

# NETWORKING AND SECURITY

*Revised 7/12/2010*

**/training/etc**

*The Art of Knowledge.*

**This Page Intentionally Left Blank**

## Table of Contents

---

A+ Essentials.....	1
Network+ Certification.....	2
Security+ Certification.....	3
Certified Network Defense Architect (CNDA).....	4
Certified Ethical Hacker.....	5
ECSCA/LPT Certification Bootcamp.....	6
Computer Hacking Forensics Investigator (CHFI).....	7
Security Certified Program: Tactical Perimeter Defense.....	8
Security Certified Program: Strategic Infrastructure Security.....	9
Security Certified Program: Advanced Security Implementation.....	10
Security Certified Program: Enterprise Security Solutions.....	11
Wireless LAN Administration.....	12
Wireless LAN Security.....	13
CISSP.....	14
ISSEP.....	15

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:** Network+ Certification is a five-day class that prepares students to take the Network+ exam. Furthermore, the Network+ Certification can be the first step in achieving a Windows MCSE or CNE Certification.

**Who Should Attend:** This course is geared toward technicians with 18 to 24 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 Theory

Networking Terminology  
Network Building Blocks  
Standard Network Models  
Network Topologies  
Network Categories

#### Network Communications Methods

Transmission Methods  
Media Access Methods  
Signaling Methods

#### Network Data Delivery

Data Addressing and Delivery  
Network Connection Mechanisms  
Reliable Delivery Techniques

#### Network Media and Hardware

Bounded Network Media  
Unbounded Network Media  
Noise Control  
Network Connectivity Devices

#### Network Implementations

The OSI Model  
Client Network Resource Access  
Ethernet Networks  
Token Ring Networks  
Fiber Distributed Data Interface (FDDI) Networks  
Wireless Technologies and Standards

#### Networking with TCP/IP

Families of Protocols  
The TCP/IP Protocol  
Default IP Addresses  
Custom IP Addresses  
The TCP/IP Protocol Suite

#### TCP/IP Services

IP Address Assignment Methods  
Host Name Resolution  
NetBIOS Name Resolution  
TCP/IP Utilities  
TCP/IP Upper-layer Services  
TCP/IP Interoperability Services

#### Other Network Protocols

The NetBEUI Protocol  
The IPX/SPX Protocol  
The AppleTalk Protocol  
The IP Version 6 (IPv6) Protocol

#### Local Area Network (LAN) Infrastructure

Bridges and Switches  
IP Routing Topology  
Static IP Routing  
Dynamic IP Routing  
Controlling Data Movement with Filters and VLANs

#### Wide Area Network (WAN) Infrastructure

WAN Switching Technologies  
WAN Transmission Technologies  
WAN Connectivity Methods  
Voice Over Data Systems

#### Network Security

Network Threats  
Virus Protection  
Local Security  
Network Authentication Methods  
Data Encryption  
Internet Security

#### Remote Networking

Remote Network Architectures  
Terminal Services Implementations  
Remote Access Networking Implementations  
Virtual Private Networking (VPN)

#### Disaster Recovery

Planning for Disaster Recovery  
Data Backup  
Fault Tolerance Methods

#### Network Data Storage

Enterprise Data Storage Techniques  
Clustering  
Network Attached Storage (NAS)  
Storage Area Network (SAN) Implementations

#### Network Operating Systems

Microsoft Operating Systems  
Novell NetWare  
UNIX and Linux Operating Systems  
Macintosh Networking

#### Network Troubleshooting

Troubleshooting Models  
TCP/IP Troubleshooting Utilities  
Hardware Troubleshooting Tools  
System Monitoring Tools  
Network Baselining

**Course Description:** Security+™ A CompTIA Certification is the primary course you will need to take if your job responsibilities include securing network services, network devices, and network traffic. It is also the main course you will take to prepare for the CompTIA Security+ examination (exam number SY0-101). In this course, you'll build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network.

**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:

#### Identifying Security Threats

Identify Social Engineering Attacks  
Classify Software Attacks  
Identify Hardware Attacks

Set Up a Honeypot  
Respond to Security Incidents

#### Hardening Internal Systems and Services

Harden Base Operating Systems  
Harden Directory Services  
Harden DHCP Servers  
Harden Network File and Print Servers

#### Hardening Internetwork Devices and Services

Harden Internetwork Connection Devices  
Harden DNS and BIND Servers  
Harden Web Servers  
Harden FTP Servers  
Harden Network News Transport Protocol (NNTP) Servers  
Harden Email Servers  
Harden Conferencing and Messaging Servers

#### Securing Network Communications

Secure Network Traffic Using IP Security (IPSec)  
Secure Wireless Traffic  
Secure Client Internet Access  
Secure the Remote Access Channel

