



Lesson Plans

Security+

(Exam SY0-201)

Version 4.0

Table of Contents

Table of Contents	1
Course Overview	3
Section 0.1: Course Overview	5
Section 0.2: Windows Networking	6
Section 1.1: Access Control Models	8
Section 1.2: Authentication	9
Section 1.3: User Accounts and Passwords	11
Section 1.4: Authorization	13
Section 1.5: Physical Security	15
Section 1.6: Access Control Best Practices	17
Section 2.1: Cryptography	18
Section 2.2: Hashing	20
Section 2.3: Symmetric Encryption	22
Section 2.4: Asymmetric Encryption	24
Section 2.5: Public Key Infrastructure (PKI)	26
Section 2.6: Cryptography Implementations	28
Section 2.7: Secure Protocols	29
Section 3.1: OSI Model Review	31
Section 3.2: Protocols and Ports	32
Section 3.3: Network Devices	34
Section 3.4: Network Authentication	35
Section 3.5: Remote Access	37
Section 3.6: RADIUS and TACACS+	39
Section 3.7: Network Address Translation	41
Section 4.1: Reconnaissance	43
Section 4.2: Denial of Service (DoS)	44
Section 4.3: Session and Spoofing Attacks	46
Section 4.4: DNS Attacks	48
Section 4.5: Switch Attacks	49
Section 5.1: Firewalls	50
Section 5.2: Security Zones	52
Section 5.4: Switch Security	55
Section 5.5: Security Solutions	57
Section 5.6: Transmission Media	59
Section 5.7: Wireless	61
Section 5.8: Mobile Devices	63
Section 5.9: Telephony	64
Section 6.1: Malware	65
Section 6.2: Device Vulnerabilities	67
Section 6.3: Hardening	68
Section 6.4: Removable Media	70
Section 6.5 BIOS Security	72
Section 6.6: File and Print Security	73
Section 7.1: Web Applications	75

Section 7.2: Web Attacks.....	77
Section 7.3: E-mail.....	79
Section 7.4: Network Applications	81
Section 7.5: Virtualization	82
Section 8.1: Security Policies	83
Section 8.2: Disaster Planning	85
Section 8.3: Redundancy	86
Section 8.4: Backup and Restore	88
Section 8.5: Environmental Controls.....	90
Section 8.6: Social Engineering.....	92
Section 8.7: Incident Response	94
Section 9.1: Risk Management	96
Section 9.2: Vulnerability Assessment	97
Section 9.3: Penetration Testing	99
Section 9.4: Monitoring	101
Section 9.5: Logging and Auditing.....	103
Practice Exams.....	105

Course Overview

This course prepares students for CompTIA's Security+ Certification Exam: SY0-201. It focuses on controlling security, access, and the network infrastructure.

Module 0 – Introduction

This module introduces the course, recommended prerequisites, and basic security terms that will be referenced throughout the course. A review of configuring Active Directory and Group policy to secure a Windows based network is presented.

Module 1 – Access Control

This module provides an overview of access control models, increasing security using authentication methods, configuring user accounts and passwords to control and restrict access to network resources, and authorization concepts to control access to resources. Students will also learn about controls that can be used to physically protect assets from threats and best practices for controlling access to resources.

Module 2 – Cryptography

This module examines the fundamentals of cryptography. Students will become familiar with hashing, symmetric encryption, asymmetric encryption concepts and how they can be combined to take advantage of the strengths of each. Core concepts of Public Key Infrastructure (PKI) are discussed as well as secure protocols that can be used to provide security services to new or existing protocols.

Module 3 – Network Infrastructure

In this module students will learn elements of the network infrastructure. A review of the OSI Model is presented as well as the major protocols and ports used for communication between network hosts. Students will become familiar with the characteristics of common network devices (hub, switch, and router) and using network authentication to prove user identity before allowing access to network resources. Implementing remote access and using RADIUS and TACACS+ to centralize the administration of remote access policies are discussed. Students will learn how to connect a private network to the Internet using Network Address Translation.

Module 4 – Network Attacks

This module teaches the students about different types of network attacks and the countermeasures to prevent them. Reconnaissance is used by an attacker to gather information about an organization prior to an attack. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks effect system availability. Session attacks capture data that can be used at a later date. Spoofing attacks hide the source of packets or redirect traffic to another location. DNS attacks redirect traffic to fake Web sites. Switch attacks are perpetrated against switches.

Module 5– Network Security

This module discusses elements that can be used to increase network security; firewalls, security zones, intrusion detection systems, and switch features. Network security solutions include proxy servers, Internet content filter, and Network Access Control (NAC). Vulnerabilities of transmission media (cables) are presented. Students will become familiar with security considerations for wireless networking and mobile devices.

Module 6 – System Security

This module examines system security concerns that the students will need to be aware of; types of malware, best practices for protection against malware, network device vulnerabilities, and recommendations for hardening systems and securing removable media. Students will learn BIOS settings that can be configured to enhance system security and how to employ security controls to file and print resources.

Module 7 – Application Security

In this module students will learn how to establish application security for Web applications, e-mail, and network applications (peer-to-peer and instant messaging). They will also learn the advantages and disadvantages of using virtualization technology.

Module 8 – Organizational Security

This module teaches the students the elements that should be in place to secure an organization; security policies, disaster recovery procedures, redundancy planning, and backup and restore procedures. Environmental controls help to protect computer systems from environmental concerns such as heat, humidity, water and fire. Students will become familiar with different types of social engineering attacks and countermeasures to these attacks. They will also learn the appropriate response to an incident to ensure that they can recover from the current attack and protect against future attacks.

Module 9 – Assessments and Audits

This module examines assessments and audits that can be made on a system to help troubleshoot and secure the system. Assessments include; risk assessments, vulnerability assessments, and assessments by penetration testing. Monitoring tools can be used to identify security-related irregularities. Procedures to implement logging and auditing on a system are discussed.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification exam.

Section 0.1: Course Overview

Summary

This section provides an overview of this course which is designed to prepare students for the CompTIA 2008 Edition of the Security+ Certification Exam SY0-201. The Security+ certification is a vendor neutral certification designed to recognize foundation level security skills and knowledge.

Security terms that are commonly used in the IT industry and will be used throughout the course are defined in this section.

Recommended prerequisites include:

- CompTIA Network+ certification or equivalent knowledge and experience
- A minimum of two years working in network administration with a focus on security

Security+ Objectives

- 5.1 Explain general cryptography concepts.
 - Confidentiality
 - Integrity and availability
 - Non-repudiation

Lecture Focus Questions:

- What is the difference between *integrity* and *non-repudiation*?
- What process provides confidentiality by converting data into a form that it is unlikely to be usable by an unintended recipient?
- What are the three main goals of security for the *CIA of Security*?
- Which security expression refers to verifying that someone is who they say they are?
- In security terms what does AAA refer to?

Time

About 7 minutes

Number of Exam Questions

2 questions

Section 0.2: Windows Networking

Summary

This section ensures the students will have the foundational knowledge they need of Active Directory and Group policy to correctly configure and secure a Windows based network. Active Directory consists of the following components:

- Domain
- Organization Unit (OU)
- Generic Containers
- Objects
- Domain Controller

Group Policy Objects (GPOs) are divided into two categories:

- Computer configuration
- User configuration

Students will learn how to:

- Configure objects in Active Directory to control access to network resources.
- Using Group Policy Management, configure security settings such as password policy settings to define requirements for user passwords.
- Using Group Policy Management, configure user right assignments to identify actions users can perform on a system.
- Create and link a new Group Policy Object (GPO). Enable security settings to apply multiple settings to multiple objects.

Security+ Objectives

- 1.3 Implement OS hardening practices and procedures to achieve workstation and server security.
 - Group policies
- 3.5 Compare and implement logical access control methods.
 - Group policies
 - Password policy
 - Domain password policy
- 5.1 Explain general cryptography concepts.
 - Confidentiality
 - Integrity and availability
 - Non-repudiation

Lecture Focus Questions:

- How does the security of a workgroup differ from the security for Active Directory?
- What is the function of an organizational unit (OU) in organizing network resources within a domain?
- What is the difference between organizational units (OU) and generic containers?
- What are common objects identified within the Active Directory?
- When are *computer* configuration policies initially applied? When are *user* configuration policies applied?

Time

About 20 minutes

Lab/Activity

- Create and Link a GPO

Section 1.1: Access Control Models

Summary

This section provides an overview of the following access control models:

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

Students will learn how to:

- Implement DAC by configuring a discretionary access control list (DACL).

Security+ Objectives

- 3.2 Explain common access control models and the differences between each.
 - MAC
 - DAC
 - Role & Rule based access control

Lecture Focus Questions:

- How does the discretionary access control (DAC) provide access control?
- What type of entries does the discretionary access control list (DACL) contain?
- What is the function of each of the two types of labels used by the Mandatory Access Control (MAC) access model?
- What is the difference between *role-based* access control and *rule-based* access control?
- How are Rule-Based Access Control and Mandatory Access Control (MAC) similar?

Time

About 15 minutes

Number of Exam Questions

8 questions

Section 1.2: Authentication

Summary

This section discusses the process of proving the identity of a user before they are allowed to access the resources of a network. This process consists of two parts:

- Identification
- Authentication

A user can prove identity to an authentication server in the following ways:

- Type 1 Something you know
- Type 2 Something you have
- Type 3 Something you are

Terms used to measure the effectiveness of authentication solutions include:

- False negative
- False positive
- Crossover error rate
- Processing rate

A combination of authentication methods that can be used to increase security include:

- Two-factor, three-factor, and multi-factor
- Strong
- One-factor
- Mutual

When using biometrics remember that they must be

- Unique
- Combined with other authentication methods for greater security
- Accurate
- Physically enrolled

Single Sign On (SSO) allows a user to log in once to a network and access all authorized resources on the network without additional login credentials or passwords.

Students will learn the advantages and disadvantages of using SSO authentication in enterprise environments.

Students will learn how to:

- Use a biometric scanner to enroll (record) fingerprints that can be used for authentication.
- Configure fingerprint settings to automate execution of an application.
- Use single sign-on to access all authorized resources on the network.

Security+ Objectives

- 3.6 Summarize the various authentication models and identify the components of each.
 - One, two and three-factor authentication
 - Single sign-on
- 3.8 Explain the difference between identification and authentication (identity proofing).

