CompTIA Security+

Course Description:
CompTIA Security+® (2008 Objectives) 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+ (2008 Edition) Certification examination (exam number SY0-201). In this course, you will 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.

Duration: Instructor-led, group-paced, classroom-delivery learning model with structured hands on activities
35 hours (5 days)

Course Materials: Students will be provided with the following software for use in the classroom:

- Certification lesson guides, workbooks
  (The above-mentioned materials are yours to keep)

Objectives: After completing this course, students will be able to:

- Identify fundamental concepts of computer security.
- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Establish security best practices for creating and running web-based applications.
- Manage public key infrastructure (pki).
- Manage certificates.
- Enforce organizational security policies.
- Monitor the security infrastructure.
- Manage security incidents.

Prerequisites: Basic Windows skills and fundamental understanding of computer and networking concepts are required. Students can obtain this level of skill and knowledge by taking the following Element K courses: Introduction to Networks and the Internet and any one or more of the following: Introduction to Personal Computers: Using Windows XP, Windows XP: Introduction to Personal Computers: Using Windows Vista, Microsoft Windows Vista: Level 1 and Level 2, CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended.

CompTIA Security+

Course Outline

Security Fundamentals
- Security Building Blocks
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Security Threats
- Social Engineering
- Software-Based Threats
- Network-Based Threats
- Hardware-Based Threats

Hardening Internal Systems and Services
- Harden Operating Systems
- Harden Directory Services
- Harden DHCP Servers
- Harden File and Print Servers

Hardening Internetwork Devices and Services
- Harden Internetwork Connection Devices
- Harden DNS and BIND Servers
- Harden Web Servers
- Harden Email Servers
- Harden Conferencing and Messaging Servers
- Secure File Transfers

Securing Web Applications
- Prevent Input Validation Attacks
- Protect Systems from Buffer Overflow Attacks
- Implement ActiveX and Java Security
- Protect Systems from Scripting Attacks
- Implement Secure Cookies
- Harden a Web Browser

Managing Public Key Infrastructure (PKI)
- Install a Certificate Authority (CA) Hierarchy
- Harden a Certificate Authority
- Backup a CA
- Restore a CA

Managing Certificates
- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up Certificates and Private Keys
- Restore Certificates and Private Keys

Enforcing Organizational Security Policies
- Perform a Risk Assessment
- Enforce Corporate Security Policy Compliance
- Enforce Legal Compliance
- Enforce Physical Security Compliance
- Educate Users
- Plan for Disaster Recovery
- Conduct a Security Audit

Monitoring the Security Infrastructure
- Scan for Vulnerabilities
- Monitor for Security Anomalies
- Setup a Honeypot

Managing Security Incidents
- Respond to Security Incidents
- Evidence Administration
- Recover from a Security Incident