



Lesson Plans

Certified Information Systems Security Professional

Version 2.0

Table of Contents

Table of Contents	1
Course Overview	2
Section 1.1: Security Management	5
Section 1.2: Risk Analysis	6
Section 1.3: Security Planning	7
Section 2.1: Operational Security Planning	8
Section 2.2: Employee Management	9
Section 2.3: Facility Management	10
Section 2.4: Auditing and Testing	11
Section 3.1: Crime and Law.....	12
Section 3.2: Incidence Response.....	13
Section 3.3: Ethics.....	14
Section 4.1: Cryptography Concepts	15
Section 4.2: Hashing	16
Section 4.3: Symmetric Cryptography.....	17
Section 4.4: Asymmetric Cryptography	18
Section 4.5: Implementations	19
Section 5.1: Access Controls	20
Section 5.2: Physical Security.....	21
Section 5.3: Authentication.....	22
Section 5.4: Authorization	23
Section 5.5: Auditing	24
Section 5.6: Academic Models	25
Section 6.1: Trusted Computing	26
Section 6.2: Computer Architecture.....	27
Section 6.3: Software Development	28
Section 6.4: Database Management.....	29
Section 7.1: Networking Models and Standards	30
Section 7.2: Network Technology	31
Section 7.3: Network Devices.....	32
Section 7.4: Fault Tolerance	33
Section 7.5: Internetworking.....	34
Section 7.6: Transmission Security.....	35
Section 7.7: Wireless.....	36
Section 8.1: Cryptosystem Attacks	37
Section 8.2: Access Control Attacks.....	38
Section 8.3: Availability Attacks	39
Section 8.4: Trusted Computing Base Attacks	40
Section 8.5: Communication Attacks	41
Summary.....	42

Course Overview

This course prepares students for the Certified Information Systems Security Professional certification exam by the International Information Systems Security Certification Consortium, Inc. (ISC)². To qualify to take the exam, a candidate must have 4 years experience in a security-related field. This course focuses on how to protect organizations' assets by providing the highest standards of security.

Module 0 – Introduction

This module introduces the instructor, the requirements for CISSP certification, and the goals of a security program.

Module 1 – Security Management

This module teaches how to manage security by identifying security needs and creating security policies, and creating a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) to implement preventive and corrective measures. Completing a risk analysis and a Business Impact Analysis (BIA) will help to determine appropriate countermeasures.

Module 2 – Operational Security

Module 2 explains the day-to-day operational security of the security program. This includes the basics of employee management, facility management, and testing the security program to identify weaknesses in the policies.

Module 3 – Law and Ethics

Module 3 discusses legal issues regarding cyber crime. Topics include procedures for collecting information and evidence, incident response plans, and an overview of United States and International legal systems. The code of ethics that should be adhered to by a security professional is also presented.

Module 4 – Cryptography

Module 4 covers cryptography from the historical ciphers to the present day technologies, which are hybrids of symmetric cryptography, asymmetric cryptography and hashing.

Module 5 – Access Control

In Module 5 students will learn the methods to control access to objects. These include access controls, controlling physical access, authentication, and authorization. Auditing, recording user and system activities, is used by organizations to detect unauthorized activities. Students will also learn about several important academic security models that can be used for analysis of security systems and guidelines for implementation.

Module 6 – Computing Architecture

Module 6 explains the methods used to ensure computer information system remain secure from the design of the computing components, to the development of hardware and software architecture, and management of databases.

Module 7 – Networking Security

Module 7 discusses the basics of networking security technology. Subjects include network devices, fault tolerance, Wide Area Network (WAN) technologies, security for LAN-based data and also for Web-based applications, and security for wireless implementations.

Module 8 – Attacks

In Module 8 students will learn that attackers have come up with multiple ways to attack information systems. They include cryptosystem attacks, access control attacks, availability attacks, Trusted Computing Base attacks, and communication attacks. Specific types of attacks for each of these are presented and the countermeasures to protect the system.

Section 0.1: Introduction

Preparation

The video introduces the video instructor for the Certified Information Systems Security Professional certification exam and requirements for CISSP certification. It also defines the goals of a security program. Students will become familiar with organizations that have additional study materials to supplement this course.

CISSP Objectives

3. Security Management

Lecture Focus Questions:

- What are the things a security program must do in order to be effective?
- What are the respective purposes of maintaining confidentiality, availability, and integrity?
- What are the main organizations with which IS professionals need to be familiar?