Lecture Focus Questions:

- Which authentication type is the most common?
- Which form of authentication is generally considered the strongest?
- What is the difference between *synchronous* and *asynchronous* token devices?
- Which type of biometric processing error is more serious, a false positive or a false negative? Why?
- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?
- What are the main advantages of SSO authentication? Disadvantages?

Time

About 40 minutes

Number of Exam Questions

15 questions

Section 1.3: User Accounts and Passwords

Summary

This section explores methods used on user accounts and passwords to control and restrict access to network resources. Methods used include:

- Account lockout
 - Account lockout threshold
 - Account lockout duration
 - Reset account lockout counter after
- Account restrictions
- Account (password) policies

Students will become familiar with:

- Methods administrators use to control user account and password security
- Methods hackers use to discover passwords
- Strategies to protect against password attacks

Students will learn how to:

- Control logical access by configuring user account and account lockout policies.
- Configure day/time restrictions, computer restrictions, and expiration dates for user accounts.
- Enable and disable user accounts.
- Configure the password policy for a domain.
- View system logon activity by using a key logger tool.

Security+ Objectives

- 3.5 Compare and implement logical access control methods.
 - Group policies
 - Password policy
 - Domain password policy
 - User names and passwords
 - Time of day restrictions
 - Account expiration
- 6.4 Identify and explain applicable legislation and organizational policies.
 - Password complexity

Lecture Focus Questions:

- What characteristics on a Microsoft system typically define a *complex* password?
- What is the *clipping level* and how does it affect an account login?

- What does the minimum password age setting prevent?
- What setting lets you take actions for a specified number of incorrect logon attempts?
- As a best practice, what should you do to user accounts that will not be used for an extended period of time?
- When is *salting* useful in passwords? What advantages does it provide?

Time

About 40 minutes

Lab/Activity

- Configure User Account Restrictions
- Configure Account Policies

Number of Exam Questions

8 questions

Section 1.4: Authorization

Summary

In this section students will learn that authorization is the process of controlling access to resources. The following concepts are examined:

- Group
- Access Control List (ACL)
- Discretionary Access List (DACL)
- System Access List (SACL)
- Assigning permissions to a group
- User rights
- Security principal
- Security ID (SID)
- Access Token

Students will learn how to:

- Create a group and add members to the group.
- Examine the elements of an access token using **whoami /all**.
- After changes to user privileges, gain access to newly assigned resources by creating a new access token (logging on again).

Security+ Objectives

- 3.3 Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.
- 3.5 Compare and implement logical access control methods.
 - ACL
 - Logical tokens

Lecture Focus Questions:

- What three types of information make up an access token?
- How is the access token used to control access to resources?
- On a Microsoft system, when is the access token generated?
- What types of objects are considered security principals?
- What is the difference between a *discretionary* access list (DACL) and a *system* access list (SACL)?

Time

About 25 minutes

Lab/Activity

- Create a Group

Number of Exam Questions

9 questions

Section 1.5: Physical Security

Summary

In this section students will learn about physically protecting assets from threats. Physical control measures discussed include:

- Perimeter barriers
- Close-circuit television (CCTV)
- Doors
- Door locks
- Physical access logs
- Physical access controls

Students will become familiar with the

- The sequence for deploying physical security.
- Implementing a layered defense system.
- Performing physical inspections and addressing violations.

Security+ Objectives

- 3.9 Explain and apply physical access security methods.
 - Physical access logs/lists
 - Hardware locks
 - Physical access control -- ID badges
 - Door access systems
 - Man-trap
 - Physical tokens
 - Video surveillance -- camera types and positioning

Lecture Focus Questions:

- What types of physical controls can be implemented to protect the perimeter of a building?
- What is the difference between a *mantrap* and a *double entry* door?
- What types of doors are effective deterrents to piggybacking?
- How does an anti-passback system work?
- What types of devices are best suited for interior motion detection? Perimeter motion detection?
- How do physical access logs help to increase the security of a facility?

Time

About 20 minutes

Number of Exam Questions

11 questions

Section 1.6: Access Control Best Practices

Summary

This section examines best practices for controlling access to resources. The following security principles are presented:

- Principle of least privilege
- Need to know
- Separation of duties
- Job rotation
- Defense-in-depth

Students will learn how to:

- Enable and disable User Account Control (UAC).
- Use alternate credentials to run programs that require elevated privileges.

Security+ Objectives

- 3.1 Identify and apply industry best practices for access control methods.
 - Implicit deny
 - Least privilege
 - Separation of duties
 - Job rotation

Lecture Focus Questions:

- What is the difference between *implicit deny* and *explicit allow*?
- What is the difference between *implicit deny* and *explicit deny*? Which is the strongest?
- How does implementing the principle of separation of duties increase the security in an organization?
- What aspects of security does job rotation provide?
- How do creeping privileges occur?

Time

About 20 minutes

Number of Exam Questions

7 questions

Section 2.1: Cryptography

Summary

This section provides the fundamentals of using cryptography to secure a message during transmission. Security services provided by cryptographic systems include:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Students will become familiar with the following terms related to cryptography:

- Plaintext
- Cipher text
- Cryptographer
- Cryptanalysis
- Cryptosystem
- Cryptology
- Key
- Algorithm
- Encryption
- Decryption
- Steganography

Security+ Objectives

- 5.1 Explain general cryptography concepts.
 - Steganography
 - Confidentiality
 - Integrity and availability
 - Non-repudiation
- 5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.
 - One time pad

Lecture Focus Questions:

- From a security standpoint, what is the difference between integrity and non-repudiation of data?
- What is a legitimate use for cryptanalysis?
- How is the strength of a cryptosystem related to the length of the key?
- Which of the following is typically kept secret, the encryption algorithm or the key (or both)?

- What is the difference between a transposition cipher and a substitution cipher?
- What is a legitimate use of steganography?

Time

About 10 minutes

Number of Exam Questions

5 questions

Section 2.2: Hashing

Summary

This section discusses using hashing to ensure the data integrity of files in transit. Hashing data produces a hash value that will change dramatically even if a very minor change is made to the data. Both the sender and receiver use the same hashing algorithm on the data. When the hashes match, the receiver can be assured that the data has not be modified.

Predominate hashing algorithms in use today are:

- MD-5 generates a message digest of 128 bits.
- SHA-1 generates a message digest of 160 bits.

Use hashing for the following:

- File integrity
- Secure logon credential exchange

The following concepts about hashes are discussed:

- Strong hashes
- High amplification
- Collision
- Collision resistance
- Birthday attack
- Rainbow table
- Salting the hash

Students will learn how to:

- Generate a hash value for a file.
- Compare hash values to verify message integrity.
- Analyze the strength of passwords by using a rainbow table to perform a cryptanalysis attack on the hashed values of passwords.

Security+ Objectives

- 5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.
 - SHA
 - MD5
 - LANMAN
 - NTLM

Lecture Focus Questions:

- What security goal or function is provided by hashes?
- Why doesn't a hash provide message encryption?
- When comparing MD-5 and SHA-1, which method provides greater security? Why?
- What is a *collision* and why is this condition undesirable in a hashing algorithm?
- Why is *high amplification* an indicator of a good hashing algorithm?
- How does *salting the hash* help to mitigate rainbow attacks?

Time

About 30 minutes

Number of Exam Questions

7 questions

Section 2.3: Symmetric Encryption

Summary

This section presents information about using symmetric encryption to secure data by encrypting and decrypting the data. Symmetric key encryption:

- Uses only one key.
- Is well suited for bulk encryption
- Requires both parties to exchange the secret key using a secure channel.
- Requires a unique shared key for each pair of communicating entities
- Uses two algorithm types
 - Block ciphers
 - Stream ciphers
- Includes the following methods:
 - Rivest Cipher (RC)
 - International Data Encryption Algorithm (IDEA)
 - Carlisle Adams Stafford Tavares (CAST)
 - Twofish
 - Blowfish
 - Data Encryption Standard (DES)
 - Triple DES (#DES)
 - Advanced Encryption Standard (AES)

Students will learn how to:

- Perform a brute force analysis of encrypted data to recover original data.

Security+ Objectives

- 5.1 Explain general cryptography concepts.
 - Symmetric key
 - Confidentiality
 - Comparative strength of algorithms
 - Use of proven technologies
- 5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.
 - DES
 - 3DES
 - AES
 - AES256

Lecture Focus Questions:

- A user needs to communicate security with 5 other users using symmetric key encryption. How many keys are required?
- How are symmetric keys typically exchanged between communication partners?
- What is an advantage of increasing the number of bits in the key? What is a disadvantage?
- Why are symmetric key stream ciphers considered to be slower than symmetric key block ciphers?
- Considering symmetric key stream ciphers and block ciphers, which would you select to process large amounts of data? Why?
- How does 3DES differ from DES?

Time

About 20 minutes

Number of Exam Questions

6 questions

Section 2.4: Asymmetric Encryption

Summary

This section examines using asymmetric encryption to secure data. Asymmetric encryption:

- Uses two keys that are mathematically related
 - Public key – made available to anyone
 - Private key – is kept secret
- Is created by a local security authority
- Requires high CPU usage
- Requires only two keys per user
- Provides confidentiality, strong authentication, and non-repudiation used for:
 - Digital signing
 - Key exchange
 - Data encryption
- Uses the following asymmetric encryption protocols
 - Diffie-Hellman
 - ElGamal
 - RSA
 - Elliptic curve cryptography (ECC)
- Uses the following protocols:
 - SSL/TLS
 - IPSec
 - VPNs (PPTP, L2TP, SSTP)
 - S/MIME and PGP for e-mail security
 - SSH tunnels

Security+ Objectives

- 5.1 Explain general cryptography concepts.
 - Asymmetric key
 - Confidentiality
 - Non-repudiation
 - Digital signatures
 - Use of proven technologies
- 5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.
 - RSA
 - PGP
 - Elliptic curve

Lecture Focus Questions:

- How do public keys differ from private keys? What is the relationship between the two?
- For which type of environment is asymmetric cryptography best suited?
- Why does asymmetric encryption require fewer keys than symmetric encryption?
- What services are provided by the cryptographic service provider (CSP)?
- What is the main use for the Diffie-Hellman protocol?

