite
Hacking Web Servers
Analyze Web Applications
Attack Authentication Mechanism
Username Enumeration
Password Attacks: Password Functionality Exploits
Password Attacks: Password Guessing
Password Attacks: Brute-forcing
Session Attacks: Session ID Prediction/Brute-forcing
Cookie Exploitation: Cookie Poisoning
Authorization Attack
Session Management Attack
Injection Attacks
Attack Data Connectivity
Attack Web App Client
Attack Web Services

Web Services Probing Attacks
Web Service Attack Tool: soapUI
Web Service Attack Tool: XMLSpy
Web Application Hacking Tool: Burp Suite Professional
Web Application Hacking Tools: CookieDigger
Web Application Hacking Tools: WebScarab
Encoding Schemes
Web Application Countermeasures
Web Application Firewall: dotDefender
Web Application Firewall: IBM AppScan
Web Application Firewall: ServerDefender VP
Web Application Pen Testing

Module 14: SQL Injection

SQL Injection is the Most Prevalent Vulnerability in 2010
SQL Injection Threats
What is SQL Injection?
SQL Injection Attacks
How Web Applications Work?
Server Side Technologies
HTTP Post Request
SQL Injection Detection
SQL Injection Black Box Pen Testing
Types of SQL Injection
What is Blind SQL Injection?
SQL Injection Methodology
Information Gathering
Database, Table, and Column Enumeration
Features of Different DBMSs
Password Grabbing
Transfer Database to Attacker's Machine
Interacting with the Operating System
Interacting with the FileSystem
Network Reconnaissance Full Query
SQL Injection Tools
Evading IDS
How to Defend Against SQL Injection Attacks?
SQL Injection Detection Tools
Short Rule to Detect SQL Injection Attacks

Module 15: Hacking Wireless Networks

Wireless Networks
Wi-Fi Usage Statistics in the US
Wi-Fi Hotspots at Public Places
Wi-Fi Networks at Home
Types of Wireless Networks
Wireless Standards
Service Set Identifier (SSID)
Wi-Fi Authentication Modes
Wireless Terminologies
Wi-Fi Chalking
Wi-Fi Hotspot Finder: jwire.com
Wi-Fi Hotspot Finder: WeFi.com
Types of Wireless Antenna
Parabolic Grid Antenna
Types of Wireless Encryption
WEP Encryption
What is WPA?
Temporal Keys
What is WPA2?
WEP vs. WPA vs. WPA2
WEP Issues
Weak Initialization Vectors (IV)
How to Break WEP Encryption?
How to Break WPA/WPA2 Encryption?
How to Defend Against WPA Cracking?
Wireless Threats: Access Control Attacks
Wireless Threats: Integrity Attacks
Wireless Threats: Confidentiality Attacks
Wireless Threats: Availability Attacks
Wireless Threats: Authentication Attacks
Rogue Access Point Attack
Client Mis-association
Misconfigured Access Point Attack
Unauthorized Association
Ad Hoc Connection Attack
HoneySpot Access Point Attack
AP MAC Spoofing
Denial-of-Service Attack
Jamming Signal Attack
Wi-Fi Jamming Devices
Wireless Hacking Methodology
Find Wi-Fi Networks to Attack
Attackers Scanning for Wi-Fi Networks
Footprint the Wireless Network
Wi-Fi Discovery Tool: inSSIDer
Wi-Fi Discovery Tool: NetSurveyor
Wi-Fi Discovery Tool: NetStumbler
Wi-Fi Discovery Tool: Vistumbler

Wi-Fi Discovery Tool: WirelessMon
Wi-Fi Discovery Tools
GPS Mapping
How to Discover Wi-Fi Network Using Wardriving?
Wireless Traffic Analysis
Wireless Cards and Chipsets
Wi-Fi USB Dongle: AirPcap
Wi-Fi Packet Sniffer: Wireshark with AirPcap
Wi-Fi Packet Sniffer: Wi-Fi Pilot
Wi-Fi Packet Sniffer: OmniPeek
Wi-Fi Packet Sniffer: CommView for Wi-Fi
What is Spectrum Analysis?
Wireless Sniffers
Aircrack-ng Suite
How to Reveal Hidden SSIDs
Fragmentation Attack
How to Launch MAC Spoofing Attack?
Denial of Service: Deauthentication and Disassociation Attacks
Man-in-the-Middle Attack
MITM Attack Using Aircrack-ng
Wireless ARP Poisoning Attack
Rogue Access Point
Evil Twin
How to Crack WEP Using Aircrack?
How to Crack WEP Using Aircrack? Screenshot 1/2
How to Crack WEP Using Aircrack? Screenshot 2/2
How to Crack WPA-PSK Using Aircrack?
WPA Cracking Tool: KisMAC
WEP Cracking Using Cain & Abel
WPA Brute Forcing Using Cain & Abel
WPA Cracking Tool: Elcomsoft Wireless Security Auditor
WEP/WPA Cracking Tools
Wi-Fi Sniffer: Kismet
Wardriving Tools
RF Monitoring Tools
Wi-Fi Connection Manager Tools
Wi-Fi Traffic Analyzer Tools
Wi-Fi Raw Packet Capturing Tools
Wi-Fi Spectrum Analyzing Tools
Bluetooth Hacking
How to BlueJack a Victim?
Bluetooth Hacking Tool: Super Bluetooth Hack
Bluetooth Hacking Tool: PhoneSnoop
Bluetooth Hacking Tool: BlueScanner
How to Defend Against Bluetooth Hacking?
How to Detect and Block Rogue AP?
Wireless Security Layers
How to Defend Against Wireless Attacks?

Wireless Intrusion Prevention Systems
Wireless IPS Deployment
Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
Wi-Fi Security Auditing Tool: AirDefense
Wi-Fi Security Auditing Tool: Adaptive Wireless IPS
Wi-Fi Security Auditing Tool: Aruba RFPProtect WIPS
Wi-Fi Intrusion Prevention System
Wi-Fi Predictive Planning Tools
Wi-Fi Vulnerability Scanning Tools
Wireless Penetration Testing

Module 16: Evading IDS, Firewalls, and Honeypots

Intrusion Detection Systems (IDS) and its Placement
How IDS Works?
Ways to Detect an Intrusion
Types of Intrusion Detection Systems
System Integrity Verifiers (SIV)
General Indications of Intrusions
General Indications of System Intrusions
Firewall
DeMilitarized Zone (DMZ)
Types of Firewall
Firewall Identification
Honeypot
How to Set Up a Honeypot?
Intrusion Detection Tool
Intrusion Detection Systems: Tipping Point
Firewall: Sunbelt Personal Firewall
Honeypot Tools
Insertion Attack
Evasion
Denial-of-Service Attack (DoS)
Obfuscating
False Positive Generation
Session Splicing
Unicode Evasion Technique
Fragmentation Attack
Overlapping Fragments

