

TestOut



Lesson Plans

CompTIA's Security+

Table of Contents

Table of Contents	2
Course Overview	3
Section 0-0: Introduction to Security	4
Section 1-0: Network Vulnerabilities and Attacks	5
Section 2-0: Cryptography	7
Section 3-0: Public Key Infrastructure (PKI)	9
Section 4-0: Authentication	11
Section 5-0: Network Infrastructure Security	12
Section 6-0: Network and Application Hardening.....	14
Section 7-0: Auditing and Intrusion Detection	16
Section 8-0: Communication Security	18
Section 9-0: Internet Services Security	20
Section 10-0: Operational Security	22
Section 11-0: Security Planning.....	24

Course Overview

0.0 Introduction to Security

This section introduces the concepts upon which security relies.

1.0 Network Vulnerabilities and Attacks

This section covers the ways in which networks are exposed to security risks.

2.0 Cryptography

This section covers the methods used to establish security through data encryption.

3.0 Public Key Infrastructure (PKI)

This section covers the combination of public and private key cryptography to provide authentication, confidentiality, integrity, and non-repudiation.

4.0 Authentication

This section covers the authentication as a means of confirming a user's identity, including the factors of authentication and implementation.

5.0 Network Infrastructure Security

This section covers the security considerations behind network design.

6.0 Network and Application Hardening

This section covers the security considerations behind network design.

7.0 Auditing and Intrusion Detection

This section covers the methods used to track network activity and to respond to network attacks.

8.0 Communication Security

This section covers the vulnerabilities in a network that allows users to connect to it remotely. The section also covers the tools available to protect remote access.

9.0 Internet Services Security

This section covers the security risks that come from Web-based services.

10.0 Operational Security

This section covers planning procedures for events that disrupt normal business operations. It also covers the methods for disaster recovery, like recovery and salvage team responsibilities and secondary site establishment.

11.0 Security Planning

This section covers security policy planning, risk analysis, and incident response, including investigatory procedures and evidence handling.

Section 0-0: Introduction to Security

Preparation

This section introduces the concepts upon which security relies. Prepare diagrams of the access control models to use for discussion during lecture.

Security+ Exam Objectives

1.1 Recognize and be able to differentiate and explain the following access control models.

- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)

Vocabulary: MAC, DAC, RBAC, TBAC, Access control

Focus Questions:

- Who is responsible for security?
- What are the primary security goals?
- What are the primary security services?
- How is accountability established?
- What is access control and why is it important to security?
- What are three models of access control?
- Which environments are best suited for each access control model?
- Why are classification schemes important?

Time

About 1 hour

Lecture Tips

- Explain what security is. What is a risk? What is the purpose of security?
- Discuss the CIA triad. How is it integral to achieving security goals?
- Explain the concept of accountability. Why is it important in a computing environment?
- Discuss the access control models. Allow the students to explore the differences among the models. Make sure that the students understand the difference between user-centric and nonuser-centric control.

Section 1-0: Network Vulnerabilities and Attacks

Preparation

This section covers the ways in which networks are exposed to security risks.

Security+ Exam Objectives

1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk.

- DOS / DDOS (Denial of Service / Distributed Denial of Service)
- Back Door
- Spoofing
- Man in the Middle
- Replay
- TCP/IP Hijacking
- Social Engineering
- Software Exploitation

1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk.

- Viruses
- Trojan Horses
- Logic Bombs
- Worms

1.6 Understand the concept of and know how reduce the risks of social engineering.

Vocabulary: Social engineering, Denial of Service, Distributed Denial of Service, Distributed Reflective Denial of Service, smurf, fraggle, ping flood, land attack, SYN flood, teardrop, DNS poisoning, spoofing, man-in-the-middle, replay, hijacking, identity spoofing, back door, cross-site scripting, buffer overflow, virus, worm trojan horse, logic bomb, dumpster diving, e-mail spoofing, impersonation

Focus Questions:

- By what means can attackers exploit software and devices?
- What are some common authentication attacks?
- How can you protect against authentication attacks?
- Why are buffer overflow errors prevalent?
- What are some examples of denial of service attacks?
- Why must networks protect against malicious code?
- By what means does malicious code enter an environment?
- What protections are available against malicious code?
- What is social engineering?

