

Security + Course Outline

1. Identifying Security Threats

- Identify Social Engineering Attacks
- Classify Software Attacks
- Identify Hardware Attacks

2. Hardening Internal Systems and Services

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

3. Hardening Internetwork Devices and Services

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

4. Securing Network Communications

- Topic 4A: Secure Network Traffic Using IP Security (IPSec)
- Topic 4B: Secure Wireless Traffic
- Topic 4C: Secure Client Internet Access
- Topic 4D: Secure the Remote Access Channel

5. Managing Public Key Infrastructure (PKI)

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

6. Managing Certificates

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

7. Enforcing Organizational Security Policy

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

8. Monitoring the Security Infrastructure

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

Appendix A: Authentication and Authorization

Appendix B: Understanding Media

Removable Media

Cabling

Appendix C: SecureSystems.doc

Appendix D: Security+ Exam Objectives Mapping

Appendix E: Automated Setup Instructions