Time-To-Live Attacks
Invalid RST Packets
Urgency Flag
Polymorphic Shellcode
ASCII Shellcode
Application-Layer Attacks
Desynchronization
Pre Connection SYN
Post Connection SYN
Other Types of Evasion
Bypass Blocked Sites Using IP Address in Place of URL
Bypass a Firewall using Proxy Server
Detecting Honeypots
HoneyPot Detecting Tool: Send-Safe
HoneyPot Hunter
Firewall Evasion Tools
Packet Fragment Generators
Countermeasures
Firewall/IDS Penetration Testing

Module 17: Buffer Overflow

Buffer Overflows
Why are Programs And Applications Vulnerable?
Understanding Stacks
Stack-Based Buffer Overflow
Understanding Heap
Stack Operations
Knowledge Required to Program Buffer Overflow Exploits
Buffer Overflow Steps
Simple Uncontrolled Overflow
Simple Buffer Overflow in C
Code Analysis
Exploiting Semantic Comments in C (Annotations)
How to Mutate a Buffer Overflow Exploit?
Identifying Buffer Overflows
How to Detect Buffer Overflows in a Program?
BOU (Buffer Overflow Utility)
Testing for Heap Overflow Conditions: heap.exe
Steps for Testing for Stack Overflow in OllyDbg Debugger
Testing for Format String Conditions using IDA Pro
BoF Detection Tools
Defense Against Buffer Overflows
Data Execution Prevention (DEP)
Enhanced Mitigation Experience Toolkit (EMET)
/GS http://microsoft.com
BoF Security Tools
Buffer Overflow Penetration Testing

Module 18: Cryptography

Cryptography
Types of Cryptography
Government Access to Keys (GAK)
Ciphers
Advanced Encryption Standard (AES)
Data Encryption Standard (DES)
RC4, RC5, RC6 Algorithms
The DSA and Related Signature Schemes
RSA (Rivest Shamir Adleman)
Message Digest (One-way Bash) Functions
Secure Hashing Algorithm (SHA)
What is SSH (Secure Shell)?
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
Cryptography Tool: Advanced Encryption Package
Cryptography Tools
Public Key Infrastructure (PKI)
Certification Authorities
Digital Signature
SSL (Secure Sockets Layer)
Transport Layer Security (TLS)
Disk Encryption
Cryptography Attacks
Code Breaking Methodologies
Meet-in-the-Middle Attack on Digital Signature Schemes
Cryptanalysis Tool: CrypTool
Cryptanalysis Tools
Online MD5 Decryption Tool

Module 19: Penetration Testing

Introduction to Penetration Testing
Security Assessments
Vulnerability Assessment
Penetration Testing
Why Penetration Testing?
What Should be Tested?
What Makes a Good Penetration Test?
ROI on Penetration Testing
Testing Points
Testing Locations
Types of Penetration Testing

Common Penetration Testing Techniques
Using DNS Domain Name and IP Address Information
Enumerating Information about Hosts on Publicly-Available Networks
Phases of Penetration Testing
Penetration Testing Methodology
Outsourcing Penetration Testing Services
Evaluating Different Types of Pentest Tools
Application Security Assessment Tool
Network Security Assessment Tool
Wireless/Remote Access Assessment Tool
Telephony Security Assessment Tool
Testing Network-Filtering Device Tool

Course Description:

The Wireless LAN Administration course provides the networking professional a complete foundation of knowledge for entering into or advancing in the wireless networking industry. From basic RF theory to 802.11 frame exchange processes, this course delivers hands on training that will benefit the novice as well as the experienced network professional.

Who Should Attend:

This course is for novice as well as experienced networking professionals.

Prerequisites:

Students should have basic networking knowledge, including OSI model and IP subnetting.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Enter into or advance in the wireless networking industry.

Course Outline:**Introduction to 802.11 WLANs**

Discuss the standards organizations responsible for shaping the 802.11 Wireless LAN protocol

Learn how standards compliance is enforced for 802.11 WLAN vendors

Examine the 802.11 standard and various amendments

Discuss additional networking standards that are commonly used to enhance 802.11 WLANs

Radio Frequency Fundamentals

Physical aspects of RF propagation

Types of losses and attenuation that affect RF communications

Types of modulation used for wireless communications

How channels and bandwidth are related to each other in wireless networks

Three types of Spread Spectrum used in wireless networking

RF Math and System Operating Margin

RF units of measure

Basic RF mathematics

RF signal measurements

Understand link budgets

Define and calculate System Operating Margin (SOM)

802.11 Service Sets

Explain three types of service sets defined for use within 802.11 WLANs

Roaming within a WLAN

Load-balancing as a method to improve congestion in WLANs

RF Power Output Regulations

Understand international, regional, and local RF spectrum management organizations

Understand RF channels in the unlicensed 2.4 GHz and 5 GHz frequency ranges

How power output limitations are enforced by the FCC for Point-to-Multipoint (PtMP) and Point-to-Point (PtP) wireless connections

Power over Ethernet

Recognize the two types of devices used in Power over Ethernet (PoE)

Recognize the differences between the two types of Power Sourcing Equipment (PSE)

Understand the two ways in which power can be delivered using PoE

Understand the importance of planning to maximize the efficiency of Power over Ethernet

Wireless LAN Operation

Ad Hoc networks

Infrastructure networks

Bridged networks

Repeater networks

Mesh networks

WLAN switched networks

Enterprise Wireless Gateway networks

Enterprise Encryption Gateway networks

Virtual AP networks

Evolution of WLAN architectures

WLAN Management

WLAN Security

Security Policy and Procedures

Legacy 802.11 Security Components

802.11i Security Components

WPA-Personal

WPA-Enterprise

WPA2-Personal

WPA2-Enterprise

Baseline Security Practices (SOHO, SMB, Enterprise)

802.11 Analysis and Troubleshooting

Introduction to 802.11 Protocol Analysis

802.11 Data Frames

802.11 Control Frames

802.11 Management Frames

Frame Fragmentation

Power Saving operations

Transmission Rates

Coordinating 802.11 Frame Transmissions

Differences between CSMA/CD and CSMA/CA

Distributed Coordination Function (DCF)

Quality of Service in 802.11 WLANs

Antennas

Antenna characteristics and behaviors

Types of antennas commonly used with WLANs

Advanced antenna systems

Antenna placement and mounting

Antenna safety

Types of antenna cables, connectors, and accessories

Site Surveying

Understanding the need for a site survey

Defining business requirements and justification

Facility analysis

Interviewing network management and users

Identifying bandwidth requirements

Determining contours of RF coverage

Documenting installation problems

Locating interference

Reporting methodology and procedures

Understanding specifics of each vertical market

Understanding the customer's network topology

Creating appropriate documentation during and after the site survey

Understanding safety hazards

Using appropriate hardware and software to perform the survey

Understanding the need for spectrum analysis

Manual RF site surveys

Predictive site surveys

Dense AP deployment

Course Description:

The Wireless LAN Security course consists of hands on learning using the latest enterprise wireless LAN security and auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with wireless LANs today, and every class and type of WLAN security solution available on the market - from wireless intrusion prevention systems to wireless network management systems.