Time

About 2 hours

Lecture Tips

- Discuss Denial of Service attacks.
 - The source of the attacks.
 - The purpose of a DoS attack.
 - The different types of DoS attack.
 - DoS
 - DDoS
 - DRDoS
 - Examples of DoS attacks.
 - Smurf
 - Fraggle
 - Ping floods
 - SYN floods
 - Land
 - Teardrop
 - DNS poisoning
 - DoS Countermeasures
- Discuss Authentication Attacks.
 - Spoofing
 - Site Spoofing
 - Identity Spoofing
 - Spoofing Countermeasures
 - Man-in-the-Middle
 - Replay
 - Hijacking
- Discuss system exploitation.
 - Backdoor
 - Backdoor countermeasures
 - Software exploitation
 - Buffer overflow
 - Software exploitation countermeasures
- Discuss threats from malicious code.
 - Viruses
 - Worms
 - Trojan Horses
 - Logic Bombs
 - Malicious code countermeasures
- Discuss the threats from social engineering.
 - Countermeasures

Section 2-0: Cryptography

Preparation

This section covers the methods used to establish security through data encryption.

Security+ Exam Objectives

1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk.

- Weak Keys
- Mathematical
- Birthday
- Password Guessing
 - Brute Force
 - Dictionary

4.1 Be able to identify and explain the of the following different kinds of cryptographic algorithms.

- Hashing
- Symmetric
- Asymmetric

4.2 Understand how cryptography addresses the following security concepts.

- Confidentiality
- Integrity
 - Digital Signatures
- Authentication
- Non-Repudiation
 - Digital Signatures
- Access Control

4.4 Identify and be able to differentiate different cryptographic standards and protocols.

Vocabulary: cipher, symmetric cryptography, cryptography, block cipher stream cipher, key, key clustering, end-to-end encryption, link encryption, RSA, IDEA, blowfish, twofish, CAST, Rhine-doll, Rijndael, DES, Triple DES, 3DES, Rivest, one-way function, El Gamal, Elliptic Curve, Diffie-Hellman, hashing password guessing, analytic attack, implementation attack, statistical attack, brute force, known plaintext/ciphertext, chosen plaintext/ciphertext, adaptive plaintext/ciphertext, birthday, meet-in-the-middle, man-in-the-middle, replay, strong passwords

Focus Questions:

- What are the goals of cryptography?
- What are the differences between symmetric and asymmetric cryptography?
- What are some specific symmetric cryptography systems?

- What are some specific asymmetric cryptography systems?
- What is hashing used for?
- Why is key exchange and key distribution important?
- What is the difference between block cryptography and stream cryptography?
- What is triple DES and why was it developed? What replaced it?
- What is a one-way function and why is it important?
- What is a digital signature?
- What are some common cryptographic attacks?
- How does password guessing work?

Time

About 1 hour

Lecture Tips

- Discuss cryptography methods.
 - Algorithm
 - Cipher
 - Block Cipher
 - Stream Cipher
 - Key
 - Clustering (Key Clustering)
 - End-to-End Encryption
 - Link Encryption
- Explain the goals of cryptography.
 - Confidentiality
 - Integrity
 - Authentication
 - Non-repudiation
- Discuss the different types of cryptography.
 - Symmetric
 - Asymmetric
 - Hashing
- Explain what a cryptographic attack is. What are the goals of a cryptographic attack? What are the ways attackers try to achieve those goals? What countermeasures are available to defeat attacks?

Section 3-0: Public Key Infrastructure (PKI)

Preparation

This section covers the combination of public and private key cryptography to provide authentication, confidentiality, integrity, and non-repudiation.

Security+ Exam Objectives

4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).

- Certificates
 - Certificate Policies
 - Certificate Practice Statements
- Revocation
- Trust Models

4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles.

- Centralized vs. Decentralized
- Storage
 - Hardware vs. Software
 - Private Key Protection
- Escrow
- Expiration
- Revocation
 - Status Checking
- Suspension
 - Status Checking
- Recovery
 - M-of-N Control (Of M appropriate individuals, N must be present to authorize recovery)
- Renewal
- Destruction
- Key Usage
 - Multiple Key Pairs (Single, Dual)

Vocabulary: X.509, PKI, Public Key Cryptography, certificates, Registration Authority, RA, CA, Certificate Authority, root CA, subordinate CA, OCSP, CRL, certificate revocation list, online certificate status protocol, key length, key storage, escrow, revocation, expired certificate, revoked certificate, suspended certificate

Focus Questions:

- What is PKI?
- What are certificates and what are they used for?
- What is the role of a certificate authority?

