CompTIA Security+ 5 Day Course

Overview

CompTIA Security+ Certification SY0-601 provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security.

This course maps to the CompTIA Security+ SY0-601 certification exam.

Target Audience

- System Administrator
- Security Administrator
- Security Specialist
- Network Consultant

Prerequisites

There are no specific prerequisites to take up this certification.

It is recommended to take the Network+ certification or equivalent before taking the Security+ training and certification exam.

Delegates will learn how to

- Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Implement secure network architecture concepts and systems design
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure

Course Outline

Module 1: Security fundamentals

- Security concepts
- Enterprise security strategy
- Security program components

Module 2: Risk management

- Understanding threats
- Risk management programs
- Security assessments

Module 3: Cryptography

- Cryptography concepts
- Public key infrastructure
- Module 4: Network connectivity
- Network attacks
- Packet flow

Module 5: Network security technologies

- Network security components
- Monitoring tools

Module 6: Secure network configuration

- Secure network protocols
- Hardening networks

Module 7: Authentication

- Authentication factors
- Authentication protocols

Module 8: Access control

- Access control principles
- Account management

Module 9: Securing hosts and data

- Malware
- Securing data
- Securing hosts

Module 10: Securing specialized systems

- Mobile security
- Embedded and specialized systems

Module 11: Application security

- Application attacks
- Securing applications

Module 12: Cloud security

- Virtual and cloud systems
- Securing cloud services

Module 13: Organizational security

- Social engineering
- Security policies
- User roles and training
- Physical security and safety

Module 14: Disaster planning and recovery

- Business continuity
- Resilient systems
- Incident response procedures