Compuserve Pvt Ltd.

Course Duration : 35 Hrs

CompTIA

Security+ Student Guide (Exam SY0-601)

COURSE BROCHURE

Overview

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations and its industry-leading IT certifications are an important part of that mission. CompTIA's Security+ certification is a foundation-level certificate designed for IT administrators with two years' experience whose job role is focused on system security.

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to assist with cybersecurity duties in small and large organizations. These duties include assessments and monitoring; secure network, host, app, and cloud provisioning; data governance; and incident analysis and response.

Course Objective

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-601) 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 cybersecurity skill set so that you can confidently perform your duties in any entry-level security role. On course completion, you will be able to:

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions
- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Audience Profile

The Official **CompTIA Security+ Guide (Exam SY0-601)** is the primary course you will need to take if your job responsibilities include securing network services, devices, and data confidentiality/privacy in your organization. You can take this course to prepare for the **CompTIA Security+ (Exam SY0-601)** certification examination.

Prerequisites

- To ensure your success in this course, you should have basic Windows and Linux administrator skills and the ability to implement fundamental networking appliances and IP addressing concepts. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Table of Contents

Lesson 8: Implementing Identity and Account Management Controls

Topic 8A: Implement Identity and Account Types

Topic 8B: Implement Account Policies

Topic 8C: Implement Authorization Solutions

Topic 8D: Explain the Importance of Personnel Policies

Lesson 9: Implementing Secure Network Designs

Topic 9A: Implement Secure Network Designs

Topic 9B: Implement Secure Switching and Routing

Topic 9C: Implement Secure Wireless Infrastructure

Topic 9D: Implement Load Balancers

Lesson 10: Implementing Network Security Appliances

Topic 10A: Implement Firewalls and Proxy Servers

Topic 10B: Implement Network Security Monitoring

Topic 10C: Summarize the Use of SIEM

Lesson 11: Implementing Secure Network Protocols

Topic 11A: Implement Secure Network Operations Protocols

Topic 11B: Implement Secure Application Protocols

Topic 11C: Implement Secure Remote Access Protocols

Lesson 12: Implementing Host Security Solutions

Topic 12A: Implement Secure Firmware

Topic 12B: Implement Endpoint Security

Topic 12C: Explain Embedded System Security Implications

Lesson 13: Implementing Secure Mobile Solutions

Topic 13A: Implement Mobile Device Management

Topic 13B: Implement Secure Mobile Device Connections

Lesson 14: Summarizing Secure Application Concepts

Topic 14A: Analyze Indicators of Application Attacks

Topic 14B: Analyze Indicators of Web Application Attacks

Topic 14C: Summarize Secure Coding Practices

Topic 14D: Implement Secure Script Environments

Topic 14E: Summarize Deployment and Automation Concepts

Lesson 15: Implementing Secure Cloud Solutions

Topic 15A: Summarize Secure Cloud and Virtualization Services

Topic 15B: Apply Cloud Security Solutions

Topic 15C: Summarize Infrastructure as Code Concepts

Lesson 16: Explaining Data Privacy and Protection Concepts

Topic 16A: Explain Privacy and Data Sensitivity Concepts

Topic 16B: Explain Privacy and Data Protection Controls

Lesson 17: Performing Incident Response

Topic 17A: Summarize Incident Response Procedures

Topic 17B: Utilize Appropriate Data Sources for Incident Response

Topic 17C: Apply Mitigation Controls

Lesson 18: Explaining Digital Forensics

Topic 18A: Explain Key Aspects of Digital Forensics Documentation

Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

Lesson 19: Summarizing Risk Management Concepts

Topic 19A: Explain Risk Management Processes and Concepts

Topic 19B: Explain Business Impact Analysis Concepts

Lesson 20: Implementing Cybersecurity Resilience

Topic 20A: Implement Redundancy Strategies

Topic 20B: Implement Backup Strategies

Topic 20C: Implement Cybersecurity Resiliency Strategies

Lesson 21: Explaining Physical Security

Topic 21A: Explain the Importance of Physical Site Security Controls

Topic 21B: Explain the Importance of Physical Host Security Controls

Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com