ANNE ARUNDEL COMMUNITY COLLEGE

Security+
CompTIA Secuirty+ Certification Exam Preparation

Course Description

This continuing education course is designed for professionals in information assurance and cyber security careers and provides instruction on the six CompTIA Security+ exam objectives. Topics include network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, as well as cryptography.

Course Objectives

Upon completion of this course, the students will be able to:

- Develop skills and knowledge necessary to successfully complete the CompTIA Security+ certification exam;
- Explain basic concepts of network security;
- Analyze and assess threats and vulnerabilities for information and information systems;
- Identify and provide examples of operational security concerns;
- Evaluate hardware and software solutions for access control and identity management.

Course Outline

I. Network Security
   A. Network architectures, devices and technologies
   B. Network administration and security
   C. TCP/IP and OSI network models
   D. Wireless and mobile networking and security

II. Threats and Vulnerabilities
   A. Threats including malware
   B. Attacks (software, hardware, networks)
   C. Vulnerability assessment and management
   D. Detect, deter mitigate and prevent

III. Operational Security
   A. Concepts, assessment, and Op security
   B. Risk identification, assessment and mitigation
   C. BCP/DR
   D. Incident response procedures and planning

IV. Access Control and Identity Management
   A. Authentication and authentication services

B. Identity management
C. Account management
D. Hardware and software solutions for authorization

Training: 40 hours