Who Should Attend:

This class is for those who want to learn the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with wireless LANs today, and every class and type of WLAN security solution available on the market - from wireless intrusion prevention systems to wireless network management systems.

Prerequisites:

Students should have basic wireless LAN literacy.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Implement and manage wireless security in the enterprise by creating layer2 and layer3 hardware and software solutions.

Course Outline:**Introduction to WLAN Security Technology**

Security policy
Security concerns
Security auditing practices
Application layer vulnerabilities and analysis
Data Link layer vulnerabilities and analysis
Physical layer vulnerabilities and analysis
802.11 security mechanisms
Wi-Fi Alliance security certifications

802.1X/EAP types and differences
802.11 handshakes
Fast BSS Transition (FT) technologies

Small Office / Home Office WLAN Security Technology and Solutions

WLAN discovery equipment and utilities.
Legacy WLAN security methods, mechanisms, and exploits
Appropriate SOHO security

WLAN Mobile Endpoint Security Solutions

Personal-class mobile endpoint security
Enterprise-class mobile endpoint security
User-accessible and restricted endpoint policies
VPN technology overview

Branch Office / Remote Office WLAN Security Technology and Solutions

General vulnerabilities
Preshared Key security with RSN cipher suites
Passphrase vulnerabilities
Passphrase entropy and hacking tools
WPA/WPA2 Personal - how it works
WPA/WPA2 Personal - configuration
Wi-Fi Protected Setup (WPS)
Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices

Enterprise WLAN Management and Monitoring

Device identification and tracking
Rogue device mitigation
WLAN forensics
Enterprise WIPS installation and configuration
Distributed protocol analysis
WNMS security features
WLAN controller security feature sets

Enterprise WLAN Security Technology and Solutions

Robust Security Networks (RSN)
WPA/WPA2 Enterprise - how it works
WPA/WPA2 Enterprise - configuration
IEEE 802.11 Authentication and Key Management (AKM)
802.11 cipher suites
Use of authentication services (RADIUS, LDAP) in WLANs
User profile management (RBAC)
Public Key Infrastructures (PKI) used with WLANs
Certificate Authorities and x.509 digital certificates
RADIUS installation and configuration
802.1X/EAP authentication mechanisms

Course Description:

This course trains students in all areas of the security Common Body of Knowledge. They will learn security policy development, secure software development procedures, network vulnerabilities, attack types and corresponding countermeasures, cryptography concepts and their uses, disaster recovery plans and procedures, risk analysis, crucial laws and regulations, forensics basics, computer crime investigation procedures, physical security, and more.

There are four processes a candidate must successfully complete to become a certified CISSP. To sit for an exam, a candidate must assert that he or she possesses a minimum of five years of professional experience in the information security field or four years of experience plus a college degree. Professional experience has to be in two or more of these 10 (ISC)² CISSP domains: Access Control, Application Development Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security Governance and Risk Management, Legal, Regulations, Investigations and Compliance, Operations Security, Physical (Environmental) Security, Security Architecture and Design, and Telecommunications and Network Security.

Who Should Attend:

Students who wish to pass the CISSP certification exam will benefit from this class.

Prerequisites:

There are no prerequisites for this course, although having taken other security courses is extremely helpful.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Confidently meet the challenge of CISSP certification exam

Course Outline:**Access Control Systems and Methodologies**

Access control concepts, methodologies, and implementation
Access controls: detective, corrective, and preventative
Access control techniques in centralized and decentralized environments
Access control risks, vulnerabilities, and exposures

Security Architecture and Models

Secure operating system principles, concepts, mechanisms, controls, and standards
Secure architecture design, modeling, and protection
Security models: confidentiality, integrity, and information flow
Government and commercial security requirements
Common criteria, ITSEC, TCSEC, IETF, IPSEC
Technical platforms
System security preventative, detective, and corrective measures

Disaster Recovery and Business Continuity Planning

Business continuity planning, business impact analysis, recovery strategies, recovery plan development, and implementation
Disaster recovery planning, implementation, and restoration
Compare and contrast disaster recovery and business continuity

Security Management Practices

Organizational security roles
Identification of information assets
Security management planning
Security policy development; use of guidelines, standards, and procedures
Security awareness training
Data classification and marking
Employment agreements and practices
Risk management tools and techniques

Law, Investigation, and Ethics

Computer crime detection methods
Applicable computer crime, security, and privacy laws
Evidence gathering and preservation methods
Computer crime investigation methods and techniques
Civil, criminal, and investigative law
Intellectual property law
ISC2 and IAB ethics application

Physical Security

Prevention, detection, and correction of physical hazards
Secure site design, configuration, and selection elements
Access control and protection methods for facility, information, equipment, and personnel

Operations Security

Resource protection mechanisms and techniques
Operation security principles, techniques, and mechanisms; principles of good practice and limitation of abuses

Operations security preventative, detective, and corrective measures
Information attacks
Access Control Subversion

Cryptography

Cryptographic concepts, methods, and practices
Construction of algorithms
Attacks on cryptosystems
Ancient cryptography and modern methods
Public and private key algorithms and uses
Key distribution and key management
Digital signature construction and use
Methods of attack, strength of function

Telecommunications and Network Security

Overview of communications and network security
Voice communications, data communications, local area, wide area, and remote access
Internet/Intranet/Extranet, firewalls, routers, and network protocols
Telecommunication and network security preventative, detective, and corrective measures
System development process and security controls
System development life cycle, change controls, application controls, and system and application integrity
Database structure, concepts, design techniques, and security implications
Object oriented programming
Data warehousing and data mining

Review and Q&A Session

Review concepts introduced in previous sessions
Answer specific questions or concerns regarding CISSP preparation material

Testing-Taking Tips and Study Techniques

Tips for additional preparation for the CISSP exam
Additional resources
Techniques for scoring well on the exam

Course Description:

This course is designed to prepare (ISC)2 CISSP-certification holders for the Information Systems Security Engineering Professional (ISSEP) exam. (ISC)2 created the CISSP-ISSEP engineering-specific concentration in conjunction with the U.S. National Security Agency (NSA) providing an invaluable tool for any systems security engineering professional. CISSP-ISSEP is the guide for incorporating security into projects, applications, business processes, and all information systems. The course guides students to understand the CISSP-ISSEP Common Body of Knowledge (CBK) by comparing it to a traditional Systems Engineering model, enabling you to see the correlation of how security fits into the design and development process for information systems. The course also introduces key points of more than 50 U.S. government policies and procedures that need to be understood in order to understand the CBK and protect U.S. government information.

Who Should Attend:

This course is designed to prepare (ISC)2 CISSP-certification holders for the Information Systems Security Engineering Professional (ISSEP) exam.

