Formatech
INTEGRATED LEARNING CENTERS
Learn from the Experts

Course Outline

SECURITY+

Duration: 5 days (30 hours)

Learning Objectives:

This course will help students prepare for the Security+ Certification exam by learning how to develop and improve security

Target Audience:

Any

Prerequisites:

Students should have knowledge and experience of personal computers and a strong understanding of networking and Internet technologies

Topics Covered:

- General Security Concepts
  - Information Security
  - Physical Security
  - Operational Security
  - Management and Policies
  - Goals of Information Security
  - The Security Process
  - Antivirus Software
  - Access Control
  - Authentication
  - Services and Protocols
  - Security Topologies
  - Design Goals
  - Security Zones
  - Technologies
  - Business Concerns
- Know Your Enemy
  - Attack Strategies
  - Access Attacks
  - Modification and Repudiation Attacks
  - Denial of Service Attacks (DoS)
  - Common Attacks
  - Security Concerns and TCP/IP
  - The TCP/IP Protocol Suite
  - Application Layer

- Host-to-Host or Transport Layer
- Internet Layer
- Network Interface Layer
- Encapsulation
- Protocols and Services
- TCP/IP Attacks
- Software Exploitation
- Surviving Malicious Code
- Viruses
- Trojan Horses
- Logic Bombs
- Worms
- Antivirus Software
- Social Engineering
- Auditing Processes and Files

➢ Infrastructure and Connectivity

- Infrastructure Security
- Hardware Components
- Software Components
- Devices
- Firewalls
- Routers
- Switches
- Wireless Access Points
- Modems
- Remote Access Services
- Telecom/PBX Systems
- Virtual Private Network
- Network Monitoring and Diagnostics
- Workstations
- Servers
- Mobile Devices
- Remote Access
- Serial Line Internet Protocol
- Point-to-Point Protocol
- Tunneling Protocols
- Internet Connections
- Ports and Sockets
- E-Mail
- Web
- File Transfer Protocol
- SNMP and Other TCP/IP Protocols
- Cabling, Wires, and Communications
- Coax

- Unshielded Twisted Pair and Shielded Twisted Pair
- Fiber Optic
- Infrared
- Radio Frequency
- Microwave
- Removable Media
- Tape
- CD-R
- Hard Drives
- Diskettes
- Flash Cards
- Smart Cards

➢ Monitoring Communications Activity
- Network Monitoring
- Types of Network Traffic
- Network Monitoring Systems
- Intrusion Detection Systems
- Network-Based IDS
- Host-Based IDS
- Honey Pots
- Incident Response
- Incident Identification
- Investigating the Incident
- Repairing the Damage
- Documenting the Response
- Adjusting the Procedures
- Wireless Systems
- WTLS
- IEEE 802.11 Wireless Protocols
- WEP/WAP
- Wireless Vulnerabilities
- Instant Messaging
- IM Vulnerabilities
- 8.3 File Naming
- Packet Sniffing
- Privacy
- Signal Analysis/Signal Intelligence
- Footprinting
- Scanning
- Enumeration

➢ Implementing and Maintaining a Secure Network
- Overview of Network Security Threats
- Security Baselines
- OS/NOS Hardening

- Network Protocol Configuration
- Microsoft Windows 9x
- Microsoft Windows NT 4
- Microsoft Windows 2000
- Microsoft Windows XP
- Windows .NET Server 2003
- UNIX/Linux
- Novell NetWare
- IBM
- Apple Macintosh
- File Systems
- Operating System Updates
- Network Hardening
- Network Device Updates
- Configuring Network Devices
- Application Hardening
- Web Servers
- E-Mail Servers
- FTP Servers
- DNS Servers
- NNTP Servers
- File and Print Servers and Services
- DHCP Services
- Data Repositories

➢ Working with a Secure Network

- Physical Security
- Access Control
- Social Engineering
- Environment
- Business Continuity Planning
- Business Impact Analysis
- Risk Assessment
- Policies, Standards, and Guidelines
- Policies
- Standards
- Guidelines
- Security Standards and ISO 17799
- Information Classification
- Public Information
- Private Information
- Government and Military Classifications
- Roles in the Security Process
- Information Access Controls

➢ Cryptography Basics and Methods

- Overview of Cryptography
- Physical Cryptography
- Mathematical Cryptography
- Quantum Cryptography
- The Myth of Unbreakable Codes
- Cryptographic Algorithms
- Hashing
- Symmetric Algorithms
- Asymmetric Algorithms
- Using Cryptographic Systems
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Access Control
- Public Key Infrastructure
- Certificate Authority
- RAs and LRAs
- Certificates
- Certificate Revocation
- Trust Models
- Cryptographic Attacks

➢ Cryptography Standards
- Cryptography Standards and Protocols
- Origins of Encryption Standards
- PKIX/PKCS
- X.509
- SSL
- TLS
- ISAKMP
- CMP
- S/MIME
- SET
- SSH
- PGP
- HTTPS
- S-HTTP
- IPSec
- FIPS
- Common Criteria
- WTLS
- WEP
- ISO 17799
- Key Management and the Key Life Cycle

- Centralized versus Decentralized Key Generation
- Key Storage and Distribution
- Key Escrow
- Key Expiration
- Key Revocation
- Key Suspension
- Recovering and Archiving Keys
- Renewing Keys
- Key Destruction
- Key Usage

➢ Security policies and Procedures

- Business Continuity
- Utilities
- High Availability
- Disaster Recovery
- Vendor Support
- Service Level Agreements
- Code Escrow
- Policies and Procedures
- Personnel Policies
- Business Policies
- Certificate Policies
- Incident Response Policies
- Privilege Management
- User and Group Role Management
- Single Sign-On
- Privilege Decision Making
- Auditing
- Access Control

➢ Security Management

- Computer Forensics
- Methodology of a Forensic Investigation
- Chain of Custody
- Preservation of Evidence
- Collection of Evidence
- Security Management
- Best Practices and Documentation
- Change Management
- Systemic Change
- Understanding the Roles in a Change Process
- Justifying the Need for Change
- Scheduling Changes
- Change Staging
- Change Documentation

- Change Notification
- Security Awareness and Education
- Communications and Awareness
- Education
- Staying on Top of Security
- Websites
- Trade Publications
- Privacy and Security Regulations
- HIPAA
- Gramm-Leach Bliley Act of 1999
- Computer Fraud and Abuse Act
- FERPA
- Computer Security Act of 1987
- Cyberspace Electronic Security Act (CESA)
- Cyber Security Enhancement Act
- Patriot Act
- International Efforts