Time

About 20 minutes

Number of Exam Questions

7 questions

Section 2.5: Public Key Infrastructure (PKI)

Summary

In this section students will explore information about managing certificates and Public Key Infrastructure. The following concepts are discussed:

- Using a digital certificate to provide non-repudiation
- Using a public key infrastructure to manage certificates
- Using SSL and certificates to secure Web transactions

Terms the students will learn include:

- Certificate Authority (CA)
- Certificate Practice Statement (CPS)
- Cryptographic Service Provider (CSP)
- Online Certificate Status Protocol (OCSP)
- Certificate Revocation List (CRL)
- Registration Authority (RA)
- X.509
- Enrollment agent

Students will learn how to:

- Manage certificates by requesting, approving, and installing certificates.
- Revoke a certificate and publish it to the CRL.
- Create and configure a subordinate CA.
- Manage certificate templates by deploying certificates for different purposes.
- Create and issue custom certificate templates.

Security+ Objectives

- 5.1 Explain general cryptography concepts.
 - Key management
 - Single vs. Dual sided certificates
- 5.5 Explain core concepts of public key cryptography.
 - Public Key Infrastructure (PKI)
 - Recovery agent
 - Public key
 - Private keys
 - Certificate Authority (CA)
 - Registration
 - Key escrow
 - Certificate Revocation List (CRL)
 - Trust models

- 5.6 Implement PKI and certificate management.
 - Public Key Infrastructure (PKI)
 - Recovery agent
 - Public key
 - Private keys
 - Certificate Authority (CA)
 - Registration
 - Key escrow
 - Certificate Revocation List (CRL)

Lecture Focus Questions:

- Who authorizes subordinate CAs? Why is this important?
- What does the issuance policy on a CA control?
- How does a client verify the information in an SSL certificate to determine if it trusts the certificate?
- What is the difference between a CSP and a CPS?
- What is the role of the Registration Authority (RA)?
- What is the difference between key *archival* and key *escrow*?
- How are revoked certificates identified? Under what circumstances would a certificate be revoked?
- What security advantage do dual key pairs provide?

Time

About 55 minutes

Lab/Activity

- Manage Certificates

Number of Exam Questions

15 questions

Section 2.6: Cryptography Implementations

Summary

This section discusses implementing cryptography by combining the strengths of hashing, symmetric and asymmetric encryption. Some of the applications for cryptography include:

- Encrypting File System (EFS)
- Digital signatures
- Digital envelope
- Whole disk encryption (BitLocker)

Students will learn how to:

- Encrypt a file to secure data using EFS.
- Authorize additional users who can access files encrypted with EFS.
- Protect hard drive contents with BitLocker.
- Configure settings to control BitLocker using Group Policy.

Security+ Objectives

- 5.1. Explain general cryptography concepts.
 - Digital signatures
 - Whole disk encryption
 - Trusted Platform Module (TPM)

Lecture Focus Questions:

- What are the advantages of asymmetric over symmetric encryption? What are the disadvantages?
- How are asymmetric encryption and hashing combined to create digital signatures?
- What is the difference between digital *signatures* and digital *envelopes*?
- With EFS, how is data encrypted? How is the encryption key protected and kept from unauthorized use?
- What role does the TPM play when using BitLocker? How does using BitLocker without a TPM modify the configuration options available?
- How does the protection offered by Bitlocker differ from EFS?

Time

About 35 minutes

Number of Exam Questions

11 questions

Section 2.7: Secure Protocols

Summary

This section examines using the following secure protocols to provide security services to new or existing protocols that were designed with little or no security controls:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Secure Shell (SSH)

Hyper Text Transfer Protocol (HTTP) is an unsecured protocol commonly used for exchanging Web content. The following protocols are used to secure HTTP:

- Hyper Text Transfer Protocol Secure (HTTPS)
- Secure Hypertext Transfer Protocol (S-HTTP)

IP Security (IPSec) is used to provide secure data transmission over unprotected TCP/IP networks. IPSec includes two protocols:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Two modes of operation can be implemented with IPSec:

- Transport mode
- Tunnel mode

Concepts that are covered include

- A Security Association (SA) supports secure communications and is established through the Internet Key Exchange (IKE) protocol.
- Use NAT-Traversal (NAT-T) to eliminate communication problems that can be caused by using Network Address Translation (NAT).

Students will learn how to:

- Add SSL bindings to a Web site to support secure connections.
- Modify Web site settings to require SSL.
- Use SSL from a browser to create a secure connection.
- Enforce the use of IPSec through Connection Security Rules.

Security+ Objectives

- 5.4. Explain and implement protocols.
 - SSL/TLS
 - HTTP vs. HTTPS vs. SHTTP
 - IPSEC
 - SSH

Lecture Focus Questions:

- How does SSL verify authentication credentials?
- What protocol is the successor to SSL 3.0?
- How can you tell that a session with a Web server is using SSL?
- What is the difference between HTTPS and S-HTTP?
- What does it mean when HTTPS is referenced as being *stateful*?
- What is the difference between IPsec *tunnel* mode and *transport* mode?

Time

About 50 minutes

Lab/Activity

- Allow SSL Connections

Number of Exam Questions

11 questions

Section 3.1: OSI Model Review

Summary

This section provides a review of the Open Systems Interconnection (OSI) model. It is important for students to understand the OSI model because network security devices and solutions are often described based on the OSI model. Facts about the following layers are presented:

- Application (Layer 7)
- Presentation (Layer 6)
- Session (Layer 5)
- Transport (Layer 4)
- Network (Layer 3)
- Data Link (Layer 2)
- Physical (Layer 1)

Lecture Focus Questions:

- What is the OSI model and why is it important in understanding networking?
- What are the advantages of using a theoretical model to describe networking?
- What is the name of Layer 3 in the OSI model? Layer 5?
- What security features are associated with the Presentation layer?
- What functions are performed by the Data Link layer?

Time

About 10 minutes

Section 3.2: Protocols and Ports

Summary

This section explores protocols and ports used for communication between network hosts. Major protocols include:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)
- Network Basic Input/Output System (NetBIOS)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)

Ports are logical connections that the TCP/IP protocol stack uses to determine what protocol incoming traffic should be directed to. The Internet Corporation for Assigning Names and Numbers (ICANN) specifies three categories and ranges for ports:

- Well known ports range from 0 to 1023
- Registered ports range from 1024 to 49,151
- Dynamic ports range from 49,152 to 65,535

Students will become familiar with a long list of well known TCP and UDP ports that correspond to common Internet services.

Students will learn how to:

- View and analyze captured traffic using a network analyzer.
- Perform a port scan on a system using **netstat** to determine connections and listening ports.
- Perform a port scan using **nmap** to find all the open ports on a remote system.

Security+ Objectives

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
 - Antiquated protocols

Lecture Focus Questions:

- How does a computer identify messages sent to a specific service?
- What are the major differences between TCP and UDP?
- How can ICMP messages be used to provide a valuable security tool?

- What threat does an antiquated protocol pose? What would be the best practice when dealing with an antiquated protocol?
- What is the best practice when deciding which protocol ports to allow through a network firewall?
- Why would an administrator find it important to run a port scanner on the system?

Time

About 30 minutes

Number of Exam Questions

3 questions

Section 3.3: Network Devices

Summary

In this section students will learn characteristics of the following network devices:

- Hub
- Switch
- Router

Security+ Objectives

- 2.3 Determine the appropriate use of network security tools to facilitate network security.
 - Firewalls
- 3.5 Compare and implement logical access control methods.
 - ACL

Lecture Focus Questions:

- What are the security advantages of using switches over hubs?
- What security problems could static routing pose on a large network?
- What security threat do broadcasts allow?
- What information does a router ACL use to allow or reject packets?

Time

About 10 minutes

Number of Exam Questions

2 questions

Section 3.4: Network Authentication

Summary

This section discusses using network authentication to prove user identity before allowing access to network resources. Authentication concepts covered include:

- The risk of authenticating using a clear text password
- The three-way handshake process
- Methods used for network authentication
 - LAN Manager (LANMAN or LM)
 - NT LAN Manager (NTLM)
 - Kerberos
 - Lightweight Directory Access Protocol (LDAP)

Students will learn how to:

- Edit Kerberos Policy settings using Group Policy Management.
- Provide authentication backwards compatibility for pre-Windows 2000 clients using Group Policy.

Security+ Objectives

- 3.7 Deploy various authentication models and identify the components of each.
 - LDAP
 - Kerberos
- 5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.
 - LANMAN
 - NTLM

Lecture Focus Questions:

- Using a challenge/response process, what information is exchanged over the network during logon? How does this provide security for logon credentials?
- What is the difference between authentication with LAN Manager and NT LAN Manager?
- What security vulnerabilities should an administrator be aware of when using Kerberos for authentication?
- What two entities are combined to make up the KDC?
- Why does Kerberos require clock synchronization between devices?
- Which authentication method is used with LDAP when Simple Authentication and Security Layer (SASL) is used?

Time

About 30 minutes

Number of Exam Questions

9 questions

Section 3.5: Remote Access

Summary

This section provides information about creating and configuring remote access to allow a host to remotely connect and access resources. Implementing remote access consists of the following processes:

- Connection to a remote access server through one of the following types:
 - Dialup connection
 - Virtual private network (VPN)
- Authentication using one of the following protocols:
 - Password Authentication Protocol (PAP)
 - Challenge Handshake Authentication protocol (CHAP)
 - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
 - Extensible Authentication Protocol (EAP)
- Authorization
- Accounting

VPN concepts covered include:

- VPNs use a tunneling protocol to encrypt IP traffic.
- Common VPN tunneling protocols include:
 - Point-to-Point Tunneling Protocol (PPTP)
 - Layer 2 Forwarding (L2F)
 - Layer Two Tunneling Protocol (L2TP)
 - Internet Protocol Security (IPSec)
 - Secure Sockets Layer (SSL)

Students will learn how to:

- Configure a remote access server to accept remote access connections.
- Control remote access authorization using network policies.
- Configure ports on a VPN server to allow VPN connections.
- Configure a VPN client connection.