Prerequisites:

Students must be ISSEP candidates.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Employ Information Assurance Technical Framework (IATF) processes to discover users' information protection needs and design systems that will effectively and efficiently address those needs.
- Understand the concepts of defense in depth, risk assessment, and the systems lifecycle.
- Describe system development models and relate security tasks to these models.
- Identify, understand, and implement the Certification and Accreditation (C+A) processes.
- Identify, understand, and apply the practices as defined by the United States Government Information Assurance regulations.
- Demonstrate his or her knowledge of the standards and regulations pertaining to systems security engineering, certification and accreditation, information assurance, and technical management.
- Demonstrate his or her knowledge of the four domains of the CISSP-ISSEP CBK through various scenarios and models
- Create a study plan to successfully pass the CISSP-ISSEP Examination

Course Outline:**Systems Security Engineering**

Employing Information Assurance Technical Framework (IATF) processes to discover users' information protection needs
Designing systems to effectively and efficiently address needs
Concepts of defense in depth, risk assessment, and the systems lifecycle

Technical Management

System development models
Relating security tasks to models

Certification and Accreditation Module Goal

Identifying, understanding, and implementing the Certification and Accreditation (C+A) processes

United States Government Information Assurance (IA) Regulations Module

identifying, understanding, and applying the practices as defined by the United States Government Information Assurance regulations

Course Description:

Malware, short for malicious software, is code designed to infiltrate and exploit a computer system or network without consent. This course provides students with a comprehensive study of the many types of Malware and their functions. The course stresses types of malware, global effects, Malware analysis and Incidence Response Plans. Lab exercises reinforce the lectures.

Who Should Attend:

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.

Prerequisites:

Students should have a basic understanding of Windows/ Linux operating systems, TCP/IP, and network security.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify, classify, and organize malware
- Identify and correlate information regarding domains, hostnames, and IP addresses
- Analyze JavaScript, PDs, Office documents, and packet captures for signs of malicious activity
- Automate the execution of malware in VMware or VirtualBox virtual machines
- Build your own API monitor
- Detect rootkits and stealth malware using forensic tools
- Scan the file system and Registry for hidden data and bypass locked file restrictions and remove stubborn malware
- Use a debugger to analyze, control, and manipulate a malware sample's behaviors
- Create debugger plug-ins that monitor API calls, output HTML behavior reports, and automatically highlight suspicious activity
- Decode, decrypt, and unpack data that attackers intentionally try to hide
- Crack domain generation algorithms
- Analyze malware distributed as Dynamic Link Libraries (DLLs)
- Debug the kernel of a virtual machine infected with malware to understand its low-level functionality
- Create scripts for WinDbg, unpack kernel drivers, and leverage IDA Pro's debugger plug-ins
- Acquire memory samples from physical and virtual machines
- Install the Volatility advanced memory forensics platform and associated plug-ins
- Detect and extract code hiding in process memory
- Rebuild binaries, including user mode programs and kernel drivers, from memory samples

Course Outline:**Anonymizing Your Activities**

Conducting online investigations without exposing your own identity

Honeypots

Using honeypots to collect the malware being distributed by bots and worms
Grabbing new variants of malware families from the wild, sharing them in real time with other researchers, analyzing attack patterns, or building a workflow to automatically analyze the samples

Malware Classification

Identifying, classifying, and organizing malware
Detecting malicious files using custom anti-virus signatures
Determining the relationship between samples
Determining exactly what functionality attackers may have introduced into a new variant

Sandboxes and Multi-AV Scanners

Leveraging online virus scanners and public sandboxes
Using scripts to control the behavior of your sample in the target sandbox
Submitting samples on command line with Python scripts

Storing results to a database
Scanning for malicious artifacts based on sandbox results

Researching Domains and IP Addresses

Identifying and correlating information regarding domains, hostnames, and IP addresses
Tracking fast flux domains
Determining the alleged owner of a domain
Locating other systems owned by the same group of attackers
Creating static or interactive maps based on the geographical location of IP addresses

Documents, Shellcode, and URLs

Analyzing JavaScript, PDs, Office documents, and packet captures for signs of malicious activity
Extracting shellcode from exploits and analyzing it within a debugger or in an emulated environment

Malware Labs

Building a safe, flexible, and inexpensive lab in which to execute and monitor malicious code
Solutions involving virtual or physical machines and using real or simulated Internet

Automation

Automating the execution of

malware in VMware or VirtualBox virtual machines
Creating custom reports about the malware's behavior, including network traffic logs and artifacts created in physical memory

Dynamic Analysis

Building your own API monitor, Preventing certain evidence from being destroyed
Logging file system and Registry activity in real time without using hooks
Comparing changes to a process's handle table
Logging commands that attackers send through backdoors

Malware Forensics

Scanning the file system and Registry for hidden data
Bypassing locked file restrictions and removing stubborn malware
Detecting HTML injection and investigating a new form of Registry "slack" space

Debugging Malware

Using a debugger to analyze, control, and manipulate a malware sample's behaviors
Creating debugger plug-ins that monitor API calls, output HTML behavior reports, and automatically highlight suspicious activity

De-obfuscation

Reverse-engineering a malware sample that encrypts its network traffic
Techniques to crack domain generation algorithms

Working with DLLs

Enumerating and examining a DLL's exported functions
Running the DLL in a process of your choice (and bypass host process restrictions)
Executing DLLs as a Windows service
Converting DLLs to standalone executables

Kernel Debugging

Debugging the kernel of a virtual machine infected with malware
Creating scripts for WinDbg
Unpacking kernel drivers
Leveraging IDA Pro's debugger plug-ins

Memory Forensics with Volatility

Acquiring memory samples from physical and virtual machines
Installing the Volatility advanced memory forensics platform and associated plug-ins
Beginning your analysis by detecting process context tricks and DKOM attacks

Memory Forensics: Code Injection and Extraction

Detecting and extracting code (unlinked DLLs, shellcode, and so on) hiding in process memory
Rebuilding binaries, including user mode programs and kernel drivers
Rebuilding the import address tables (IAT) of packed malware based on information in the memory dump

Memory Forensics: Rootkits

Detecting various forms of rootkit activity, including the presence of IAT, EAT, Inline, driver IRP, IDT, and SSDT hooks on a system
Identifying malware that hides in kernel memory without a loaded driver
Locating system-wide notification routines
Detecting attempts to hide running Windows services

Network and Registry

Exploring the artifacts created on a system due to a malware sample's network activity
Detecting active connections, listening sockets, and the use of raw sockets and promiscuous mode network cards
Extracting volatile Registry Keys and values from memory

Course Description:

ECSA/LPT is a security class like no other! Providing real world hands on experience, it is the only in-depth Advanced Hacking and Penetration Testing class available that covers testing in all modern infrastructures, operating systems and application environments.

EC-Council's Certified Security Analyst/LPT program is a highly interactive 5-day security class designed to teach Security Professionals the advanced uses of the LPT methodologies, tools and techniques required to perform comprehensive information security tests. Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the tools and ground breaking techniques for security and penetration testing, this class will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure. As students learn to identify security problems, they also learn how to avoid and eliminate them, with the class providing complete coverage of analysis and network security-testing topics.

