

CompTIA Security+ (SYO-401)

Prerequisites: CompTIA A+ certification and CompTIA Network+ certification or equivalent experience.

Length: 5 Days

Overview: This training covers topics such as maintenance problem solutions of PC's, Mobile Devices, Laptops, Operating Systems and Printers and is training is intended for junior IT staff and helpdesk employees. It confirms your ability to react to security incidents, and it validates your skill in anticipating security risks and guarding against them. After completion of this training, student will be well prepared to take the SYO-401 exam.

Target Audience: Candidates for the Security+ certification (SYO-401)

Objectives:

- Implementing and monitoring security on networks, applications, and operating systems
- Access control and authentication
- Certificate management
- Risk analysis and risk management
- Security breach response and recovery

Course Content

SECURITY FUNDAMENTALS

- Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

SECURITY THREATS AND VULNERABILITIES

- Social Engineering
- Physical Threats and Vulnerabilities
- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Software-Based Threats

NETWORK SECURITY

- Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols
- Apply Network Security Administration Principles
- Secure Wireless Traffic

MANAGING APPLICATION, DATA, AND HOST SECURITY

- Establish Device/Host Security
 - Application Security
 - Data Security
 - Mobile Security
-

ACCESS CONTROL, AUTHENTICATION, AND ACCOUNT MANAGEMENT

- Access Control and Authentication Services
- Implement Account Management Security Controls

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

- Business Continuity
- Plan for Disaster Recovery
- Execute Disaster Recovery Plans and Procedures

MANAGING CERTIFICATES

- Install a Certificate Authority (CA) Hierarchy
- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up and Restore Certificates and Private Keys

COMPLIANCE AND OPERATIONAL SECURITY

- Physical Security
- Legal Compliance
- Security Awareness and Training

RISK MANAGEMENT

- Risk Analysis
- Implement Vulnerability Assessment Tools and Techniques
- Scan for Vulnerabilities
- Mitigation and Deterrent Techniques

MANAGING SECURITY INCIDENTS

- Respond to Security Incidents
 - Recover from a Security Incident
-