Security+ Objectives

- 3.7 Deploy various authentication models and identify the components of each.
 - RAS
 - Remote access policies
 - Remote authentication
 - VPN
 - CHAP
 - PAP

- Mutual

Lecture Focus Questions:

- Why should PPP instead of SLIP be used with remote access authentication?
- How does EAP differ from CHAP or MS-CHAP?
- What is the difference between *authentication* and *authorization*?
- How does tunneling protect packets in transit through an unsecured network?
- Which IPSec protocol provides data encryption?
- How does tunnel mode differ from transport mode with IPSec?
- Why is using SSL for a VPN connection often a better solution than using other VPN protocols?

Time

About 60 minutes

Lab/Activity

- Configure a Remote Access Server
- Configure a Remote Access Connection
- Configure a VPN Connection

Number of Exam Questions

15 questions

Section 3.6: RADIUS and TACACS+

Summary

In this section students will learn the basics of using RADIUS and TACACS+ to centralize the administration of remote access policies by using an AAA (authentication, authorization, and accounting server).

Common AAA server solutions discussed include:

- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System Plus (TACACS+)

Students will learn how to:

- Configure a RADIUS server to perform authentication and authorization for RADIUS clients.
- Configure a remote access server to forward authentication, authorization, and accounting requests to a RADIUS server.

Security+ Objectives

- 3.7 Deploy various authentication models and identify the components of each.
 - RADIUS
 - TACACS

Lecture Focus Questions:

- What is an advantage of using RADIUS or TACACS+ in your remote access solution?
- How does RADIUS differ from TACACS+?
- When comparing RADIUS and TACACS+, which is more secure? Which performs better?
- What is the difference between a RADIUS server and a RADIUS client?
- What are common vulnerabilities of RADIUS and TACACS+?

Time

About 30 minutes

Lab/Activity

- Configure a RADIUS Server
- Configure a RADIUS Client

Number of Exam Questions

9 questions

Section 3.7: Network Address Translation

Summary

This section covers using Network Address Translation to connect a private network to the Internet without obtaining registered addresses for every host. Hosts on the private network share the registered IP addresses.

Concepts covered include:

- IP address ranges used to connect a private network to the Internet through NAT
 - 10.0.0.0 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- The role of a router running NAT
- NAT translates one address to another
- The role of Port address translation (PAT)
- Dynamic NAT
- Static NAT
- Possible issue when using both IPSec and NAT
- Combining NAT with packet filter or firewalls

Students will learn how to:

- Add the NAT protocol and enable interfaces for NAT.
- Configure static NAT by mapping private IP addresses to public IP addresses and ports.

Security+ Objectives

- 2.2 Distinguish between network design elements and components.
 - NAT

Lecture Focus Questions:

- What are two advantages to using NAT?
- What is the difference between static NAT and dynamic NAT?
- How does NAT provide a measure of security to network devices?
- What address ranges should you use on private networks connected to the Internet using NAT?
- What might cause problems when using IPSec with NAT?

Time

About 20 minutes

Lab/Activity

- Configure Dynamic NAT

Number of Exam Questions

4 questions

Section 4.1: Reconnaissance

Summary

This section discusses reconnaissance, the process of gathering information about an organization prior to an attack. Students will become familiar with two types of reconnaissance:

- Organizational
- Technical
 - Horizontal scan
 - Vertical scan

Students will learn how to:

- Identify who has registered a domain name using **Whois.net** and **SamSpade.org**.
- Gather organizational information using Google, job boards, or other common Internet tools.

Security+ Objectives

- 1.3 Identify the following address formats
 - IPv6

Lecture Focus Questions:

- What types of resources make organizational reconnaissance so readily available?
- What types of information can be gathered using organizational reconnaissance?
- What is the difference between a *horizontal* scan and a *vertical* scan when performing technical reconnaissance?
- How is *footprinting* used to determine the operating system of the recipient?
- When performing technical reconnaissance, what information does port scanning provide?

Time

About 15 minutes

Number of Exam Questions

1 question

Section 4.2: Denial of Service (DoS)

Summary

In this section students will learn how an attacker can use Denial of Service (DoS) attacks to impact system availability. The goal of a DoS attack is to make a service or device unavailable to respond to legitimate requests. Students will become familiar with:

- The network components that are commonly impacted by DoS attacks.
- The difference between a DoS and a Distributed DoS (DDoS) attack.
- Increasing the severity of the attack using a Distributed Reflective Denial of Service (DRDoS).
- DoS attacks that use the ICMP protocol
 - Ping flood
 - Ping-of-death
 - Smurf
- DoS attacks that exploit the TCP protocol
 - SYN flood
 - LAND
- DoS attacks that exploit the UDP protocol
 - Fraggle
 - Teardrop
- Countermeasure for DoS and DDOS attacks

Students will learn how to:

- Implement a packet analyzer tool to capture network traffic.
- Analyze captured traffic to determine the extent to which the bandwidth is being compromised.

Security+ Objectives

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
 - DOS
 - DDOS
- 2.5 Explain the vulnerabilities and mitigations associated with network devices.
 - DOS

Lecture Focus Questions:

- What is the difference between a DoS and a DDoS attack?
- Why is it difficult to identify a DDoS attacker?
- How does a Distributed Reflective Denial of Service (DRDoS) increase the severity of a DoS attack?

- What is the difference between a *ping flood* and a *ping-of-death*?
- What is the main reason that a victim can't respond to LAND attack packets?
- How is a Fraggle attack similar to a Smurf attack? How are they different?
- What countermeasures will help to mitigate DoS and DDoS attacks?

Time

About 20 minutes

Number of Exam Questions

3 questions

Section 4.3: Session and Spoofing Attacks

Summary

This section provides the basics for understanding and preventing session and spoofing attacks. In a session based attack, the attacker takes over the TCP/IP session or captures information that can be used at a later date. Session based attacks include:

- Man-in-the-middle
- TCP/IP (session) hijacking
- HTTP (session) hijacking
- Replay attack
- Null session

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks include:

- IP spoofing
- MAC spoofing
- ARP spoofing

Countermeasures to prevent spoofing include:

- Firewall and router filters
- Certificates
- Reverse DNS lookup
- Encrypted communication protocols
- Ingress and egress filters

Students will learn how to:

- Scan for MAC addresses and the corresponding IP addresses using a MAC address scanning tool.
- Perform an ARP poisoning attack on a host to identify vulnerabilities.
- Use a sniffer to detect an unusually high traffic pattern of ARP replies.

Security+ Objectives

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
 - TCP/IP hijacking
 - Null sessions
 - Spoofing
 - Man-in-the-middle
 - Replay
 - ARP poisoning

Lecture Focus Questions:

- Why is a man-in-the-middle attack so dangerous for the victim?
- What countermeasures can be used to control TCP/IP hijacking?
- What methods should you employ to prevent a replay attack?
- What types of tools does an attacker use to capture authentication information to perform a replay attack?
- What countermeasures can help prevent spoofing?

Time

About 25 minutes

Number of Exam Questions

11 questions

Section 4.4: DNS Attacks

Summary

This section discusses facts about how a DNS attack redirects traffic to fake Web sites for malicious purposes. Concepts covered include:

- The role of Standard DNS
- The role of Secondary DNS servers
- The process of zone transfer
- Methods to attack a DNS server include:
 - Reconnaissance
 - DNS poisoning
 - Domain name kiting
- The role of the HOSTS file to improve security and reduce bandwidth usage

Students will learn how to:

- Perform queries on name server records using **nslookup**.
- Restrict zone transfers to specific servers.
- Map malicious Web sites to a loopback address (127.0.0.1) in the HOSTS file.

Security+ Objectives

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
 - Domain Name Kiting
 - DNS poisoning

Lecture Focus Questions:

- What is the difference between a primary and a secondary DNS server?
- What methods are employed by an attacker to discover DNS records including computer names and IP addresses?
- How does domain name kiting work?
- In what ways can the HOSTS file be used to improve security?

Time

About 20 minutes

Number of Exam Questions

3 questions

Section 4.5: Switch Attacks

Summary

This section explores attacks that are perpetrated against switches. These attacks include:

- MAC flooding
- ARP spoofing/poisoning
- MAC spoofing
- Dynamic Trunking Protocol (DTP)

Security+ Objectives

- 2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.
 - Spoofing
 - ARP poisoning

Lecture Focus Questions:

- What types of attacks are commonly perpetrated against switches?
- How does MAC flooding make a switch function as a hub? What is this state called?
- How are switches indirectly involved in ARP poisoning?
- How does the attacker hide his identity when performing MAC spoofing?
- What is a more secure alternative to using the Dynamic Trunking Protocol (DTP)?

Time

About 10 minutes

Number of Exam Questions

2 questions

Section 5.1: Firewalls

Summary

This section examines using firewalls to inspect, identify, and block specified traffic.

Concepts covered include:

- The function of a network-based firewall
- The function of a host-based firewall
- Filtering Rules
- Firewall protections
- Firewall types
 - Packet filtering
 - Stateful
 - Application
- Facts about managing firewalls

Students will learn how to:

- Enable Windows Firewall and configure exceptions to control communications through the firewall.
- Configure inbound and outbound rules to control traffic.
- Create a custom rule to allow ICMP Echo Requests through a firewall.
- Import and export firewall rules to other machines to create firewalls with uniform settings.

Security+ Objectives

- 1.5 Implement security applications.
 - Personal software firewalls
- 2.3 Determine the appropriate use of network security tools to facilitate network security.
 - Firewalls
 - Proxy servers
- 2.4 Apply the appropriate network tools to facilitate network security.
 - Firewalls
 - Proxy servers

Lecture Focus Questions:

- What is the difference between a network-based firewall and a host-based firewall?
- When would you choose to implement a host-based firewall?
- What types of characteristics of traffic can be specified for a filtering rule for a packet filtering firewall?

- How does a packet filtering firewall differ from a circuit-level gateway?
- Why is a packet filtering firewall a *stateless* device?
- What types of filter criteria can an application layer firewall use for filtering?