Who Should Attend:

This course is for Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Prerequisites:**Benefits of Attendance:**

Upon completion of this course, students will be able to:

- Design, secure and test networks to protect organizations from the threats hackers and crackers pose.
- Perform the intensive assessments required to effectively identify and mitigate risks to the security of infrastructures.
- Identify security problems, and know how to avoid and eliminate them.

Course Outline:

Module 1: The Need for Security Analysis

Module 2: Advanced Googling

Module 3: TCP/IP Packet Analysis

Module 4: Advanced Sniffing Techniques

Module 5: Vulnerability Analysis with Nessus

Module 6: Advanced Wireless Testing

Module 7: Designing a DMZ

Module 8: Snort Analysis

Module 9: Log Analysis

Module 10: Advanced Exploits and Tools

Module 11: Penetration Testing Methodologies

Module 12: Customers and Legal Agreements

Module 13: Rules of Engagement

Module 14: Penetration Testing Planning and Scheduling

Module 15: Pre Penetration Testing Checklist

Module 16: Information Gathering

Module 17: Vulnerability Analysis

Module 18: External Penetration Testing

Module 19: Internal Network Penetration Testing

Module 20: Routers and Switches Penetration Testing

Module 21: Firewall Penetration Testing

Module 22: IDS Penetration Testing

Module 23: Wireless Network Penetration Testing

Module 24: Denial of Service Penetration Testing

Module 25: Password Cracking Penetration Testing

Module 26: Social Engineering Penetration Testing

Module 27: Stolen Laptop, PDAs and Cell phones Penetration Testing

Module 28: Application Penetration Testing

Module 29: Physical Security Penetration Testing

Module 30: Database Penetration testing

Module 31: VoIP Penetration Testing

Module 32: VPN Penetration Testing

Module 33: War Dialing

Module 34: Virus and Trojan Detection

Module 35: Log Management Penetration Testing

Module 36: File Integrity Checking

Module 37: Blue Tooth and Handheld Device Penetration Testing

Module 38: Telecommunication and Broadband Communication Penetration Testing

Module 39: Email Security Penetration Testing

Module 40: Security Patches Penetration Testing

Module 41: Data Leakage Penetration Testing

Module 42: Penetration Testing Deliverables and Conclusion

Module 43: Penetration Testing Report and Documentation Writing

Module 44: Penetration Testing Report Analysis

Module 45: Post Testing Actions

Module 46: Ethics of a Licensed Penetration Tester

Module 47: Standards and Compliance

Course Description:

This class will immerse the student in an interactive environment where they will be shown how to scan, test, hack, and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. When a student leaves this intensive 5-day class, they will have hands on understanding and experience in Ethical Hacking. This course prepares you for CNDA exam 312-99.

Who Should Attend:

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites:

Students should have experience working with network infrastructures.

Course Outline:

Module 1: Introduction to Ethical Hacking

Module 2: Hacking Laws

Module 3: Footprinting

Module 4: Google Hacking

Module 5: Scanning

Module 6: Enumeration

Module 7: System Hacking

Module 8: Trojans and Backdoors

Module 9: Viruses and Worms

Module 10: Sniffers

Module 11: Social Engineering

Module 12: Phishing

Module 13: Hacking Email Accounts

Module 14: Denial-of-Service

Module 15: Session Hijacking

Module 16: Hacking Web Servers

Module 17: Web Application Vulnerabilities

Module 18: Web-Based Password Cracking Techniques

Module 19: SQL Injection

Module 20: Hacking Wireless Networks

Module 21: Physical Security

Module 22: Linux Hacking

Module 23: Evading IDS, Firewalls and Detecting Honey Pots

Module 24: Buffer Overflows

Module 25: Cryptography

Module 26: Penetration Testing

Module 27: Covert Hacking

Module 28: Writing Virus Codes

Module 29: Assembly Language Tutorial

Module 30: Exploit Writing

Module 31: Smashing the Stack for Fun and Profit

Module 32: Windows Based Buffer Overflow Exploit Writing

Module 33: Reverse Engineering

Module 34: MAC OS X Hacking

Module 35: Hacking Routers, cable Modems and Firewalls

Module 36: Hacking Mobile Phones, PDA and Handheld Devices

Module 37: Bluetooth Hacking

Module 38: VoIP Hacking

Module 39: RFID Hacking

Module 40: Spamming

Module 41: Hacking USB Devices

Module 42: Hacking Database Servers

Module 43: Cyber Warfare- Hacking, Al-Qaida and Terrorism

Module 44: Internet Content Filtering Techniques

Module 45: Privacy on the Internet

Module 46: Securing Laptop Computers

Module 47: Spying Technologies

Module 48: Corporate Espionage- Hacking Using Insiders

Module 49: Creating Security Policies

Module 50: Software Piracy and Warez

Module 51: Hacking and Cheating Online Games

Module 52: Hacking RSS and Atom

Module 53: Hacking Web Browsers (Firefox, IE)

Module 54: Proxy Server Technologies

Module 55: Data Loss Prevention

Module 56: Hacking Global Positioning System (GPS)

Module 57: Computer Forensics and Incident Handling

Module 58: Credit Card Frauds

Module 59: How to Steal Passwords

Module 60: Firewall Technologies

Module 61: Threats and Countermeasures

Module 62: Case Studies

Module 63: Botnets

Module 64: Economic Espionage

Module 65: Patch Management

Module 66: Security Convergence

Module 67: Identifying the Terrorist

Course Description:

This course will give students the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware, and specialized techniques.

Who Should Attend:

This course is for police and other law enforcement personnel, Defense and Military personnel, e-Business Security professionals, Systems administrators, Legal professionals, Banking, Insurance and other professionals, Government agencies, and IT managers.

Prerequisites:

It is strongly recommended that students attend the CEH class before enrolling into CHFI program.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify an intruder's footprints and properly gather the necessary evidence to prosecute.

Course Outline:**Today's Computer Forensics**

Ways of Forensic Data Collection
Objectives of Computer Forensics
Benefits of Forensic Readiness
Categories of Forensics Data
Computer Facilitated Crimes
Tracking Cyber Criminals
Key Steps in Forensics Investigations
Need for Forensic Investigator
Advocates Contacting the Forensic Investigator
Enterprise Theory of Investigation
When do you use Computer Forensics
Legal Issues
Reporting the Results

Law & Computer Forensics

Privacy Issues in Investigations
Fourth Amendment Definition
Interpol- IT Crime Center
Internet Laws and Statutes
Intellectual Property Rights
Cyber Stalking
Crime Investigating Organizations
Principles to Combat High-tech Crime
Laws in Other Countries
Internet Crime Schemes

Computer Investigation Process

Securing the Computer Evidence
Preparation for Searches
Chain-of Evidence Form
Accessing the Policy Violation Case
Preparing for an Investigation
Investigation Process
Maintaining Professional Conduct

First Responder Procedure

Electronic Evidence
The Forensic Process
Types of Electronic Devices
Evidence Collecting Tools
First Response Rule
Incident Response: Different Situations
Securing and Evaluating Electronic Crime Scene
Health and Safety Issues
Consent
Planning the Search and Seizure
'Chain of Custody'
Findings of Forensic Examination by Crime Category

CSIRT

How to Prevent an Incident?
Relationship between Incident Response, Handling, and Management
Incident Response Checklist
Incident Management
Why Don't Organizations Report Computer Crimes?
Estimating Cost of an Incident
Vulnerability Resources
Category of Incidents
CSIRT: Goals and Strategy
World CERTs
IRTs Around the World

Computer Forensic Lab

Ergonomics
Forensic Laboratory Requirements
Portable Systems and Towers
Write Protection Devices and Kits
Power Supplies and Switches
DIBS® Mobile Forensic Workstation
Forensic Archive and Restore Robotic Devices
Forensic Workstations
Tools: LiveWire Investigator
Laboratory Imaging System
Computer Forensic Labs, Inc
Data Destruction Industry Standards

File Systems & Hard Disks

Types of Hard Disk Interfaces
EFS Key
FAT vs. NTFS
Windows Boot Process (XP/2003)

Digital Media Devices

Digital Storage Devices
Magnetic Tape
Floppy and Compact Disk
CD-ROM and DVD
Blu-Ray
CD Vs DVD Vs Blu-Ray
HD-DVD vs. Blu-Ray
iPod and Zune
Flash Memory Cards
USB Flash Drives

Boot Processes

Terminologies
Boot Loader and Sector
Anatomy of MBR
Basic System Boot Process
MS-DOS Boot Process
Windows XP Boot Process
Common Startup Files in UNIX
Important Directories in UNIX
Linux Boot Process
Macintosh Forensic Software by BlackBag
Carbon Copy Cloner (CCC)
MacDrive6

Windows Forensics

Windows Forensics Tool: Helix
MD5 Generator: Chaos MD5
Registry Viewer Tool: RegScanner
Virtual Memory
System Scanner
X-Ways Forensics
Tool: Traces Viewer
Investigating ADS Streams

Linux Forensics

File System Description
Mount Command
Popular Linux Forensics Tools

Data Acquisition and Duplication

Mount Image Pro
Snapshot Tool
Snapback DatArrest
Image MASSter Solo-3 Forensic
Save-N-Sync
ImageMASSter 6007SAS and Disk Jockey IT
SCSI/PAK
IBM DFMSDss
QuickCopy

Computer Forensic Tools

Software Forensics Tools
Hardware Forensics Tools

Investigations Using Encase

Evidence File
Verifying File Integrity
Hashing
Acquiring Image
Configuring Encase
Viewers in Bottom Pane
Searching
Keywords and Bookmarks
Starting the Search
Recovering Deletions in FAT Partition
Master Boot Record
NTFS Starting Point
Viewing Disk Geometry
Recovering Deleted Partitions
Hash Values
Viewers
Signature Analysis
Viewing the Results
Copying Files Folders
E-mail Recovery
Reporting
Encase Boot Disks
IE Cache Images

Recovering Deleted Files and Deleted Partitions

Deleting Files
What happens when a File is Deleted in Windows?
Storage Locations of Recycle Bin in FAT and NTFS System
How The Recycle Bin Works
Damaged or Deleted INFO File
Damaged Files in Recycled Folder
Damaged Recycle Folder
Tools to Recover Deleted Files
Deletion of Partition
Recovery of Deleted Partition
Deleted Partition Recovery Tools

Image Files Forensics

Understanding Image File Formats
How File Compression Works
Huffman Coding Algorithm
Lempel-Ziv Coding Algorithm
Vector Quantization
Picture Viewer: AD and Max
FastStone Image Viewer
XnView
Faces - Sketch Software
Steganalysis
GFE Stealth (Graphics File Extractor)

Steganography

Classification of Steganography
Steganography vs. Cryptography
Steganography Tools
Application of Steganography
How to Detect Steganography?

Application Password Crackers

Brute Force Attack
Dictionary Attack
Syllable Attack/Rule-based
Attack/Hybrid Attack
Password Guessing
Rainbow Attack
CMOS Level Password Cracking
Pdf Password Crackers
Password Cracking Tools

Common Recommendations for Improving Password Security
Standard Password Advice

Network Forensics and Investigating Logs

Looking for Evidence
Log Files as Evidence
Records of Regularly Conducted Activity
Legality of Using Logs
Maintaining Credible IIS Log Files
Log File Accuracy
Log Everything
Keeping Time
Use Multiple Logs as Evidence
Avoid Missing Logs
Log File Authenticity
Work with Copies
Access Control
Chain of Custody
Importance of Audit Logs
Why Synchronize Computer Times?
What is NTP Protocol?
NIST Time Servers
Configuring the Windows Time Service

Network Traffic

Network Addressing Schemes
Tool: Tcpdump
CommView
Softperfect Network Sniffer
HTTP Sniffer
EtherDetect Packet Sniffer
OmniPeek
Iris Network Traffic Analyzer
SmartSniff
NetSetMan Tool
Evidence Gathering at the Data-link Layer: DHCP database
DHCP Log
Siemens Monitoring Center
Netsurfer Tool
eTrust Network Forensics
IDS Policy Manager
<http://www.activeworx.org>

Wireless Attacks

Association of Wireless AP and Device
Search Warrant for Wireless Networks
Key Points to Remember
Testing the Wireless Network
Methods to Access a Wireless Access Point
Aircrack: Points to Note
Searching for Additional Devices
Forcing Associated Devices to Reconnect
Check for MAC Filtering
Passive Attack
Active Attacks on Wireless Networks

Web Attacks

Types of Web Attacks
Example of FTP Compromise
Acunetix Web Vulnerability Scanner
Intrusion Detection
CounterStorm-1: Defense against Known, Zero Day and Targeted Attacks

Router Forensics

Routing Information Protocol

Hacking Routers
Router Attack Topology
Recording your Session
Router Logs
NETGEAR Router Logs
Link Logger
Sawmill: Linksys Router Log Analyzer
Real Time Forensics
Router Audit Tool (RAT)

DoS Attacks

Types of DoS Attacks
DDoS Attack
DoS Attack Modes
Indications of a DoS/DDoS Attack
Techniques to Detect DoS Attack
Challenges in the Detection of DoS Attack

Internet Crimes

Internet Crimes and Forensics
IP Address
Domain Name System (DNS)
Email Headers
Switch URL Redirection
Recovering Information from Web Pages
HTTP Headers
Examining Information in Cookies
Tracing Geographical Location of a URL: www.centralops.net
NetScanTools Pro
Tool: Proxy <http://www.privoxy.org>