Time

About 15 minutes

Section 1.1: Security Management

Preparation

In this section, students will learn security management is the overall security vision for an organization to preserve confidentiality, integrity and availability of assets. Under the direction of senior management, security professionals establish security policies for implementation.

CISSP Objectives

3. Security Management

Lecture Focus Questions:

- How do the five components of a security policy document work together to provide an overall security program for an organization?
- In what situations would you use a security guideline instead of a security procedure?
- How does a Business Continuity Plan differ from a Disaster Recovery Plan?
- Which security documents use data from the Business Impact Analysis?
- What is senior management's role in security management?
- What is the most important function of the Business Impact Analysis?
- How are baseline documents used?

Time

About 20 minutes

Section 1.2: Risk Analysis

Preparation

This section discusses how by completing a risk analysis of critical assets and types of possible threats the security professional should be able to determine appropriate countermeasures.

CISSP Objectives

3. Security Management
8. Business Continuity Planning

Lecture Focus Questions:

- What is the relationship between the control gap and residual risk?
- How does the single loss expectancy affect the annualize rate of occurrence?
- What are the five steps for performing a risk analysis?
- When should a countermeasure *not* be implemented?
- When is risk acceptance appropriate? When is risk rejection appropriate?

Time

About 20 minutes

Section 1.3: Security Planning

Preparation

This section presents information about planning operational security through the use of Disaster Recovery Planning (DRP) to identify short-term corrective actions and Business Continuity Planning (BCP) to identify long-term actions. Also discussed, is the purpose and functionality of a Business Impact Analysis (BIA).

CISSP Objectives

3. Security Management
8. Business Continuity Planning

Lecture Focus Questions:

- What is the highest priority of security planning?
- How do the primary tasks of the recovery team differ from the primary tasks of the salvage team?
- How does a parallel test of the security plan differ from a full interruption test?
- How does the Business Impact Analysis use data from risk management and risk analysis?
- Why is it important to establish maximum tolerable down time?

Time

About 45 minutes

Section 2.1: Operational Security Planning

Preparation

This section discusses how operational security is the day-to-day implementation of the security program as defined by the security policies. It defines the major components of a security policy, timelines, multiple layers of security and operational tasks. It also identifies the roles of an operational security program team.

CISSP Objectives

3. Security Management

Lecture Focus Questions:

- Why are security awareness and employee management important components of operational security?
- How does change control enhance security?
- How do the four components of operational security work together to establish defense and depth in securing an organization?
- What security principle is being implemented when the Information System Security Administrator is required to report to different management than the Network Administrator?
- How does role counterbalancing work?
- How does the role of the Data Owner differ from the role of the Data Custodian?

Time

About 30 minutes

Section 2.2: Employee Management

Preparation

This section covers the basics of managing employees to protect company assets. This includes hiring and termination procedures, employee agreements, employee monitoring, and security awareness training.

CISSP Objectives

7. Operations Security

Lecture Focus Questions:

- How can pre-employment processing improve the security of an organization?
- Why is security awareness training so important?
- What is the role of the policy handbook regarding security?
- What guidelines must be considered when deploying employee monitoring?
- Why should employees be required to sign employment agreements?

Time

About 20 minutes

Section 2.3: Facility Management

Preparation

This section discusses the points to be considered when selecting a secure facility to protect personnel and assets. In case of a disaster, redundant systems and facilities can assure availability of critical assets to speed recovery. Another important part of facility management is fire prevention, detection, and suppression.

CISSP Objectives

10. Physical Security

Lecture Focus Questions:

- What is the relationship between redundant site selection to maximum tolerable down time?
- Why are hot sites typically not implemented? Why might cold sites be of little use when recovering from a disaster?
- How is EMI different than RFI?
- What is the difference between a UPS and a redundant power source?
- Why are positive pressure HVAC system recommended over negative pressure systems?
- What common disadvantages do mutual aid agreements and service bureaus have as redundant solutions?
- What is the best type of fire suppression system to use in a data center?

Time

About 45 minutes

Section 2.4: Auditing and Testing

Preparation

This section discusses how auditing and penetration testing are used to ensure systems are secure. Audits are used to protect an organization from unwanted change in security settings. Penetration testing attempts to breach security to evaluate the effectiveness of system security and identify vulnerabilities.