Time

About 30 minutes

Lab/Activity

- Configure Windows Firewall

Number of Exam Questions

14 questions

Section 5.2: Security Zones

Summary

This section provides information about security zones. Common zones include:

- Intranet
- Internet
- Extranet

Concepts covered include:

- The role of a demilitarized zone (DMZ)
- The role of the screening router
- Different types of DMZ configurations
 - Dual-homed gateway
 - Screened gateway
- Firewall design practices
- The role of bastion hosts
- Actions to harden a bastion host

Security+ Objectives

- 2.2 Distinguish between network design elements and components.
 - DMZ
- 2.4 Apply the appropriate network tools to facilitate network security.
 - Firewalls
 - Proxy servers

Lecture Focus Questions:

- How is an *intranet* different than an *extranet*?
- How does a screening router provide security to the network?
- What is the typical configuration for a DMZ configured as *dual-homed gateway*?
- A screened subnet uses two firewalls. What are the functions of each firewall?
- What type of computers might exist inside of a demilitarized zone (DMZ)?
- What makes bastion hosts vulnerable to attack? What should you do to harden bastion hosts?

Time

About 15 minutes

Number of Exam Questions

7 questions

Section 5.3: Intrusion Detection

Summary

This section provides an overview of using an intrusion detection system (IDS) to detect attacks. Students will become familiar with:

- Elements of an IDS
 - Operator
 - Sensor
 - Engine/analyzer
 - Alert
- IDS interpretation of traffic
 - Positive
 - False positive
 - Negative
 - False negative
- Detection systems
- Response capability
 - Passive IDS
 - Active IDS
- Recognition methods
 - Signature recognition
 - Anomaly recognition
- Detection scope
 - Host-based IDS (HIDS)
 - Network-based IDS (NIDS)
- Methods of protecting a network
 - Honeypot
 - Honeynet
 - Tarpit
- Enticement vs. entrapment
- Security facts about intruder detection

Students will learn how to:

- Monitor network activity using intrusion detection software to capture and view network traffic.

Security+ Objectives

- 1.5 Implement security applications.
 - HIDS
 - Antivirus

- 2.3 Determine the appropriate use of network security tools to facilitate network security.
 - NIDS
 - NIPS
 - Honeypot
- 2.4 Apply the appropriate network tools to facilitate network security.
 - NIDS
- 4.5 Compare and contrast various types of monitoring methodologies.
 - Behavior-based
 - Signature-based
 - Anomaly-based

Lecture Focus Questions:

- What does it mean when traffic is labeled as a *false negative*?
- What data sources does an IDS system use to gather information that it will analyze to find attacks?
- How does an IPS differ from an IDS?
- What type of recognition method is used by most virus scanning software?
- What should you regularly do when using a signature-based IDS?
- What is the advantage to using a network-based IDS instead of a host-based IDS?
- What are the security reasons for using a honeypot or honeynet?
- After an attack, what types of data should you backup to retain information about the attack for future investigations?

Time

About 30 minutes

Number of Exam Questions

15 questions

Section 5.4: Switch Security

Summary

In this section students will learn how to increase network security using the following switch features:

- Virtual LAN (VLAN)
- MAC filtering/port security
- Port authentication (802.1x)

Concepts covered about implementing switch security include the:

- Administrative benefits of creating VLANs with switches.
- Role of routers.
- Role of VLAN when used with Voice over IP (VoIP).
- Role of MAC filtering and port authentication.

Students will learn how to:

- Create VLANs and assign switch ports to VLANs.
- Configure a trunk port on a switch.

Security+ Objectives

- 2.2 Distinguish between network design elements and components.
 - VLAN
 - Network interconnections

Lecture Focus Questions:

- How does a switch identify devices that are in different VLANs?
- What is the function of a trunk port?
- When trunking is used, how is the receiving switch able to identify which VLAN the frame belongs to?
- What is required for devices to communicate between VLANs?
- What are the administrative advantages to creating VLANs with switches?
- How is port security different from port filtering?
- What does port filtering use to control access?
- When using 802.1x authentication, a device connected to an unauthenticated port can communicate with which other devices on the LAN?
- What element does port security use to identify allowed or denied devices?

Time

About 30 minutes

Lab/Activity

- Exploring VLANs

Number of Exam Questions

7 questions

Section 5.5: Security Solutions

Summary

This section discusses network security solutions that can be configured to increase network security. Solutions discussed include:

- Proxy server
- Internet content filter
- Network Access Control (NAC)

Students will learn how to:

- Enable Parental Controls for a user and configure control settings for allowed Web sites, time limits, games, and specific programs.
- Enable *activity reporting* to view Web browsing activities of a user in which you have configured parental controls.
- Configure Network Access Protection to restrict network access to only clients that meet specified health criteria.

Security+ Objectives

- 2.2 Distinguish between network design elements and components.
 - NAC
- 2.3 Determine the appropriate use of network security tools to facilitate network security.
 - Proxy servers
 - Internet content filters
- 2.4 Apply the appropriate network tools to facilitate network security.
 - Proxy servers
 - Internet content filters

Lecture Focus Questions:

- Which security device might you choose to restrict access by user account?
- What types of restrictions can be configured for proxy servers?
- What types of entities commonly use Internet content filtering software?
- What functions does keyword filtering provide?
- How can Network Access Controls (NAC) help to improve the security of a network?
- How does a remediation server help a client to gain access to a network to which it has been denied access?

Time

About 45 minutes

Lab/Activity

- Configure Parental Controls

Number of Exam Questions

5 questions

Section 5.6: Transmission Media

Summary

This section examines media (cable) used for transmission of data on a network. Vulnerabilities that could affect the networking cable include:

- Availability
- Interference
- Tapping
 - Physical tap
 - Network tap
- Data emanation

Students will become familiar with the security concerns for the following networking cable types:

- Unshielded twisted pair (UTP)
- Shielded twisted pair (STP)
- Coaxial
- Fiber Optic

Additional terms that are presented in this section include:

- Electromagnetic interference (EMI)
- Phone tap or vampire tap
- Data emanation
- Thicknet

Security+ Objectives

- 2.6 Explain the vulnerabilities and mitigations associated with various transmission media.
 - Vampire taps
- 6.5 Explain the importance of environmental controls.
 - Shielding

Lecture Focus Questions:

- What kinds of security problems can interference cause?
- What is the difference between a *physical* tap and a *network* tap?
- How does tapping affect the security of a network?
- Why are fiber optic cables immune to data emanation?
- How does crosstalk occur?
- Which type of cable is most susceptible to security concerns?

Time

About 15 minutes

Number of Exam Questions

6 questions

Section 5.7: Wireless

Summary

In this section students will learn security practices for wireless communication.

Security concerns include:

- SSID broadcast
- Rogue access point
- MAC address filtering
- Data emanation
- Interference

Wireless authentication methods include:

- Open
- Shared key
- 802.1x

Wireless security standards include:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2) or 802.11i

Students will learn how to:

- Configure a wireless access point by disabling the SSID broadcast and enabling security.
- Configure a wireless network profile to automatically connect even if the SSID broadcast is turned off.
- Scan a network to detect wireless access points and determine if the access points are secure.

Security+ Objectives

- 2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.
 - Data emanation
 - War driving
 - SSID broadcast
 - Rogue access points
- 3.7 Deploy various authentication models and identify the components of each.
 - RADIUS

- 802.1x
- 5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.
 - AES
 - Transmission encryption (WEP TKIP, etc)

Lecture Focus Questions:

- How does turning off the SSID broadcast help to secure the wireless network?
- What are some methods that an attacker can use to capture information using a rogue access point?
- How can an attacker bypass address MAC filtering to gain access to a wireless network?
- What methods can you use to secure a wireless network from data emanation?
- What does open authentication use for authenticating a device? Why is this not a very secure solution?
- What two additional components are required to implement 802.1x authentication?
- What does WEP use for the encryption key? Why does this present a security problem?
- Why should you *not* use shared key authentication with WEP?
- What is the difference between WPA Personal and WPA Enterprise?
- You have an access point that currently supports only WEP. What would you typically need to do to support WPA2?
- What is the encryption method used with WPA? WPA2?

Time

About 55 minutes

Lab/Activity

- Configure a Wireless Profile

Number of Exam Questions

13 questions

Section 5.8: Mobile Devices

Summary

This section discusses security considerations for the following mobile devices:

- Infrared (IR)
- Bluetooth
- PDA/Smart phone
- Wireless Application Protocol (WAP)

Security+ Objectives

- 2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.
 - Blue jacking
 - Bluesnarfing

Lecture Focus Questions:

- What types of personal area network (PAN) devices are commonly used with Bluetooth technology?
- What is the difference between *bluejacking* and *bluesnarfing*?
- Why is a successful bluebugging attack more dangerous for the victim than a bluesnarfing attack?
- What is the best method to protect against attacks directed towards Bluetooth capabilities?
- How does the *Gap in the Wap* expose data in cleartext?

Time

About 7 minutes

Number of Exam Questions

3 questions

Section 5.9: Telephony

Summary

This section provides details of managing telephony solutions. Technologies discussed include:

- Private Branch Exchange (PBX)
- Voice over IP (VoIP)

Common phone exploitation attacks discussed are:

- Cramming
- Slamming
- War dialing

Cell phone exploitation attacks include:

- Cloning
- Sniffing
- Tumbling

Security+ Objectives

- 1.2 Explain the security risks pertaining to system hardware and peripherals.
 - Cell phones
- 2.2 Distinguish between network design elements and components.
 - Telephony

Lecture Focus Questions:

- What methods can be used to send digital data through Plain Old Telephone System (POTS) lines?
- What are common threats to a PBX system? How do you secure the PBX?
- What types of security issues must be considered when using VoIP?
- What is the difference between *cramming* and *slamming*?
- What countermeasures protect against war dialing?
- What types of cell phone attacks are becoming common?

Time

About 15 minutes

Number of Exam Questions

5 questions

Section 6.1: Malware

Summary

This section explores types of malware that can take over or damage a computer, without the user's knowledge or approval. Malware that are discussed include:

- Virus
 - Stealth
 - Multipartite
 - Macro
 - Polymorphic
 - Retro
 - Armored
 - Companion
 - Phage
- Worm
- Trojan horse
- Zombie
- Botnet
- Rootkit
- Logic bomb
- Spyware
- Adware
- Crimeware

Best practices for protecting against malware and recovering from a malware attack are presented.

Students will learn how to:

- Scan a system with anti-malware software to identify potential threats.
- Configure Windows Defender protections to secure a network from malware.
- Quarantine and remove malware.
- Analyze startup programs to detect possible malware.

Security+ Objectives

- 1.1 Differentiate among various systems security threats.
 - Virus
 - Worm
 - Trojan
 - Spyware
 - Spam
 - Adware

- Rootkits
 - Botnets
 - Logic bomb
- 1.5 Implement security applications.
 - Antivirus
 - Anti-spam
 - Popup blockers

Lecture Focus Questions:

- What is the difference between a *virus* and a *worm*?
- Which types of malware can be spread through e-mail?
- How are Trojans and botnets related?
- What does it mean for software to be quarantined?
- Why is it a good practice to show file extensions?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?

Time

About 45 minutes

Lab/Activity

- Configure Windows Defender

Number of Exam Questions

14 questions

Section 6.2: Device Vulnerabilities

Summary

This section discusses the following network device vulnerabilities:

- Default accounts and passwords
- Weak passwords
- Privilege escalation
- Backdoor

Students will learn how to:

- Search a database for default passwords for network devices.

Security+ Objectives

- 1.1 Differentiate among various systems security threats.
 - Privilege escalation
- 2.5 Explain the vulnerabilities and mitigations associated with network devices.
 - Privilege escalation
 - Weak passwords
 - Back doors
 - Default accounts

Lecture Focus Questions:

- For security's sake, what is the first thing you should do when new hardware and software is turned on for the first time?
- How are attackers able to recover passwords?
- What are the characteristics of a complex password?
- How is privilege escalation different than hacking into a system to gain access to resources?
- What measures should be completed to protect against backdoors?

Time

About 10 minutes

Number of Exam Questions

6 questions

Section 6.3: Hardening

Summary

This section provides recommendations for hardening systems to improve security.

Topics covered include:

- Controlling logon
- Limiting administrative privileges
- Installing security software
- Reducing the attack surface
- Identifying configuration baselines
- Using security templates
- Applying updates
 - Hotfix
 - Patch
 - Service pack
- Managing updates

Students will learn how to:

- Harden a system by changing default account passwords and verifying user and group assignments.
- Lock down system security by only installing required software and roles and disabling unnecessary services.
- Use security templates to apply or audit security settings on your system.
- Use Group Policy to deploy multiple settings to multiple machines in an Active Directory domain.
- Use Windows Updates and WSUS to automate patch management of your Windows system.

Security+ Objectives

- 1.3 Implement OS hardening practices and procedures to achieve workstation and server security.
 - Hotfixes
 - Service packs
 - Patches
 - Patch management
 - Group policies
 - Security templates
 - Configuration baselines

Lecture Focus Questions:

- What is *hardening*? How does it benefit the security of an organization?
- How do you reduce the attack surface of a device?
- What is a *security baseline*?
- What is the difference between a *hotfix* and a *patch*? Why would you use one over the other?

Time

About 30 minutes

Lab/Activity

- Configure Automatic Updates

Number of Exam Questions

11 questions

Section 6.4: Removable Media

Summary

This section explores considerations for securing removable media. Topics covered include:

- Storing backup media
- Protecting magnetic media from electromagnetic fields
- Disabling removable devices
- Utilizing the Group Policy to control removable media
- Scanning removable media with antivirus software before using it on the system
- Deleting and formatting still leave data remanence
- Disposing of media
 - Formatting
 - Sanitization
 - Destruction

Students will learn how to:

- Use Group Policy to prevent installation of all removable devices.
- Use Group Policy to block removable devices that match certain device IDs.
- Use sanitization software to permanently delete data from a hard disk and prevent data recovery of data remanence.

Security+ Objectives

- 1.2 Explain the security risks pertaining to system hardware and peripherals.
 - USB devices
 - Cell phones
 - Removable storage

Lecture Focus Questions:

- Removable devices pose threats to which security goal?
- Why is just formatting a hard drive with sensitive information not considered a secure method of disposing of the data?
- What method would you use to clean a hard disk which contains sensitive information when the disk will be reused in another department of the company?
- What methods should be employed if the data is extremely sensitive and the media should be destroyed?

Time

About 25 minutes

Lab/Activity

- Control Device Installation

Number of Exam Questions

6 questions

Section 6.5 BIOS Security

Summary

This section examines configuring Basic Input Output System (BIOS) settings to enhance system security.

Note: Ensure that the students are aware that the factory default setting for the BIOS can be restored and that will allow access.

Students will learn how to:

- Secure the BIOS by setting a supervisor BIOS password.
- Disable removable devices in the BIOS.
- Configure additional settings in the BIOS to increase system security.

Security+ Objectives

- 1.2 Explain the security risks pertaining to system hardware and peripherals.
 - BIOS

Lecture Focus Questions:

- Why is setting a password on the BIOS a good practice?
- How does an administrator or supervisor BIOS password differ from a user password?
- How can attackers bypass a BIOS password?
- How does setting the boot sequence to boot from hard disk first increase security?
- Why would you enable Trusted Platform Module (TPM) settings in the BIOS?
How could this increase security?

Time

About 15 minutes

Lab/Activity

- Configure BIOS Security

Number of Exam Questions

4 questions

Section 6.6: File and Print Security

Summary

This section provides facts about managing security for the file and print resources. Topics covered include.

- Vulnerable to Denial of Service (DoS) and access attacks
- Protecting the server
- Shared server
- Network Attached Storage (NAS)
- Storage Area Network (SAN)
- Securing data during transfer
- TCP/IP protocols used for securing file transfer
 - File Transfer Protocol (FTP)
 - Trivial File Transfer Protocol (TFTP)
 - Secure Copy Protocol (SCP)
 - Secure Shell File Transfer Protocol (SFTP)
 - Secure FTP
 - FTP Secure (FTPS)
- Using File Server Resource Manager to control files saved on a file server

Students will learn how to:

- Secure FTP by disabling anonymous access.
- Secure FTP 7 by configuring authentication, authorization, SSL, and user isolation settings.
- Manage file permissions by configuring file share permissions and NTFS permissions.
- Configure printer permissions to control who can manage the printer and documents.

Security+ Objectives

- 1.2 Explain the security risks pertaining to system hardware and peripherals.
 - Network attached storage
- 3.4 Apply appropriate security controls to file and print resources.

Lecture Focus Questions:

- How would you create hidden shares in a Windows file system?
- Why is a Storage Area Network (SAN) typically more secure than Network Attached Storage (NAS)?
- What methods can you use to secure the transfer of files between a client and a server?

- What are the vulnerabilities of FTP?
- How do share permissions differ from NTFS permissions?
- How do share and NTFS permissions combine to restrict access?
- What printer tasks can a user perform who is a member of the Print Operators group?

Time

About 50 minutes

Lab/Activity

- Configure File System Permissions
- Configure Printer Permissions

Number of Exam Questions

16 questions

Section 7.1: Web Applications

Summary

This section discusses using the following Web applications to make use of Web-enabled systems:

- ActiveX
- JavaScript
- Java applets
- Common Gateway Interface (CGI)
- Cookies

Configure the following Internet Explorer security settings to enhance privacy and security for browsing the Web:

- Zones
 - Local Intranet
 - Trusted sites
 - Restricted sites
 - Internet
- Add-ons
- Privacy
- Cache

Indications of an unsecured connection or an attack include:

- The loading of a Web document with a URL containing a new or different domain name than the site you intended to visit.
- A menu bar that includes new commands or is missing common commands.
- The status line of the browser displaying an unlocked symbol when SSL should be in use.

Students will learn how to:

- Customize security levels and security settings for security zones in Internet Explorer.
- Download and manage add-ons in Internet Explorer.
- Protect privacy by configuring cookie handling.
- Clear the browser cache.

Security+ Objectives

- 1.4 Carry out the appropriate procedures to establish application security.
 - ActiveX

- Java
- Scripting
- Browser
- Cookies

Lecture Focus Questions:

- What is the function of ActiveX controls?
- How does Authenticode validate the origin of ActiveX controls?
- Java runs applets in a security context known as a sandbox. What are the aspects of a sandbox that make it desirable?
- What is the recommendation to improve security if your company is using Common Gateway Interface (CGI) to capture data from forms?
- What types of information do cookies store? Why could this be a security concern?
- What steps should you take to secure the browser from add-ons that are not appropriate for your environment?
- For security's sake what should you do whenever you use a public computer to access the Internet and retrieve personal data?
- What elements might indicate an unsecured connection or an attack?

Time

About 45 minutes

Lab/Activity

- Customize IE Security Zones
- Configure Cookie Handling
- Clear the Browser Cache

Number of Exam Questions

11 questions

Section 7.2: Web Attacks

Summary

This section presents information about common Web attacks.

- Drive-by-download
- Buffer overflow
- Cross-site scripting (XSS)
- SQL injection
- DLL injection

Also discussed are mitigations practices to protect Internet-based activities from Web application attacks.

Students will learn how to:

- Configure pop-up blockers to block or allow pop-ups.
- Implement phishing protection within the browser.
- Improve security by using a Firefox add-on, NoScript, to protect against XSS and drive-by-downloads.
- Configure Internet Explorer Enhanced Security Configuration security settings to manage the security levels of security zones.

Security+ Objectives

- 1.4 Carry out the appropriate procedures to establish application security.
 - Buffer overflows
 - Input validation
 - Cross-site scripting (XSS)
- 1.5 Implement security applications.
 - Pop-up blockers

Lecture Focus Questions:

- What are two ways that drive-by download attacks occur?
- What countermeasures can be used to eliminate buffer overflow attacks?
- How can cross-site scripting (XSS) be used to breach the security of a Web user?
- What is the best method to prevent SQL injection attacks?
- What mitigation practices will help to protect Internet-based activities from Web application attacks?

Time

About 25 minutes

Lab/Activity

- Configure IE Popup Blocker and Phishing Filter

Number of Exam Questions

7 questions

Section 7.3: E-mail

Summary

This section examines securing e-mail from the following e-mail attacks:

- Virus
- Spam
- Open SMTP relay
- Phishing

Students will learn how to:

- Filter junk mail by selecting the level of junk e-mail protection you want.
- Control spam on the client by configuring safe sender, blocked senders, white lists, and black lists.
- Configure e-mail filtering to block e-mails from specified countries and languages.
- Configure relay restrictions to specify who can relay through the SMTP server.

