SECURITY+ COURSE

The CompTIA Security+ Certification is an internationally recognized and vendor neutral certificate that validates the foundation-level of information and data security.

At completion of this course students will have the knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, students will be able to apply security controls to maintain confidentiality, integrity, and availability, Identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.

Students who pass these exams will have higher opportunities to become a Security Engineer, Security Consultant, Network Administrator and IA Technician or Manager.

The Security+ course will cover the most important foundational principles for securing a network and managing risk. Access control, identity management and cryptography are important topics on the exam, as well as selection of appropriate mitigation and deterrent techniques to address network attacks and vulnerabilities.

COURSE OUTLINE:

BASED ON EXAM SY0-401

Network Security

- Implement security configuration parameters on network devices and other technologies
- Secure network administration principles
- Network design elements and components
- Implement common protocols and services
- Troubleshoot security issues related to wireless networking

Compliance and Operational Security

- The importance of risk related concepts
- Security implications of integrating systems and data with third parties
- Implement appropriate risk mitigation strategies

- Basic forensic procedures
- Common incident response procedures
- The importance of security related awareness and training
- Contrast of physical security and environmental controls
- Risk management best practices
- The appropriate control to meet the goals of security

Threats and Vulnerabilities

- Types of malware and various types of attacks
- Social engineering attacks and the associated effectiveness with each attack
- Types of wireless and application attacks
- Mitigation and deterrent techniques
- Discover security threats and vulnerabilities
- The proper use of penetration testing versus vulnerability scanning

Application, Data and Host Security

- The importance of application security controls and techniques
- Mobile security concepts and technologies
- Solution to establish host security
- Implement the appropriate controls to ensure data security
- Contrast of alternative methods to mitigate security risks in static environments

Access Control and Identity Management

- Contrast of the function and purpose of authentication services
- Authentication, authorization or access control
- Install and configure security controls when performing account management, based on best practices

Cryptography

- General cryptography concepts
- Appropriate cryptographic methods

BASED ON EXAM SY0-301

Network Security

- The security function and purpose of network devices and technologies
- Apply and implement secure network administration principles

- Network design elements and components
- Implement and use common protocols
- Identify commonly used default network ports
- Implement wireless network in a secure manner

Compliance and Operational Security

- Risk related concepts and risk mitigation strategies
- Incident response procedures
- Security related awareness and training
- Contrast of aspects of business continuity
- Impact and proper use of environmental controls
- Disaster recovery plans and procedures
- The concepts of confidentiality, integrity and availability (CIA)

Threats and Vulnerabilities

- Differences among types of malware
- Differences among types of attacks
- Differences among types of social engineering attacks
- Differences among types of wireless attacks
- Differences among types of application attacks
- Differences among types of mitigation and deterrent techniques
- Discover security threats and vulnerabilities
- Proper use of penetration testing versus vulnerability scanning

Application, Data and Host Security

- The importance of application security
- Appropriate procedures to establish host security
- The importance of data security

Access Control and Identity Management

- Function and purpose of authentication services
- The fundamental concepts and best practices related to authentication, authorization and access control
- Implement appropriate security controls when performing account management

Cryptography

- General cryptography concepts
- Appropriate cryptographic tools and products

- The core concepts of public key infrastructure
- Implement PKI, certificate management and associated components