- What are the elements of certificate management?
- Why is key management important?
- What are the aspects or elements of a key lifetime?

Time

About 1 hour

Lecture Tips

- Discuss PKI.
 - Certificates
 - Certificate Authority
 - Certificate Policies
 - Trust Models
 - Cross certification
 - Hierarchical
 - Single CA
 - Web of Trust
- Explain key management. What are good key management practices? What is the difference between centralized and decentralized key management? What are the advantages and disadvantages of each?

Section 4-0: Authentication

Preparation

This section covers the authentication as a means of confirming a user's identity, including the factors of authentication and implementation.

Security+ Exam Objectives

1.2 Recognize and be able to differentiate and explain the following methods of authentication.

- Kerberos
- CHAP (Challenge Handshake Authentication Protocol)
- Certificates
- Username / Password
- Tokens
- Multi-factor
- Mutual
- Biometrics

Vocabulary: biometrics, two-factor authentication, strong authentication, mutual authentication, retina scans, voice recognition, token, certificates, synchronous dynamic password, asynchronous dynamic password, PIN, passphrase, cognitive password, composition password, one-time password, single sign-on, kerberos, PAP, CHAP, EAP

Focus Questions:

- What are the three types of authentication?
- Why is secure authentication important?
- What is Kerberos?
- How do directory services relate to authentication?

Time

About 1 hour

Lecture Tips

- Authentication establishes a user's identity. How can authentication be performed? What are physical forms of authentication? What are non-physical forms of authentication? Which are more effective?
- Discuss the role of Kerberos in authentication. What are its weaknesses? Why is it effective?
- Explain how dial-up authentication works.
 - PAP
 - CHAP
 - PAP

Section 5-0: Network Infrastructure Security

Preparation

This section covers the security considerations behind network design.

Security+ Exam Objectives

3.1 Understand security concerns and concepts of the following types of devices.

- Firewalls
- Routers
- Switches
- Workstations
- Servers

3.2 Understand the security concerns for the following types of media.

- Coaxial Cable
- UTP / STP (Unshielded Twisted Pair / Shielded Twisted Pair)
- Fiber Optic Cable
- Removable Media
 - Tape
 - CD-R (Recordable Compact Disks)
 - Hard Drives
 - Diskettes
 - Flashcards
 - Smartcards

3.3 Understand the concepts behind the following kinds of Security Topologies.

- Security Zones
 - DMZ (Demilitarized Zone)
 - Intranet
 - Extranet
- VLANs (Virtual Local Area Network)
- NAT (Network Address Translation)

Vocabulary: ports, TCP, UDP, IP, transmission control protocol, user datagram protocol, Internet protocol, router, switch, VLAN, server, workstation, firewall, proxy, stateful inspection firewall, media security, UTP, STP, fiber optic, coax, packet filtering firewall, application level gateway, gateway, DMZ, demilitarized zone, screened subnet, acid dipping

Focus Questions:

- Why is a thorough knowledge of TCP/IP important for security?
- What are common devices found on a network?
- What are the common types of firewalls?
- How can a firewall be deployed?
- What are security zones?

- Why use a DMZ?
- What is NAT and why is it useful?
- What is a VLAN?
- How can you manage network cabling and data store media securely?

Time

About 1 hour

Lecture Tips

- Discuss network design. What aspects of network design relate to security? How do these aspects of network design contribute to a secure networking environment?
- Explain the concept of firewalls along with the different types of firewalls. Point out the advantages and disadvantages of each type of firewall. Explain the circumstances under which each type of firewall performs best.
 - Packet Filtering
 - Circuit level proxy
 - Application level gateway
 - Stateful inspection firewall
- Explain the ways that security zones can be designed to increase network security.
- Cable vulnerability constitutes an ongoing security concern. Discuss the types of cabling available. Which cabling types are less susceptible to security breach? What is the trade off between a high degree of cable security and a low degree of cabling security?

Section 6-0: Network and Application Hardening

Preparation

This section covers the methods used to strengthen security by reducing the vulnerabilities of devices and software.