#### Managing Public Key Infrastructure (PKI)

Install a Certificate Authority (CA) Hierarchy  
Harden a Certificate Authority  
Back Up Certificate Authorities  
Restore a Certificate Authority

#### Managing Certificates

Enroll Certificates for Entities  
Secure Network Traffic Using Certificates  
Renew Certificates  
Revoke Certificates  
Back Up Certificates and Private Keys  
Restore Certificates and Private Keys

#### Enforcing Organizational Security Policy

Enforce Corporate Security Policy Compliance  
Enforce Legal Compliance  
Enforce Physical Security Compliance  
Educate Users

#### Monitoring the Security Infrastructure

Scan for Vulnerabilities  
Monitor for Intruders

**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 30: Exploit Writing	Module 55: Data Loss Prevention
Module 2: Hacking Laws	Module 31: Smashing the Stack for Fun and Profit	Module 56: Hacking Global Positioning System (GPS)
Module 3: Footprinting	Module 32: Windows Based Buffer Overflow Exploit Writing	Module 57: Computer Forensics and Incident Handling
Module 4: Google Hacking	Module 33: Reverse Engineering	Module 58: Credit Card Frauds
Module 5: Scanning	Module 34: MAC OS X Hacking	Module 59: How to Steal Passwords
Module 6: Enumeration	Module 35: Hacking Routers, cable Modems and Firewalls	Module 60: Firewall Technologies
Module 7: System Hacking	Module 36: Hacking Mobile Phones, PDA and Handheld Devices	Module 61: Threats and Countermeasures
Module 8: Trojans and Backdoors	Module 37: Bluetooth Hacking	Module 62: Case Studies
Module 9: Viruses and Worms	Module 38: VoIP Hacking	Module 63: Botnets
Module 10: Sniffers	Module 39: RFID Hacking	Module 64: Economic Espionage
Module 11: Social Engineering	Module 40: Spamming	Module 65: Patch Management
Module 12: Phishing	Module 41: Hacking USB Devices	Module 66: Security Convergence
Module 13: Hacking Email Accounts	Module 42: Hacking Database Servers	Module 67: Identifying the Terrorist
Module 14: Denial-of-Service	Module 43: Cyber Warfare- Hacking, Al-Qaida and Terrorism	
Module 15: Session Hijacking	Module 44: Internet Content Filtering Techniques	
Module 16: Hacking Web Servers	Module 45: Privacy on the Internet	
Module 17: Web Application Vulnerabilities	Module 46: Securing Laptop Computers	
Module 18: Web-Based Password Cracking Techniques	Module 47: Spying Technologies	
Module 19: SQL Injection	Module 48: Corporate Espionage- Hacking Using Insiders	
Module 20: Hacking Wireless Networks	Module 49: Creating Security Policies	
Module 21: Physical Security	Module 50: Software Piracy and WareZ	
Module 22: Linux Hacking	Module 51: Hacking and Cheating Online Games	
Module 23: Evading IDS, Firewalls and Detecting Honey Pots	Module 52: Hacking RSS and Atom	
Module 24: Buffer Overflows	Module 53: Hacking Web Browsers (Firefox, IE)	
Module 25: Cryptography	Module 54: Proxy Server Technologies	
Module 26: Penetration Testing		
Module 27: Covert Hacking		
Module 28: Writing Virus Codes		
Module 29: Assembly Language Tutorial		

**Course Description:** Students will be shown how to scan, test, and hack their own systems. Each student will gain in-depth knowledge and practical experience with the current essential security systems. Students will be taught how perimeter defenses work and will then learn how intruders escalate privileges. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. At the end of the course, they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50. This course is an entry-level penetration testing course designed for those with IT security experience but not experienced penetration testers.

**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:

Introduction to Ethical Hacking

Footprinting

Scanning

Enumeration

System Hacking

Trojans and Backdoors

Sniffers

Denial of Service

Social Engineering

Session Hijacking

Hacking Web Servers

Web Application Vulnerabilities

Web-based Password Cracking Techniques

SQL Injection

Hacking Wireless Networks

Virus and Worms

Physical Security

Linux Hacking

Evading IDS, Firewalls, and Honeypots

Buffer Overflows

Cryptography

Penetration Testing

Self-Study Modules

**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 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 MASTer Solo-3 Forensic Save-N-Sync  
ImageMASTer 6007SAS and Disk Jockey IT  
SCSI/PAK  
IBM DFMSDsss  
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: Topdump  
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  
Netresident Tool  
eTrust Network Forensics  
IDS Policy Manager  
<http://www.activework.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  
Airodump: 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](http://www.centralops.net)  
NetScan Tools Pro  
Tool: Privoxy <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  
Challenges in the Detection of DoS Attack  
Internet Crimes 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  
EnCase  
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 Dons 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

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  
Setting Up the Linux CA

**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

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  
802.1X/EAP types and differences  
802.11 handshakes

**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.

**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