



551 W. Dimond Blvd
Anchorage, AK 99515
(907) 267-4216

SECURITY+ CERTIFICATION

Course Description: In this course, students will build on their knowledge and professional experience with computer hardware, operating systems, and networks as they acquire the specific skills required to implement basic security services on any type of computer network.

Course Content

Lesson 1: Security Fundamentals

- Security Building Blocks
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Lesson 2: Security Threats

- Social Engineering
- Software-Based Threats
- Hardware-Based Threats

Lesson 3: Hardening Internal Systems and Services

- Harden Operating Systems
- Harden Directory Services
- Harden DHCP Servers
- Harden File and Print Servers

Lesson 4: Hardening Internetwork Devices and Services

- Harden Internetwork Connection Devices
- Harden DNS and BIND Servers
- Harden Web Servers
- Harden File Transfer Protocol (FTP) Servers
- Harden Network News Transfer Protocol (NNTP) Servers
- Harden Email Servers
- Harden Conferencing and Messaging Servers

Lesson 5: Securing Network Communications

- Protect Network Traffic with IP Security (IPSec)
- Secure Wireless Traffic
- Harden a Web Browser
- Secure the Remote Access Channel

Lesson 6: Managing Public Key

Infrastructure (PKI)

- Install a Certificate Authority (CA) Hierarchy
- Harden a Certificate Authority
- Back Up a CA
- Restore a CA

Lesson 7: Managing Certificates

- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up Certificates and Private Keys
- Restore Certificates and Private Keys

Lesson 8: Enforcing Organizational Security Policies

- Enforce Corporate Security Policy Compliance
- Enforce Legal Compliance
- Enforce Physical Security Compliance
- Educate Users

Lesson 9: Monitoring the Security

Infrastructure

- Scan for Vulnerabilities
- Monitor for Intruders
- Set Up a Honeypot
- Respond to Security Incidents