

Course Description:

This course will prepare students to pass the current CompTIA Security+ SY0-301 certification exam. After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field. Comes with CertBlaster exam prep software (download).

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:**Mitigating threats**

System maintenance
Application security
Physical security
Malware
Social engineering

Cryptography

Symmetric cryptography
Public key cryptography

Authentication

: Authentication factors and requirements
Authentication systems
Authentication system vulnerabilities

User- and role-based security

Baseline security policies
Resource access

Peripheral security

File and disk encryption
Peripheral and component security
Mobile device security

Public key infrastructure

Public key cryptography
Implementing public key infrastructure
Web server security with PKI

Application and messaging security

Application security
E-mail security
Social networking and messaging

Ports and protocols

TCP/IP basics
Protocol-based attacks

Network security

Network devices
Secure network topologies
Secure networking
Virtualization and cloud computing

Wireless security

Wireless network security
Mobile device security

Remote access security

Remote access
Virtual private networks

Vulnerability testing and monitoring

Risk and vulnerability assessment
Auditing and logging
Intrusion detection and prevention systems
Incident response

Organizational security

Organizational policies
Education and training
Disposal and destruction

Business continuity

Business continuity planning
Disaster recovery
Environmental controls