


Course Outline

The Learning Center

Technology Training Center 

SECURITY + CERTIFICATION

Length of Course: 5 days

Prerequisites: CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP.

Course Objective: In this course, you'll build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network. Students will implement and monitor security on networks and computer systems, and respond to security breaches.

Course Outline:

Systems Security

- Differentiate among various systems security threats
- Explain the security risks pertaining to system hardware and peripherals
- Implement OS hardening practices and procedures to achieve workstation and server security
- Carry out the appropriate procedures to establish application security
- Implement security applications
- Explain the purpose and application of virtualization technology

Network Infrastructure

- Differentiate between the different ports and protocols, their respective threats and mitigation techniques
- Distinguish between network design elements and components
- Determine the appropriate use of network security tools to facilitate network security
- Apply the appropriate network tools to facilitate network security
- Explain the vulnerabilities and mitigations associated with network devices
- Explain the vulnerabilities and mitigations associated with various transmission media
- Explain the vulnerabilities and mitigations associated with wireless networking

Course Outline

The Learning Center

Technology Training Center



Access Control

- Identify and apply industry best practices for access control methods
- Explain common access control models and the differences between each
- Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges
- Apply appropriate security controls to file and print resources
- Compare and implement logical access control methods
- Summarize the various authentication models and identify the components of each
- Deploy various authentication models and identify the components of each
- Explain the difference between identification and authentication
- Explain and apply physical access security methods

Assessments & Audits

- Conduct risk assessments and implement risk mitigation
- Carry out vulnerability assessments using common tools
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning
- Use monitoring tools on systems and networks and detect security-related anomalies
- Compare and contrast various types of monitoring methodologies
- Execute proper logging procedures and evaluate the results
- Conduct periodic audits of system security settings

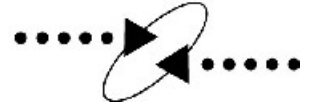
Cryptography

- Explain general cryptography concepts
- Explain basic hashing concepts and map various algorithms to appropriate applications
- Explain basic encryption concepts and map various algorithms to appropriate applications
- Explain and implement protocols
- Explain core concepts of public key cryptography
- Implement PKI and certificate management

Course Outline

The Learning Center

Technology Training Center



Organizational Security

- Explain redundancy planning and its components
- Implement disaster recovery procedures
- Differentiate between and execute appropriate incident response procedures
- Identify and explain applicable legislation and organizational policies
- Explain the importance of environmental controls
- Explain the concept of and how to reduce the risk of social engineering

This document was created with Win2PDF available at <http://www.daneprairie.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.