Security+ Exam Objectives

- 1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols.
- 3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system.
 - OS / NOS (Operating System / Network Operating System) Hardening
 - File System
 - Updates (Hotfixes, Service Packs, Patches)
 - Network Hardening
 - Updates (Firmware)
 - Configuration
 - Enabling and Disabling Services and Protocols
 - Access Control Lists
 - Application Hardening
 - Updates (Hotfixes, Service Packs, Patches)
 - File / Print Servers
 - Data Repositories
 - Directory Services
 - Databases

Vocabulary: OS hardening, hardening, NetBIOS, Web server, FTP server, NNTP server, e-mail server, MIME, anonymous FTP, SMTP relay

Focus Questions:

- What is involved in OS hardening?
- What is required to harden a network?
- Why is securing applications important?
- What is a security baseline?
- What publicly accessible services need to be locked down?
- How do system updates relate to system security?

Time

About 1 hour

Lecture Tips

- Discuss how to use a security baseline.

- Discuss OS hardening.
 - NTFS offers native file security. FAT and FAT32 do not.
 - System updates include fixes for security vulnerabilities
 - Removing services (like the command line or the Run dialog box) keeps users from performing operations on the system that violate the security baseline.
- Explain the steps of network hardening.

Section 7-0: Auditing and Intrusion Detection

Preparation

This section covers the methods used to track network activity and to respond to network attacks.

Security+ Exam Objectives

- 1.7 Understand the concept and significance of auditing, logging and system scanning.
- 3.1 Understand security concerns and concepts of the following types of devices.
 - IDS (Intrusion Detection System)
 - Network Monitoring / Diagnostics
- 3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system.
 - Network Based
 - Active Detection
 - Passive Detection
 - Host Based
 - Active Detection
 - Passive Detection
 - Honey Pots

Vocabulary: padded cell, honey pot, IDS, auditing, logging, port scanning, system scanning

Focus Questions:

- What is auditing?
- What is the goal or purpose of auditing?
- Why is penetration testing important?
- What is port scanning?
- What is an IDS?
- What is a network based IDS useful for?
- Why would you deploy a host based IDS?
- How can IDS respond to incidents?
- What is a honey pot?

Time

About 1 hour

Lecture Tips

- Discuss the ways auditing can improve security. What information can expose system vulnerabilities? Explain that auditing and logging take a lot of time if they're done effectively.

- Discuss the different types of intrusion detection systems. What is the difference between a host IDS and a network IDS? What is a detection method? What are appropriate responses to an attack? Which responses are most effective and why?

Section 8-0: Communication Security

Preparation

This section covers the vulnerabilities in a network that allows users to connect to it remotely. The section also covers the tools available to protect remote access.

Security+ Exam Objectives

2.1 Recognize and understand the administration of the following types of remote access technologies.

- 802.1x
- VPN (Virtual Private Network)
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)
- L2TP / PPTP (Layer Two Tunneling Protocol / Point to Point Tunneling Protocol)
- SSH (Secure Shell)
- IPSEC (Internet Protocol Security)
- Vulnerabilities

2.3 Recognize and understand the administration of the following Internet security concepts.

- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer)

2.6 Recognize and understand the administration of the following wireless technologies and concepts.

- WTLS (Wireless Transport Layer Security)
- 802.11 and 802.11x
- WEP / WAP (Wired Equivalent Privacy / Wireless Application Protocol)
- Vulnerabilities
 - Site Surveys

3.3 Understand the concepts behind the following kinds of Security Topologies.

- Tunneling

Vocabulary: site survey, 802.11x, WEP, WAP, WML, WAE, WTP, WDP, PBX, RAS, remote access server, PPTP, L2F, L2TP, IPsec, AH, ESP, SSL, TLS, HTTPS, SHTTP, RADIUS, TACACS

Focus Questions:

- What are common remote access security issues?
- What security functions can a remote access server provide?
- How can you secure a PBX?
- What is RADIUS and TACACS?
- What can SSH be used for?

- What are common VPN protocols?
- What is IPSec?
- What are SSL and TLS?
- What mechanisms can be used to protect communications?
- What are the two primary means of securing wireless communications?
- What are some vulnerabilities of wireless networks?
- Can VPNs be used to secure wireless communications?