CISSP Objectives

3. Security Management
8. Business Continuity Planning

Lecture Focus Questions:

- Why are physical penetration and operations penetration tests valuable to system security?
- What boundaries should you define before starting a penetration test? Why?
- Why does a double blind penetration test provide more valuable data than a single blind test?
- What is the difference between network enumeration and system enumeration?
- How do creeping privileges occur? What countermeasures are used to prevent them?
- How do audits enhance security?

Time

About 25 minutes

Section 3.1: Crime and Law

Preparation

In this section students will learn that cyber crime, a criminal act dealing with computers, is on the rise both locally and internationally. Organizations need to be aware of and in compliance with the laws and regulations for the areas in which business is conducted.

CISSP Objectives

9. Law, Investigations, and Ethics

Lecture Focus Questions:

- What are some obstacles that prosecutors face when dealing with cyber crime?
- How might you be liable to attacks carried out on other organizations?
- What are the differences between common, customary, and religious laws?
- What are the different types of punishments associated with administrative, civil, and criminal law?
- What is the difference between a misdemeanor and a felony?
- How could the Sarbanes-Oxley Act affect your business?
- What mechanisms can you put in place to protect company intellectual assets?

Time

About 30 minutes

Section 3.2: Incident Response

Preparation

This section discusses how to create an incidence response plan to deal with an incident that is a result of a security policy violation or a catastrophic event. This will include identifying members of a Computer Emergency Response Team (CERT) and their roles to act in the event of an emergency. Specialized training is required for evidence collection to be effective for successful prosecution.

CISSP Objectives

9. Law, Investigations, and Ethics

Lecture Focus Questions:

- What are the main objectives of a security response plan?
- Who are the people that should be included in a CERT and how does that affect incident response?
- What are the main goals of short-term, mid-term, and long-term incident response?
- What is the biggest consideration that should be made when deciding to involve the police?
- What is the importance of the chain of custody? When should it start?
- Under what circumstances is hearsay evidence considered admissible?
- What is the correct process for collecting evidence from a crime scene involving a computer or its components?

Time

About 35 minutes

Section 3.3: Ethics

Preparation

This section covers the ethics required of a CISSP security professional. They consist of the ISC2 Code of Ethics, Internet Architecture Board (IAB) standards, and the National Institute of Standards and Technology (NIST) security standards. The students should be familiar and compliant with these general principles of ethical behavior.

CISSP Objectives

9. Law, Investigations, and Ethics

Lecture Focus Questions:

- Following the ISC² code of ethics, how do you decide between conflicting canons?
- What are the consequences of violating the ISC² code of ethics?
- What types of actions does the IAB board deem unethical?
- What are the most important security principles proposed by NIST?

Time

About 10 minutes

Section 4.1: Cryptography Concepts

Preparation

In this section the students will learn how our security is based on cryptography to protect confidentiality and integrity of data. Historical ciphers are presented and also the components of current cryptographic systems. The students will need to become familiar with several cryptographic terms that are defined to help understand cryptographic concepts.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- Why is non-repudiation an important component of cryptography?
- What are the advantages of asymmetric key cryptography over symmetric key cryptography?
- What is the relationship between keyspace and a cryptosystem's work factor?
- How are digital certificates used in asymmetric key cryptography?
- When would you sign and seal a document?
- How do changes in computing power affect cryptosystems?

Time

About 15 minutes

Section 4.2: Hashing

Preparation

This section discusses the use of hashing to ensure the data integrity of files and messages. Four commonly used hashing algorithms are presented as well as several types of hashing methods.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- What service or function is provided by hashes?
- How are hashes used in digital signatures?
- In what ways are HAVAL different from SHA-1? Which method provides greater security?
- What is *collision* and why is this condition undesirable in a hashing algorithm?
- Why is high amplification an indicator of a good hashing algorithm?
- How does HMAC differ from MAC?

Time

About 20 minutes

Section 4.3: Symmetric Cryptography

Preparation

This section discusses how symmetric cryptography is up to 1000 times faster than asymmetric cryptography and is best used on large amounts of data when confidentiality only is sufficient. Two types of symmetric key ciphers are presented; block cipher, and stream cipher. The students will also learn about the vulnerabilities of symmetric cryptography.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- Why are symmetric key stream ciphers considered to be stronger than symmetric key block ciphers?
- How is a pseudo-random number generator different than an initialization vector?
- What advantage does cipher block chaining have over other cipher block encryption methods?
- What is the main disadvantage of symmetric key cryptography?
- What advantages does AES have over Triple DES?

