/training/etc
CARE TO LEARN

CompTIA Security+ Certification

Course Length
40 Hours
TE3410_20150820

Course Description: CompTIA® Security+® (Exam SY0-401) is the primary course you will need to take if your job responsibilities include securing network services, devices, and traffic and your organization as a whole including the physical security elements and operational security measures. It is also the main course you will take to prepare for the CompTIA Security+ Certification examination. In this course, you will build on your knowledge and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-401) Certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of computer security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your computer security skill set so that you can confidently perform your duties in any security-related professional role.

Who Should Attend: This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS® X, Unix, or Linux, and 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 / experience.

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:

Lesson 1: Security Fundamentals
The Information Security Cycle
Information Security Controls
Authentication Methods
Cryptography Fundamentals
Security Policy Fundamentals

Lesson 2: Security Threats and Vulnerabilities
Social Engineering
Physical Threats and Vulnerabilities
Network-Based Threats
Wireless Threats and Vulnerabilities
Software-Based Threats

Lesson 3: Network Security
Network Devices and Technologies
Network Design Elements and Components
Implement Networking Protocols
Apply Network Security Administration Principles
Secure Wireless Traffic

Lesson 4: Managing Application, Data, and Host Security
Establish Device/Host Security
Application Security
Data Security
Mobile Security

Lesson 5: Access Control, Authentication, and Account Management
Access Control and Authentication Services
Implement Account Management Security Controls

Lesson 6: Managing Certificates
Install a CA Hierarchy
Enroll Certificates
Secure Network Traffic by Using Certificates
Renew Certificates
Revoke Certificates
Back Up and Restore Certificates and Private Keys

Lesson 7: Compliance and Operational Security
Physical Security
Legal Compliance
Security Awareness and Training

Lesson 8: Risk Management
Risk Analysis
Implement Vulnerability Assessment Tools and Techniques
Scan for Vulnerabilities
Mitigation and Deterrent Techniques

Lesson 9: Managing Security Incidents
Respond to Security Incidents
Recover from a Security Incident

Lesson 10: Business Continuity and Disaster Recovery Planning
Business Continuity
Plan for Disaster Recovery
Execute DRPs and Procedures
Appendix A: CompTIA® Security+® (Exam SY0-401) Objectives Mapping