E-mails and E-mail Crimes

Client and Server in E-mail
E-mail Client and Server
Real E-mail System
Received: Headers
Forging Headers
List of Common Headers
Exchange Message Tracking Center
MailDetective Tool
U.S. Laws Against Email Crime
Email crime law in Washington

Corporate Espionage

Motives
Information that Corporate Spies Seek
Corporate Espionage:
Insider/Outsider Threat
Techniques of Spying
Defense Against Corporate Spying
Netspionage
Investigating Corporate Espionage Cases
Employee Monitoring: Activity Monitor
Spy Tool: SpyBuddy

Trademark & Copyright Infringement

Characteristics of Trademarks
Copyright
Copyright Infringement: Plagiarism
Investigating Intellectual Property
US Laws for Trademarks and Copyright
Laws for Trademarks and Copyright in Other Countries

Sexual Harassment

Types of Sexual Harassment
Consequences of Sexual Harassment
Responsibilities of Supervisors
Responsibilities of Employees

Complaint Procedures
Investigation Process
Sexual Harassment Investigations
Sexual Harassment Policy
Preventive Steps
U.S Laws on Sexual Harassment

Investigating Child Pornography

Motive Behind Child Pornography
People Involved in Child Pornography
Role of Internet in Child Pornography
Preventing Dissemination
Controlling Child Pornography
Guidelines for Investigating Cases
Sources of Digital Evidence
Tools to Protect Children
Innocent Images National Initiative
Internet Crimes Against Children (ICAC)
Reports on Child Pornography
U.S. Laws against Child Pornography
Laws in Other Countries

PDA and iPod Forensics

PDA Forensics Steps
iPod
Apple HFS+ and FAT32
Application Formats
Misuse of iPod
iPod Investigation
Testing Mac Version
Full System Restore
Testing Windows Version
User Account
Calendar and Contact Entries
Macintosh Version
Deleted Files
Windows Version
Registry Key Containing the iPod's USB/Firewire Serial Number

BlackBerry Forensics

Functions
As Operating System
How BlackBerry (RIM) Works
Serial Protocol
Security
Forensics
Acquisition
Collecting Evidence
Review of Evidence
Simulator - Screenshot
BlackBerry Attacks
Protecting Stored Data
Data Hiding in BlackBerry
BlackBerry Signing Authority Tool

Investigative Reports

Understanding the Importance of Reports
Investigating Report Requirements
Guidelines for Writing Reports
Important Aspects of a Good Report
Dos and Don'ts of Forensic Computer Investigations
Case Report Writing and Documentation
Create a Report to Attach to the Media Analysis Worksheet
Investigative Procedures
Best Practices for Investigators

Becoming an Expert Witness

What is Expert Witness?
Types of Expert Witnesses
Scope of Expert Witness Testimony
Checklists for Processing Evidence
Examining Computer Evidence
Dealing with Media

Course Description:

This course is the official courseware for the Security Certified Program SC0-451 certification exam. The Tactical Perimeter Defense course is designed to provide network administrators and certification candidates with hands-on tasks on the most fundamental perimeter security technologies. The network perimeter is often the first line of defense in an organization's network, and this course covers the issues with which every administrator must be familiar.

Who Should Attend:

This course is for network administrators and certification candidates.

Prerequisites:

To ensure your success, we recommend that you have CompTIA's Security+ certification, or have equivalent experience. This course assumes that the reader has fundamental working knowledge of networking concepts, and foundational security knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the core issues of building a perimeter network defense system.
- Investigate the advanced concepts of the TCP/IP protocol suite.
- Secure routers through hardening techniques and configure Access Control Lists.
- Design and configure multiple firewall technologies.
- Examine and implement IPSec and Virtual Private Networks.
- Design and configure an Intrusion Detection System.
- Secure wireless networks through the use of encryption systems.

Course Outline:**Lesson 1: Network Defense Fundamentals**

Network Defense
Defensive Technologies
Objectives of Access Control
The Impact of Defense
Network Auditing Concepts

Lesson 2: Advanced TCP/IP

TCP/IP Concepts
Analyzing the Three-way Handshake
Capturing and Identifying IP Datagrams
Capturing and Identifying ICMP Messages
Capturing and Identifying TCP Headers
Capturing and Identifying UDP Headers
Analyzing Packet Fragmentation
Analyzing an Entire Session

Lesson 3: Routers and Access Control Lists

Fundamental Cisco Security
Routing Principles
Removing Protocols and Services
Creating Access Control Lists
Implementing Access Control Lists
Logging Concepts

Lesson 4: Designing Firewalls

Firewall Components
Create a Firewall Policy
Rule Sets and Packet Filters
Proxy Server
The Bastion Host
The Honeypot

Lesson 5: Configuring Firewalls

Understanding Firewalls
Configuring Microsoft ISA Server 2006
IPTables Concepts
Implementing Firewall Technologies

Lesson 6: Implementing IPSec and VPNs

Internet Protocol Security
IPSec Policy Management
IPSec AH Implementation
Combining AH and ESP in IPSec
VPN Fundamentals
Tunneling Protocols
VPN Design and Architecture
VPN Security
Configuring a VPN

Lesson 7: Designing an Intrusion Detection System

The Goals of an Intrusion Detection System
Technologies and Techniques of Intrusion Detection
Host-based Intrusion Detection

Network-based Intrusion Detection
The Analysis
How to Use an IDS
What an IDS Cannot Do

Lesson 8: Configuring an IDS

Snort Foundations
Snort Installation
Snort as an IDS
Configuring Snort to Use a Database
Running an IDS on Linux

Lesson 9: Securing Wireless Networks

Wireless Networking Fundamentals
Wireless LAN (WLAN) Fundamentals
Wireless Security Solutions
Wireless Auditing
Wireless Trusted Networks

Course Description:

This course is the official courseware for the Security Certified Program SC0-471 certification exam. The Strategic Infrastructure Security (SIS) course is designed to follow the hands-on skills utilized in the Tactical Perimeter Defense (TPD) course. The SIS course continues with hardening of strategic elements of your infrastructure, such as your Windows and Linux servers, and goes into detail on one of the most critical areas to understand in security, Cryptography.

Who Should Attend:

This course is for network administrators and certification candidates.

Prerequisites:

To ensure your success, we recommend that you have completed the SCP Tactical Perimeter Defense (TPD) course. The TPD course will ensure you have the core security concepts and skills in developing a secure perimeter for your organization.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Detail the core issues of cryptography, including public and private key.
- Harden SuSe Linux 10 Server computers.
- Harden Windows Server 2003 computers.
- Utilize ethical hacking attack techniques.
- Secure DNS and web servers, and examine Internet and WWW security.
- Perform a risk analysis.
- Create a security policy.
- Analyze packet signatures.