Time

About 1 hour

Lecture Tips

- Explain how modems can become a source of security vulnerabilities.
 - Very common and often ignored.
 - Prone to have weaker security protections.
 - Security policy may ignore them.
 - Power users may bypass firewall through modems.
- Discuss the different tools available for securing remote access, including PBX systems.
- Explain how to secure a VPN connection. Discuss the protocols available. What affects the choice of protocol for securing VPN connections?
- Discuss the wireless connection standards. How are wireless connections vulnerable to attacks? What are the differences between the two standards for protecting wireless networks?

Section 9-0: Internet Services Security

Preparation

This section covers the security risks that come from Web-based services.

Security+ Exam Objectives

2.2 Recognize and understand the administration of the following email security concepts.

- S/MIME (Secure Multipurpose Internet Mail Extensions)
- PGP (Pretty Good Privacy) like technologies
- Vulnerabilities
 - SPAM
 - Hoaxes

2.3 Recognize and understand the administration of the following Internet security concepts.

- Instant Messaging
 - Vulnerabilities
 - Packet Sniffing
 - Privacy
- Vulnerabilities
 - Java Script
 - ActiveX
 - Buffer Overflows
 - Cookies
 - Signed Applets
 - CGI (Common Gateway Interface)
 - SMTP (Simple Mail Transfer Protocol) Relay

2.4 Recognize and understand the administration of the following directory security concepts.

- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- LDAP (Lightweight Directory Access Protocol)

2.5 Recognize and understand the administration of the following file transfer protocols and concepts.

- S/FTP (File Transfer Protocol)
- Blind FTP (File Transfer Protocol) / Anonymous
- File Sharing
- Vulnerabilities
 - Packet Sniffing
 - 8.3 Naming Conventions

Vocabulary: Web server, FTP server, CGI scripting, ASP, JavaScript, VBScript, client-side scripting, server-side scripting, cookies, ActiveX, directory traversals, anonymous FTP, blind FTP, FTP sharing, SMTP relay, S/MIME, MIME, PGP,

SMTP, POP3, IMAP4, IM, instant messaging, e-mail, eDirectory, Active Directory, LDAP, SASL, SSL

Focus Questions:

- What are some common vulnerabilities to Web communications?
- What are cookies?
- How can Web traffic be secured?
- What is IM? What weaknesses are inherent in IM?
- What are the vulnerabilities of FTP? How can FTP be secured?
- What security issues are related to e-mail? How can e-mail be secured?
- What are the protocols used by common e-mail solutions?
- What is a directory service? What is LDAP?
- What can you do to secure a directory?

Time

About 1 hour

Lecture Tips

- Discuss the countermeasures available to secure Web servers. Discuss which countermeasures work best with specific threats. What are the advantages and disadvantages of the various countermeasures? How do those factors influence the choice of countermeasures?
- Discuss the ways to secure Web-based communications, including email and instant messaging. How can the security vulnerabilities of email and IM influence an organization's security policy? What are some safe use practices? What are countermeasures to attacks?
- Discuss LDAP. What characteristics of LDAP aid security? What are LDAP security vulnerabilities and countermeasures?

Section 10-0: Operational Security

Preparation

This section covers planning procedures for events that disrupt normal business operations. It also covers the methods for disaster recovery, like recovery and salvage team responsibilities and secondary site establishment.

Security+ Exam Objectives

5.1 Understand the application of the following concepts of physical security.

- Access Control
 - Physical Barriers
 - Biometrics
- Social Engineering
- Environment
 - Wireless Cells
 - Location
 - Shielding
 - Fire Suppression

5.2 Understand the security implications of the following topics of disaster recovery.

- Backups
 - Off Site Storage
- Secure Recovery
 - Alternate Sites
- Disaster Recovery Plan

5.3 Understand the security implications of the following topics of business continuity.

- Utilities
- High Availability / Fault Tolerance
- Backups

Vocabulary: Recovery team, Salvage team, BCP, DRP, Downtime, Prioritization, Mutual Aid Agreement, Hot site, Warm site, Cold site, Service Bureau

Focus Questions:

- What can affect business continuity?
- What is the difference between a business continuity plan and a disaster recovery plan?
- What is the primary purpose of a BCP or DRP?
- How can continuity be supported?
- What are the steps in developing a BCP and DRP?
- What are some examples of secondary processing sites?
- Why is physical security important?

- How does fire suppression relate to security?
- Why are backups important?
- What are some mechanisms to protect your facility?

Time

About 1 hour

Lecture Tips

- Discuss the types of disruptions businesses commonly experience, including layoffs, terminations, natural disasters, and strikes. Discuss recent (or past) examples of disruptive events in the business world. Explain that a disruptive event is something that keeps a business from normal functions. Operational security planning must attempt to anticipate all types of disruptive events.
- Discuss the elements of a disaster recovery procedure. What are the responsibilities of the different teams? When would these responsibilities overlap? What elements of a business should return first to the primary site? Why? What are the best indicators that a disaster is over?
- Discuss the use of secondary sites in operational security planning. How do the site types differ? Given the advantages and disadvantages of each, what other factors influence the choice of secondary site?

Section 11-0: Security Planning

Preparation

This section covers security policy planning, risk analysis, and incident response, including investigatory procedures and evidence handling.

Security+ Exam Objectives

3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system.

- Incident Response

5.4 Understand the concepts and uses of the following types of policies and procedures.

- Security Policy
 - Acceptable Use
 - Due Care
 - Privacy
 - Separation of Duties
 - Need to Know
 - Password Management
 - SLAs (Service Level Agreements)
 - Disposal / Destruction
 - HR (Human Resources) Policy
 - Termination (Adding and revoking passwords and privileges, etc.)
 - Hiring (Adding and revoking passwords and privileges, etc.)
 - Code of Ethics
- Incident Response Policy

5.5 Explain the following concepts of privilege management.

- User / Group / Role Management
- Single Sign-on
- Centralized vs. Decentralized
- Auditing (Privilege, Usage, Escalation)
- MAC / DAC / RBAC (Mandatory Access Control / Discretionary Access Control / Role Based Access Control)

5.6 Understand the concepts of the following topics of forensics.

- Chain of Custody
- Preservation of Evidence
- Collection of Evidence

5.7 Understand and be able to explain the following concepts of risk identification.

- Asset Identification
- Risk Assessment

- Threat Identification
- Vulnerabilities

5.8 Understand the security relevance of the education and training of end users, executives and human resources.

- Communication
- User Awareness
- Education
- On-line Resources

5.9 Understand and explain the following documentation concepts.

- Standards and Guidelines
- Systems Architecture
- Change Documentation
- Logs and Inventories
- Classification
 - Notification
- Retention / Storage
- Destruction

Vocabulary: Policies, Standards, Guidelines, Procedures, Acceptable Use Policy, Due care, Due diligence, Separation of Duties, Personnel Control, Service Level Agreement (SLA), Media Control, Code of Ethics, Risk Management, Vulnerability, Threat Agent, Threat, Risk, Exposure, Countermeasure, Quantitative Analysis, Qualitative Analysis, CIRT, Evidence Life Cycle

Focus Questions:

- What is a security policy?
- Who is responsible for the development and implementation of a security policy?
- What is an acceptable use policy?
- How does due care and due diligence relate to security?
- What is separation of duties?
- What is the principle of least privilege?
- What is a service level agreement?
- How do ethics relate to security?
- What are the elements of risk management?
- What are the proper responses to risk?
- How should countermeasures be selected?
- Why is security awareness training important?
- How does documentation aid in supporting security?
- What is a security incident?
- How should you respond to security violations?
- Who is responsible to managing breaches of security?
- Why are cyber crime investigations difficult?
- What is required to ensure admissibility of evidence in court?

- What are the common types of evidence?
- Is computer based hearsay evidence ever admissible?
- What is the evidence chain of custody?

Time

About 1 hour

Lecture Tips

- Explain how to establish a security policy.
 - Security policy components
 - Separation of duties
 - Personnel control
 - SLAs
 - Media controls
 - Code of ethics
- Discuss risk analysis.
 - Qualitative versus Quantitative
 - What are the differences?
 - Which is easiest? Which is most effective?
 - Risk analysis steps
 - Countermeasure criteria. What is the measure of an effective countermeasure?
- Discuss incident response. How does an organization know it needs to respond to an incident? What are proper responses to incidents?
- Discuss how to conduct investigations into incidents.
 - Suspects generally need MOM (Motive, Opportunity, Means)
 - Evidence life cycle
 - Chain of custody
 - Rules of evidence
 - Evidence admissibility
 - Types of evidence