Time

About 50 minutes

Section 4.4: Asymmetric Cryptography

Preparation

This section discusses how asymmetric cryptography provides, not only confidentiality, but also strong authentication, integrity and non-repudiation. This allows users to communicate securely. The components of a Public Key Infrastructure (PKI) and PKI hierarchy are discussed. Students will also learn about the process of ensuring security and availability of digital certificates through certificate management.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- How do public keys differ from private keys? What is the relationship between the two?
- How does sealing differ from signing?
- When is a two tier PKI hierarchy appropriate?
- How does a hierarchy of trust differ from a web of trust?
- When should a private hierarchy be implemented? When should a public hierarchy be implemented?
- How does signing and sealing differ from a mutual authentication and return receipt?

Time

About 85 minutes

Section 4.5: Implementations

Preparation

In this section students will learn how combining the technologies of symmetric cryptography, asymmetric cryptography, and hashing provides much of our current security. The weaknesses and strength of each is discussed as well as the implemented technologies.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- For expired keys, when should you issue new keys? When should you reissue the expired keys?
- What are two ways that the M of n function can be used in key archival?
- How do distribution methods vary for symmetric and asymmetric keys?
- How can symmetric and asymmetric cryptography be used together?
- What are the advantages of symmetric key cryptography over asymmetric key cryptography?

Time

About 40 minutes

Section 5.1: Access Controls

Preparation

This section discusses access controls, which limit a subject's access to objects. Three different types of access control types are presented, Administrative, Technical, and Physical. Students will also become familiar with the characteristics for access controls.

CISSP Objectives

1. Access Controls

Lecture Focus Questions:

- How does authentication differ from authorization?
- What are the differences between administrative, physical, and technical access controls?
- How are corrective and recovery access controls similar?
- How can layering improve access control implementation?
- How do preventive access controls differ from deterrent access controls?

Time

About 10 minutes

Section 5.2: Physical Security

Preparation

In this section students learn how restricting physical access to facilities and computer systems is an organization's first line of defense. Different types of physical access controls are presented including doors, locks, guards, cameras, fences, mantraps, lighting, and sensors. Also discussed, is protecting and securing data on removable or disposed data storage devices.

CISSP Objectives

10. Physical Security

Lecture Focus Questions:

- What advantages do security guards give you over various physical and technological controls?
- What can be added to a mantrap to increase its effectiveness?
- The use of guard dogs should be limited to which area of your facility?
- What two purposes are served by closed-circuit television?
- Why do removable media drives pose a security threat?
- What is the difference between *cleaning* and *sanitizing*?
- Why doesn't deleting files from a hard disk offer sufficient protection against disclosure?

Time

About 30 minutes

Section 5.3: Authentication

Preparation

This section discusses providing authentication credentials to access an object. Three forms of authentication are discussed; something you know, something you have, something you are. A combination of authentication methods can be used to increase security. Methods to improve security of password authentication are also presented. Students will learn the advantages and disadvantages of a Single Sign-On (SSO) as well as two SSO systems, Kerberos and Sesame.

CISSP Objectives

1. Access Controls

Lecture Focus Questions:

- Which form of authentication is generally considered the strongest?
- What are common attributes examined in a biometric system?
- What is the difference between *synchronous* and *asynchronous* token devices?
- What is the difference between strong authentication and two-factor authentication?
- How do behavioral biometric systems work? What types of information do they use for authentication?
- What types of attacks can be directed against smart cards?
- Which biometric error type is the most severe (Type I or Type II)? Why?
- What additional benefits does SESAME provide over Kerberos?

Time

About 50 minutes

Section 5.4: Authorization

Preparation

In this section students will learn how authorization is implemented through privileges and permissions to identify the level of access granted to a subject. Three authorization types are presented; centralized, decentralized, and hybrid. The most commonly used access control models are discussed.

CISSP Objectives

1. Access Controls

Lecture Focus Questions:

- What are the advantages of a centralized authentication system?
- Which access control model uses a matrix? Which method uses classifications labels?
- How does role-based access control differ from rule-based access control?
- What is the best security configuration for a new system?
- What three components are required for a lattice?
- In what ways does a lattice protect data better than a matrix?

Time

About 30 minutes

Section 5.5: Auditing

Preparation

In this section students will discover that organizations use auditing to record user and system actions. Auditing can be used as a preventive method by informing users that their activities are being logged or can be done in a more passive manner as a detection security system.

