TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Check Point Certified Security Administrator

9032803832

9032803832

contact@techyedz.com

www.techyedz.com

CompTIA Security+ 501

Course Overview:

There are many career opportunities for IT and cybersecurity professionals. If you're wondering where to start to help fill this gap, start with the CompTIA Security+ SY0-501 certification. This certification course helps you prove your competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security.

If you're wondering where to start in cybersecurity to help fill this gap, start with Security+. The CompTIA Security+ SY0-501 exam is an internationally recognized validation of foundation-level security skills and knowledge and is used by organizations and security professionals around the globe. The CompTIA Security+ certification proves an IT security professional's competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security. This course covers those topics to prepare students for the CompTIA SY0-501 certification exam. The fundamentals taught in this class will prepare you for a career as a cybersecurity analyst.

Course Outline:

1. Introduction

- Who Should Read This Book?
- CompTIA Security+ Exam Topics

2. Introduction to Security

- Security 101
- Think Like a Hacker
- Threat Actor Types and Attributes
- Review Key Topics

3. Computer Systems Security Part I

- Malicious Software Types
- Delivery of Malware
- Preventing and Troubleshooting Malware
- Lesson Summary

- Review Key Topics
- Complete the Real-World Scenarios

4: Computer Systems Security Part II

- Implementing Security Applications
- Securing Computer Hardware and Peripherals
- Securing Mobile Devices
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

5. OS Hardening and Virtualization

- Hardening Operating Systems
- Virtualization Technology
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

6. Application Security

- Securing the Browser
- Securing Other Applications
- Secure Programming
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

7. Network Design Elements

- Network Design
- Cloud Security and Server Defense
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

8. Networking Protocols and Threats

- Ports and Protocols
- Malicious Attacks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

9. Network Perimeter Security

- Firewalls and Network Security
- NIDS Versus NIPS
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

10. Securing Network Media and Devices

- Securing Wired Networks and Devices
- Securing Wireless Networks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

11. Physical Security and Authentication Models

- Physical Security
- Authentication Models and Components
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

12. Access Control Methods and Models

- Access Control Models Defined
- Rights, Permissions, and Policies
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

13. Vulnerability and Risk Assessment

- Conducting Risk Assessments
- Assessing Vulnerability with Security Tools
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

14. Monitoring and Auditing

- Monitoring Methodologies
- Using Tools to Monitor Systems and Networks
- Conducting Audits
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

15. Encryption and Hashing Concepts

- Cryptography Concepts
- Encryption Algorithms
- Hashing Basics
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

16. PKI and Encryption Protocols

- Public Key Infrastructure
- Security Protocols
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

17. Redundancy and Disaster Recovery

- Redundancy Planning
- Disaster Recovery Planning and Procedures
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

18. Social Engineering, User Education, and Facilities Security

- Social Engineering
- User Education
- Facilities Security
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

19. Policies and Procedures

- Legislative and Organizational Policies
- Incident Response Procedures
- IT Security Frameworks
- Lesson Summary
- Review Key Topics
- Complete the Real-World Scenarios

Prerequisites:

- One or two years of experience in networking support and IT administration
- Able to use Windows to create and manage files and use basic administrative features (Explorer, Control Panel and Management Consoles).
- Know basic network terminology and functions (such as OSI Model, topology, Ethernet, TCP/IP, switches and routers).
- Understand TCP/IP addressing, core protocols and troubleshooting tools.

Who can Attend:

- The CompTIA Security+ course is ideal for professionals who are working in the roles of system administrators, network administrators, security administrators, and IT auditors.

Certification: CompTIA Security+ SY0-501

- **Number of Hours: 50hrs**

- **Key Features:**

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification