



CENTRAL PIEDMONT COMMUNITY COLLEGE

CORPORATE & CONTINUING EDUCATION

Course Number: DPT7014
Course Title: Security+
Course Hours: 40

Last Revised On: 11/17/2008

Description:

This course teaches materials that map to all skill and knowledge objectives for the CompTIA Security+ certification exam (SY0-101). Skills the student will learn include identifying access control and authentication methods, identifying services provided by encryption, and managing a Public Key Infrastructure (PKI). Upon completion of this course, the student will better understand common types of network-based attacks, and how to respond to them. The student will also learn how to harden operating systems, secure remote access, and ensure physical security. In addition to teaching firewall and intrusion-detection technologies, this course teaches critical incident response and system forensics concepts.

Objectives:

- Learn to support network operating systems, secure remote access and ensure physical security.
- Learn to create and manage security policies,
- Students will understand common types of network-based attacks, and how to respond to them.
- Preparation for CompTIA's Security+ Certification exam.

Content:

1. Authentication Methods

- Defining security terms
- Authentication, multifactor, single sign-on and mutual authentication
- User name and password
- Understanding Kerberos
- Certificates
- Token-based and challenge handshake authentication protocol (CHAP)
- Smart cards
- Biometrics
- Extensible authentication protocol (EAP)

2. Access Control

- Access control terminology and concepts and methods
- Balancing responsibilities of security

3. Cryptography Essentials

- Cryptography and encryption
- Hash, symmetric-key, asymmetric-key and applied encryption
- Creating a security matrix



CENTRAL PIEDMONT COMMUNITY COLLEGE

CORPORATE & CONTINUING EDUCATION

4. Public Key Infrastructure

- Public key infrastructure (PKI) essentials
- Key management and the certificate life cycle

5. Network Attacks and Vulnerabilities

- Network attack overview
- Protocol overview
- Spoofing and scanning, denial of service (DOS), distributed denial of service (DDOS)
- Man in the middle and password guessing attacks
- Profile of an attack
- Software exploitation
- Attacks against encryption
- Social engineering
- Malicious code and auditing

6. Operating System and Application Hardening

- Security baselines
- Client security issues
- Server side issues: application hardening
- Operating system hardening

7. Securing Remote Access

- Remote access concepts and terminology
- Overview of remote access methods
- Virtual private networks (VPN's)
- Terminal access controller access control system (TACACS) and TACACS+
- Remote authentication dial-in user service (RADIUS), IPSec and 802.1x
- Remote administration methods
- Secure shell (SSH)

8. Wireless Network Security

- Wireless network technologies
- Wireless application protocol (WAP)
- Wireless security vulnerabilities
- Solutions for network security vulnerabilities
- Site surveys

9. Security Topologies and Infrastructure Security



CENTRAL PIEDMONT COMMUNITY COLLEGE

CORPORATE & CONTINUING EDUCATION

- Firewall overview
- Security topologies
- Traffic control methods
- Configuring firewalls
- Network hardening, network security and physical security concerns
- Cabling and network security

10. Risk Analysis, Intrusion Detection and Business Continuity

- Risk identification
- Intrusion detection
- Elements of an incident response policy, forensics and disaster recovery
- Business continuity

11. Security Policy Management

- Security policy, privilege management
- Training secure practices and documentation

Prerequisites:

- Experience in network administration with focus on security
- Day to day technical information security experience
- Broad knowledge of security concerns and implementation

Method of Instruction:

- Instructor led lecture, hands on lab

Evaluation:

- None