Security+ Objectives

- 1.4 Carry out the appropriate procedures to establish application security.
 - SMTP open relays
- 1.5 Implement security applications.
 - Anti-spam
- 6.6 Explain the concept of and how to reduce the risks of social engineering.
 - Phishing

Lecture Focus Questions:

- What are the advantages of scanning for e-mail viruses at the server instead of at the client?
- How can spam cause denial of service?
- What is a best practice when configuring an SMTP relay to prevent spammers from using your mail server to send mail?
- How can you protect yourself against phishing attacks?
- What services do S/MIME and PGP provide for e-mail?
- How does S/MIME differ from PGP?

Time

About 45 minutes

Lab/Activity

- Configure E-mail Filters

Number of Exam Questions

14 questions

Section 7.4: Network Applications

Summary

This section provides an overview of security concerns for the following networking software:

- Peer-to-peer (P2P)
- Instant messaging

Students will learn how to:

- Set up content filters for downloading or uploading copyrighted materials.
- Use P2P file sharing programs to search for and share free files.
- Block ports used by P2P software.
- Secure instant messaging by blocking invitations from unknown persons.

Security+ Objectives

- 1.4 Carry out the appropriate procedures to establish application security.
 - Instant messaging
 - P2P

Lecture Focus Questions:

- What kinds of security problems might you have with P2P software?
- What types of malware are commonly spread through instant messaging (IM)?
- What security concerns should you be aware of with instant messaging (IM) software?
- What security measures should you incorporate to control the use of networking software?

Time

About 15 minutes

Number of Exam Questions

3 questions

Section 7.5: Virtualization

This section discusses using virtualization to allow a single physical machine to run multiple virtual machines. Advantages of virtualization are:

- Networked
- Server consolidation
- Isolation
- Applications virtualization

Disadvantages of virtualization include:

- An attack on the host machine could compromise all guest machines operating on that host.
- A bottleneck or failure of any hardware component that is shared between multiple guests, such as a failure in a disk subsystem, could affect multiple virtual machines.
- While administration is centralized, virtualization is a newer technology and requires new skills, and managing virtual servers could add complexity.

Students will learn how to:

- Create and configure a new virtual machine.
- Configure the virtual machine by allocating resources for memory and a virtual hard disk.
- Create a virtual network and configure it as an external, internal or private virtual network.

Security+ Objectives

- 1.6 Explain the purpose and application of virtualization technology.

Lecture Focus Questions:

- What is the relationship between the host and the guest operating systems?
- How can virtualization be used to increase the security on a system?
- What are the advantages of virtualization? Disadvantages?

Time

About 15 minutes

Number of Exam Questions

5 questions

Section 8.1: Security Policies

Summary

This section examines implementing security policies to document the security concerns of an organization. Types of documents used when creating security policies are:

- Regulation
- Procedure
- Baseline
- Guideline

Security policy documents include the following:

- Acceptable use policy
- Privacy policy
- Change and configuration management policy
- Human resource policies
- User education and awareness training
- Resource allocation policy
- User management policy
- Password policy
- Code escrow agreement
- Service Level Agreement (SLA)

Common classification levels include:

- Public with full distribution
- Public with limited distribution
- Private internal
- Private restricted

Government and military classifications are:

- Unclassified
- Sensitive, but unclassified
- Confidential
- Secret
- Top secret

Strategies for destroying information before it is disposed of include:

- Shredding
- Burning

- Degaussing magnetic materials
- Disk wiping or formatting
- Destruction of media such as crushing, incineration, and acid dipping

Security+ Objectives

- 6.4 Identify and explain applicable legislation and organizational policies.
 - Secure disposal of computers
 - Acceptable use policies
 - Password complexity
 - Change management
 - Classification of information
 - Mandatory vacations
 - Personally Identifiable Information (PII)
 - Due care
 - Due diligence
 - Due process
 - SLA
 - Security-related HR policy
 - User education and awareness training

Lecture Focus Questions:

- What is the difference between a *regulation* and a *guideline*?
- What are the main reasons for implementing security policies within an organization?
- How is *due diligence* different than *due process*?
- How can a *code escrow* agreement provide security for an organization?
- When a new security plan is distributed, why is it important to destroy all copies of the old version?
- What are the characteristics of a strong password policy?
- How is the government's *secret* classification different than the *top secret* classification?

Time

About 40 minutes

Number of Exam Questions

15 questions

Section 8.2: Disaster Planning

Summary

In this section students will learn facts about disaster planning. The three major objectives of disaster planning are presented:

- Protect the safety of employees. Personal safety is the top priority in responding to an incident.
- Identify and implement corrective actions to ensure the survival of the organization.
- Return all processes to normal operations.

A disaster plan should include the following:

- Business Continuity Plan (BCP)
- Business Impact Analysis (BIA)
- Disaster Recovery Plan (DRP)

Security+ Objectives

- 6.2 Implement disaster recovery procedures.
 - Planning
 - Disaster recovery exercises

Lecture Focus Questions:

- When is the best time to start planning for disaster recovery?
- How is the Disaster Recovery Plan (DRP) related to the Business Continuity Plan (BCP)?
- What is the top priority when planning for a disaster?
- How does a Business Impact Analysis (BIA) help to improve the security of an organization?
- In addition to planning for how to keep operations going in the event of an incident, what else should a disaster recovery plan include?

Time

About 5 minutes

Section 8.3: Redundancy

Summary

This section examines using redundancy to provide fault tolerance by providing multiple components to perform the same function. This may include redundant:

- Network paths
- System components
- Spare parts
- Power sources (such as UPS and backup generators)
- Servers
- Internet Service Providers (ISP)

Types of redundant physical sites include:

- Hot site
- Warm site
- Cold site

Important aspects of redundant facilities are:

- Fully document procedures for moving operations
- Selecting the location
- Acquisition of the facility
- Maintain up-to-date systems at the backup facility
- Contracts for redundant sites
- Moving operation to a backup facility
- Returning services from a backup facility

Redundant Array of Independent Disks (RAID) discussed include:

- RAID 0 (striping)
- RAID 5 (striping with distributed parity)
- RAID 1 (mirroring)
- RAID 0+1
- RAID 1+0

Students will learn how to:

- Configure a striped volume to increase performance.
- Configure a mirrored or a RAID 5 volume for data redundancy.

Security+ Objectives

- 6.1 Explain redundancy planning and its components.
 - Hot site
 - Cold site
 - Warm site
 - Single point of failure
 - RAID
 - Spare parts
 - Redundant servers
 - Redundant ISP
 - Redundant connections

Lecture Focus Questions:

- What is the usual activation goal time for a *hot site*? How does that differ from a *warm site*?
- Why is a *hot site* so much more expensive to operate than a *warm site*?
- Why is it important that two companies with a *reciprocal agreement* should not be located too closely to each other?
- Of the three redundancy solutions, which is the most common redundant site type? Why is it the most common?
- Which functions should be returned first when returning services from the backup facility back to the primary facility?
- Why should you locate redundant sites at least 25 miles from the primary site?
- What is the main advantage of RAID 0? Disadvantage?
- What is the difference between RAID 0+1 and RAID 1+0?

Time

About 45 minutes

Lab/Activity

- Configure Fault Tolerant Volumes

Number of Exam Questions

16 questions

Section 8.4: Backup and Restore

Summary

In this section students will learn facts about backup and restore of system data. Backup types include:

- Full
- Incremental
- Differential
- Image
- Copy Daily

Backup strategies that combine backup types are:

- Full Backup
- Full + Incremental
- Full + Differential

Topics covered about managing backups include:

- Backups must be current
- Image backups
- Store backups secure location (offsite in fire and water proof cabinets)
- Electronic vaulting
- Backup media rotation systems:
 - Grandfather Father Son (GFS)
 - Tower of Hanoi
 - Round Robin
- Type of data to back up:
 - System state data
 - Application data
 - User data
- Rights required by users responsible to back up data
- Assign backup and restore privileges to different users
- Test the backup and restore strategy

Students will learn how to:

- Use **Ntbackup** to back up Windows systems.
- Schedule automatic backups for Windows Vista computers.

Security+ Objectives

- 6.2 Implement disaster recovery procedures.

- Planning
- Backup techniques and practices -- storage
- Schemes
- Restoration

Lecture Focus Questions:

- How is an *incremental* backup different than a *differential* backup?
- When is the archive bit set? Which backup types reset the archive bit?
- What is the advantage of the Full + Incremental backup strategy? What is the disadvantage?
- Why should backup tapes be stored offsite?
- What are common types of backup media rotation systems used to provide protection to adequately restore data?
- How do you back up Active Directory?
- What should you regularly do to make sure your backup strategy is working properly?

Time

About 30 minutes

Lab/Activity

- Schedule an Automatic Backup

Number of Exam Questions

13 questions

Section 8.5: Environmental Controls

Summary

This section discusses the environmental controls that are used to maintain an optimal environment for employee comfort and protection of computer systems from heat, humidity, water, and fire. Categories of controls include:

- Heating, ventilation, and air conditioning (HVAC)
- AC power
- Interference
- Water and gas

Recommendations for the location of the data center are presented to protect data from water, fire, and thieves.

Fire-suppression systems discussed include:

- Portable
- Fixed

Extinguishing agents include:

- Water
- Gas
- Dry chemicals, wet chemicals and foam

Students will become familiar with U.S. fire classes and the appropriate suppressant type:

Class	Fuel Type	Suppressant Type
Class A	Wood, paper, cloth, plastics	Water or soda acid
Class B	Petroleum, oil, solvent, alcohol	CO ₂ or FM200
Class C	Electrical equipment, circuits, wires	Halon or CO ₂
Class D	Sodium, potassium	Dry powders
Class K	Oil, solvents, electrical wires	Halon, CO ₂ , soda acid

Security+ Objectives

- 6.1 Explain redundancy planning and its components.
 - Backup generator
 - UPS
- 6.5 Explain the importance of environmental controls.
 - Fire suppression
 - HVAC

- Shielding

Lecture Focus Questions:

- What temperature range protects equipment from overheating?
- What is a good HVAC practice to help prevent electrostatic discharge?
- What is the difference between a *positive* pressure system and a *negative* pressure system? Which is the best to use for the HVAC for a company?
- What is the difference between a *sag* and a *brownout*?
- How does a deluge sprinkler function differently than a wet pipe system?
- What should you do *first* in the event of a fire?
- When using a portable fire extinguisher it is recommended that you use the PASS system to administer the fire suppressant. How does the PASS system work?
- What is the recommended range for extinguishing a small fire using a fire extinguisher?
- What are the advantages of using a gas as a fire suppressant? Disadvantages?