Course Outline:**Lesson 1: Cryptography and Data Security**

History of Cryptography
Math and Algorithms
Private Key Exchange
Public Key Exchange
Message Authentication

Concepts of Security Policies
Policy Design
Policy Contents
An Example Policy
Incident Handling and Escalation Procedures
Partner Policies

Lesson 2: Hardening Linux Computers

Linux Filesystem and Navigation
General Secure System Management
User and Filesystem Security Administration
Network Interface Configuration
Security Scripting
Useful Linux Security Tools

Analyzing Packet Signatures
Signature Analysis
Common Vulnerabilities and Exposures (CVE)
Signatures
Normal Traffic Signatures
Abnormal Traffic Signatures

Lesson 3: Hardening Windows Server 2003

Windows 2003 Infrastructure Security
Windows 2003 Authentication
Windows 2003 Security Configuration Tools
Windows 2003 Resource Security
Windows 2003 Auditing and Logging
Windows 2003 EFS
Windows 2003 Network Security

Lesson 4: Attack Techniques

Network Reconnaissance
Mapping the Network
Sweeping the Network
Scanning the Network
Vulnerability Scanning
Viruses, Worms, and Trojan Horses
Gaining Control Over the System
Recording Keystrokes
Cracking Encrypted Passwords
Revealing Hidden Passwords
Social Engineering
Gaining Unauthorized Access
Hiding Evidence of an Attack
Performing a Denial of Service

Lesson 5: Security on the Internet and the WWW

Describing the Major Components of the Internet
Securing DNS Services
Describing Web Hacking Techniques
Describing Methods Used to Attack Users

Lesson 6: Performing a Risk Analysis

Concepts of Risk Analysis
Methods of Risk Analysis
The Process of Risk Analysis
Techniques to Minimize Risk
Continuous Risk Assessment

Lesson 7: Creating a Security Policy

Course Description:

This course is designed to provide the foundation knowledge to network administrators and security professionals who are seeking to learn about advanced security issues surrounding PKI and biometrics. Advanced Security Implementation is designed to provide network administrators and security architects with an awareness of security-related issues and the essential skills they need to implement security in a given network. It is the first course offered in the second level of the Security Certified Program. This course is followed by Enterprise Security Solutions (ESS).

Who Should Attend:

This class is for network administrators and security professionals who are seeking to learn about advanced security issues surrounding PKI and biometrics.

Prerequisites:

To ensure your success, you are strongly recommended to first take Security Certified Program: Tactical Perimeter Defense and Security Certified Program: Strategic Infrastructure Security or have equivalent knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Describe the fundamentals of trusted networks.
- Describe the concepts and principles of cryptography.
- Implement computer forensic tools.
- Identify current laws and legislation that influence computer security professionals.
- Describe biometric solutions, including fingerprint scanning, iris scanning, and vocal scanning.
- Describe strong authentication solutions and implement token-based strong authentication.
- Describe the function of digital certificates.
- Describe the implementation of digital signatures.

Course Outline:**Lesson 1: Introduction to Trusted Networks**

The Need For Trusted Networks
Authentication and Identification
Public Key Infrastructure
Applications of PKI

Lesson 2: Cryptography and Data Security

History of Cryptography
Math and Algorithms
Private Key Exchange
Public Key Exchange
Message Authentication

Lesson 3: Computer Forensics

Incident Response
Computer Forensic Fundamentals
Hard Disk Structure
Forensic Tools
Investigating Computers
Computer Forensics Solutions

Lesson 4: Law and Legislation

Intellectual Property
Categories and Types of Law
Process of Handling Evidence
Information Security-related Laws and Acts

Lesson 5: Biometrics—Who You Are

The Process of Biometrics Today
Accuracy of Biometrics
Applications of Biometrics
Fingerprint Scanning
Facial Scanning
Iris and Retinal Scanning
Vocal Scanning
Further Biometric Technologies
Techniques for Compromising Biometrics

Lesson 6: Strong Authentication

Why Strong Authentication
Authentication Tokens
RSA SecurID
Smart Cards

Lesson 7: Digital Certificates

Paper Certificates and Identity Cards
Authorities that Issue Physical Certificates
The Importance of Protecting the Identity of the CA
Differences between Physical and Digital Certificates
Standards for Digital Certificates
X.509 as an Authentication Standard

Case Study—VeriSign's Digital Certificates

Lesson 8: Digital Signatures

Signatures as Identifiers
Features of Digital Signatures
Digital Signatures in Practice
Standards for Digital Signatures
Digital Signatures and PKI

Appendix A: About FIPS PUB

Federal Information Processing Standards Publication

Appendix B: PKI-related Acronyms

PKI-related Acronyms

Course Description:

Enterprise Security Solutions is designed to provide network administrators and security architects with an awareness of security-related issues and the essential skills they need to implement security in a given network. It is the second course offered in the second level of the Security Certified Program. This course is preceded by Advanced Security Implementation (ASI).

Who Should Attend:

This course is for network administrators and security architects.

Prerequisites:

To ensure your success, we recommend you first take Security Certified Program: Tactical Perimeter Defense, Security Certified Program: Strategic Infrastructure Security, and Security Certified Program: Advanced Security Implementation or have equivalent knowledge.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Identify, describe the transition towards, and implement trusted networks.
- Implement a stand-alone Microsoft CA and a Microsoft Enterprise Root CA.
- Implement a Linux CA.
- Manage digital certificates.
- Configure local file encryption.
- Protect local files using biometrics.
- Configure and secure wireless networks.
- Secure email using PGP and S/MIME.
- Build trusted networks.

Course Outline:**Lesson 1: Trusted Network Implementation**

Defended Networks of Today
Trusted Network Services
Cryptography Primer
The Role of Strong Authentication
PKI Roles and Fundamentals

Setting Up the Linux CA
Certificate Authority Trust—Cross Trust
Secure Email
Certificate Revocation

Lesson 2: Planning a Trusted Network

Required Components
Certificate Paths
Planning Documents
Certificate Practices Framework

Lesson 3: Microsoft Trusted Networks

Certificate Authority Requirements
Major Functions of a CA Hierarchy
Certificate Standard and Format
Implement Microsoft Certificate Authorities
Implement a Microsoft Enterprise Root CA

Lesson 4: Linux Certificate Authorities

Introduction to Linux Certificate Authorities
Certificate Authorities for Linux
Prepare to Install a CA
OpenLDAP
Use CATool

Lesson 5: Managing Certificates

Certificate Lifecycle and Certificate Management
Create Certificates
Process Certificate Requests
Assign a Certificate
Certificates on Smart Cards

Lesson 6: Local Resource Security

Windows 2000 EFS Fundamentals
Configure EFS
Control EFS Use
Store Encrypted Files on a Floppy Disk with EFS
Secure Data with Biometrics

Lesson 7: Wireless Network Security

Wireless Networking Fundamentals
Wireless LAN (WLAN) Fundamentals
Wireless Security Solutions
Wireless Auditing
Wireless Trusted Networks

Lesson 8: Secure Email

Secure Email Fundamentals
Secure Email with PGP
S/MIME Background

Lesson 9: Building Trusted Networks

Building Windows Domains—Enterprise of Trust
Configuring the Enterprise CA