Time

About 25 minutes

Number of Exam Questions

11 questions

Section 8.6: Social Engineering

Summary

This section covers understanding social engineering and implementing countermeasures. Forms of social engineering include:

- Passive
- Active

Social Engineering attacks include:

- Shoulder surfing
- Eavesdropping
- Dumpster diving
- Piggybacking
- Masquerading
- Phishing
- Hoax e-mails
- Spyware/Adware

Effective countermeasures for social engineering include:

- Providing employee awareness training
- Implementing strong identity verification methods

Students will learn how to:

- Identify and ignore e-mail hoaxes to protect system resources.
- Train users to identify phishing scams by mousing over links, verifying the URL, and verifying HTTPS.

Security+ Objectives

- 6.6 Explain the concept of and how to reduce the risks of social engineering.
 - Phishing
 - Hoaxes
 - Shoulder surfing
 - Dumpster diving
 - User education and awareness training

Lecture Focus Questions:

- How is *passive* social engineering different than *active* social engineering?
- What methods do attackers use to make an interaction appear legitimate?

- How is employee awareness training the most effective countermeasure for social engineering?
- What specific countermeasures should be implemented to mitigate social engineering?

Time

About 30 minutes

Number of Exam Questions

11 questions

Section 8.7: Incident Response

Summary

This section discusses incident response (actions to deal with an incident during and after the incident).

- Identification and containment of the problem.
- Investigation of how the problem occurred and the forensics to preserve evidence that may be used in a criminal investigation.
- Removal and eradication of the cause of the incident.
- Recovery and repair of any damages.
- Document and report the incident, and take actions to implement countermeasures and processes to reduce the likelihood of a future attack.

Terms the students will become familiar with include:

- Live analysis
- Dead analysis
- Chain of custody

Students will learn how to:

- Gather and authenticate forensic information from a system using a computer forensic tool.
- Analyze and record forensic evidence.
- View and build a case using the forensic evidence that has been gathered.

Security+ Objectives

- 6.3 Differentiate between and execute appropriate incident response procedures.
 - Forensics
 - Chain of custody
 - First responders
 - Damage and loss control
 - Reporting -- disclosure of

Lecture Focus Questions:

- What actions should take place when an incident occurs?
- What types of things would a computer forensic investigator want to analyze if he selected a *live* analysis over a *dead* analysis?
- What methods can be used to save the contents of memory as part of a forensic investigation?
- How should you ensure the integrity of collected digital evidence?

- Why is *chain of custody* so important with forensic investigations?

Time

About 25 minutes

Number of Exam Questions

12 questions

Section 9.1: Risk Management

Summary

In this section students will learn countermeasures to take to manage risk. Risk management consists of the following:

- Asset identification
 - Tangible asset
 - Intangible asset
- Threat identification
- Risk assessment
 - Quantitative analysis
 - Qualitative analysis
- Risk response
 - Reduce the risk
 - Transfer the risk
 - Accept the risk
 - Reject the risk

Security+ Objectives

- 4.1 Conduct risk assessments and implement risk mitigation.

Lecture Focus Questions:

- What kinds of components are *tangible* assets?
- How can an asset have both a tangible and intangible value?
- Why is determining the value of an asset important to an organization?
- How is *quantitative* analysis different than *qualitative* analysis?
- Which components are used to measure risk quantitatively?
- What method is typically deployed in risk *transference*?
- Why is risk *rejection* not a wise risk response?

Time

About 20 minutes

Number of Exam Questions

11 questions

Section 9.2: Vulnerability Assessment

Summary

This section provides the basics of assessing the vulnerabilities of a system or network. Tools used to monitor the vulnerability of a system include:

- Vulnerability scanners
 - Nessus
 - Microsoft Baseline Security Analyzer (MBSA)
 - Retina Vulnerability Assessment Scanner
- Ping scanner
- Port scanner
- Network mapper
- Password cracker
 - John the Ripper
 - Cain and Abel
 - L0phtcrack, now called LC4
- Open Vulnerability and Assessment Language (OVAL)

Students will learn how to:

- Scan a network with a vulnerability scanner, such as Nessus or MBSA, to identify risk factors.
- Download the latest security update information before starting a vulnerability scan.
- View security scan reports and identify vulnerabilities.
- Perform a port scan using **nmap** on a single machine.
- Use a password cracker to analyze a network for password vulnerabilities.

Security+ Objectives

- 4.2 Carry out vulnerability assessments using common tools.
 - Port scanners
 - Vulnerability scanners
 - Protocol analyzers
 - OVAL
 - Password crackers
 - Network mappers

Lecture Focus Questions:

- Why should an administrator perform a vulnerability assessment on the system?
- What is the most important step to perform before running a vulnerability scan? Why?

- How does a *port scanner* identify devices with ports that are in a listening state?
- How do *network mappers* discover devices and identify open ports on those devices?
- What types of items does OVAL identify as a *definition*?

Time

About 45 minutes

Number of Exam Questions

13 questions

Section 9.3: Penetration Testing

Summary

This section explores using penetration testing to identify vulnerabilities in information systems.

Types of penetration testing include:

- Physical penetration methods by gaining access without authorization to
 - Buildings
 - Servers and workstations
 - Wiring closets
 - Power and other services
- Operations penetration methods
 - Dumpster diving
 - Over the shoulder reconnaissance
 - Social engineering
- Electronic penetration
 - System scanning
 - Port scanning
 - Network monitoring
 - Sniffing
 - Fingerprinting

The amount of knowledge that the attacker and system personnel have prior to the attack classifies the penetration test as a:

- Zero knowledge test (black box test)
- Full knowledge test (white box test)
- Partial knowledge test (grey box test)
- Single blind test
- Double blind test

Students will learn how to:

- Identify available penetration testing tools that can be used to analyze the security of a network.
- Utilize penetration testing tools to identify vulnerabilities in information systems.
- Verify the distribution of a security tool to ensure its integrity.

Security+ Objectives

- 4.3 Within the realm of vulnerability assessments, explain the proper use of penetration testing verses vulnerability scanning.

Lecture Focus Questions:

- What is the main goal of penetration testing?
- What type of tools or methods does a penetration test use? Why should you be careful in the methods you deploy?
- What should you do first before performing a penetration test?
- How does a penetration test differ from a vulnerability assessment or scan?
- What types of details do the Rules of Engagement identify?
- What types of actions might a tester perform when attempting a physical penetration?
- What security function does the Open Source Security Testing Methodology Manual (OSSTMM) provide?

Time

About 20 minutes

Number of Exam Questions

5 questions

Section 9.4: Monitoring

Summary

This section explores using monitoring tools to troubleshoot a system. The following tools are discussed:

- Performance Monitor
- Reliability Monitor
- Protocol analyzers
 - Wireshark
 - Ethereal
 - dSniff
 - Ettercap
 - Tcpdump
 - Microsoft Network Monitor

Students will learn how to:

- Monitor network performance using Reliability and Performance Monitor.
- Configure data collector sets to log activities over time.
- Capture and analyze packets to troubleshoot a network using Wireshark.

Security+ Objectives

- 4.4 Use monitoring tools on systems and networks and detect security-related anomalies.
 - Performance monitor
 - System monitor
 - Performance baseline
 - Protocol analyzers

Lecture Focus Questions:

- Why is performance monitoring important to secure a network?
- How can a performance baseline be used to help to identify a denial of service (DoS) in progress?
- What elements does Performance Monitor use to track performance?
- When using a protocol analyzer, why is it necessary to configure the NIC in *promiscuous* mode?
- When running a protocol analyzer on a switch, how does *port mirroring* work?

Time

About 30 minutes

Number of Exam Questions

10 questions

Section 9.5: Logging and Auditing

Summary

This section examines implementing logging procedures and conducting auditing to gather and evaluate information about systems. Topics covered for logging include:

- Types of logs
 - System log
 - Security log
 - Performance log
 - Firewall log
- Analyzing logs
- Enabling and disabling logs
- Archiving logs
- Role of a remote log server
- Role of Syslog
- Protecting log files from alteration

Topics covered for auditing include:

- Goal of auditing
- Information included in audited events
 - Date and time of action
 - Identity of user logged in
 - What action took place
 - Success or failure of action
- Auditor types
 - Internal
 - External
- User access and rights review
- Privilege auditing
- Usage auditing logs
- Escalation auditing

Students will learn how to:

- Use Event Viewer to troubleshoot a system by viewing details of a logged event.
- Manage logging by saving or clearing logs, configuring filtering of logs, or attaching a task to a log or event.
- Identify operating system activities, warnings, informational messages, and error message using *system logs*.
- Configure the *audit logon events* policy to audit the failure of a logon attempt.
- View and evaluate the recorded logs under Security in Event Viewer.

Security+ Objectives

- 4.6 Execute proper logging procedures and evaluate the results.
 - Security application
 - System
 - Performance
 - Access
 - Firewall
- 4.7 Conduct periodic audits of system security settings.
 - User access and rights review
 - Storage and retention policies
 - Group policies

Lecture Focus Questions:

- How does logging affect system resources?
- What factors should you take into considerations when archiving log files?
- How can you protect log files from access and modification attacks?
- What types of information are included in events recorded in logs?
- When would you choose an *external auditor* over an *internal auditor*?
- How can *escalation auditing* help to secure the system?

Time

About 30 minutes

Number of Exam Questions

15 questions

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 1.0: System Security** are grouped together and presented in practice exam *Domain 1: System Security, All Questions*. Students will typically take about 60-90 minutes to complete each of the following practice exams.

Domain 1: Systems Security, All Questions (77 questions)

Domain 2: Network Infrastructure, All Questions (105 questions)

Domain 3: Access Control, All Questions (108 questions)

Domain 4: Assessments and Audits, All Questions (62 questions)

Domain 5: Cryptography, All Questions (88 questions)

Domain 6: Organizational Security, All Questions (93 questions)

The *Certification Practice Exam* consists of 100 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 90 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification exam.