CISSP Objectives

1. Access Controls

Lecture Focus Questions:

- How can auditing be a preventative security measure?
- In addition to defining the actions to record in an audit log, what else must you do to make auditing effective?
- What problems are associated with logging too many events in the audit trail?
- Why is auditing considered to be a passive detection system?
- What purposes can audit trails serve other than detecting unauthorized activities?

Time

About 10 minutes

Section 5.6: Academic Models

Preparation

This section discusses access control models used for the analysis of security and guidelines for the implementation of system security. Students will learn about important academic security models; Bell-LaPadula, Biba, Clark-Wilson, Brewer and Nash Model, and Take-Grant.

CISSP Objectives

6. Security Architecture

Lecture Focus Questions:

- In the Bell-LaPadula model, how does the * property differ from the strong * property?
- Which academic model(s) address confidentiality? Integrity?
- Which model addresses conflict of interest?
- Which model(s) are examples of Mandatory Access Control (MAC)?
- What are the integrity goals included in the Clark-Wilson model?
- What are the requirements for the Clark-Wilson model?

Time

About 20 minutes

Section 6.1: Trusted Computing

Preparation

This section discusses how a Trusted Computing Base (TCB) is used to ensure that computer information systems remain secure at all times by defining the design, assembly, installation and configuration of the system. Evaluation criteria standards have been created to ensure that a specific computing component meets the security needs. Students will become familiar with three evaluation criteria standards developed by several different countries.

CISSP Objectives

6. Security Architecture

Lecture Focus Questions:

- What are the defining qualities of the state machine? What should take place in the event of a system restart?
- According to the trusted recovery model, what should happen in the case of a security breach?
- How does certification differ from accreditation?
- What is the difference between provisional and full accreditation?
- Which evaluation criteria uses different classes for functionality and assurance?
- What is a major limitation of the TCSEC criteria compared to the ITSEC criteria?
- What are two disadvantages to obtaining a higher classification level with any evaluation criteria?

Time

About 40 minutes

Section 6.2: Computer Architecture

Preparation

This section covers the basics of computer architecture. This will include discussions of hardware and operating system architecture. Hardware architecture of computer systems is designed to support the security requirements of the trusted computing base (TCB) and allow for secure computing. Topics under hardware will include CPU, ALU, Control Unit and buffers. The operating system can include security features to prevent unauthorized access. Topics under software include layering, ring architecture, hiding, isolation and virtual machine. Also discussed are the actions to take to harden the devices and software used to tighten security controls.

CISSP Objectives

6. Security Architecture

Lecture Focus Questions:

- What are the steps of the processing cycle?
- What is the difference between dynamic RAM, ROM, static RAM, and EEPROM?
- While examining system events for a computer, you notice that a page fault has been logged. What has happened?
- What is the role of the virtual memory manager?
- How does physical segmentation differ from logical segmentation? How does each provide a level of security?
- What is the difference between multitasking and multithreading?
- How can asymmetric multiprocessing provide security?
- What three principles must a security kernel satisfy?

Time

About 40 minutes

Section 6.3: Software Development

Preparation

This section discusses the fact that applications can introduce vulnerabilities into information systems. Several methods have been implemented at each phase of application development to ensure security. These include secure planning models, phases of application development, and coding practices. Also discussed is a basic overview and understanding of the concepts of object oriented programming that allows programmers to string together pre-programmed objects to rapidly produce sophisticated applications.

CISSP Objectives

4. Applications Security

Lecture Focus Questions:

- How does the spiral model combine the waterfall model and the prototype model?
- How do object-oriented languages simplify development and improve software quality?
- Why is change control necessary?
- What is the difference between a save point and a check point?
- How do temporary files present a security risk?
- Why do programmers sometimes add back doors during development?
- What is the difference between interpreters, compilers, and assemblers?

Time

About 40 minutes

Section 6.4: Database Management

Preparation

This section discusses the basics of database management. When databases are written securely they can help to protect the confidentiality and integrity of information assets. The integrity of data in a database is ensured through rules imposed by the database management system and through secure database scripting techniques. A basic overview of distributed processing is also presented including multiple standards of technology that have been put in place to regulate and standardize distributed object-oriented systems.

CISSP Objectives

4. Applications Security

Lecture Focus Questions:

- What are the main differences between hierarchal, distributed, and relational databases?
- Which AI system type is best used to analyze concrete data with a discrete number of options?
- What functions are provided by the database management system?
- How can database views be used to provide a measure of security?
- How are a primary key and a foreign key different?
- How does locking protect the integrity of a database? How does locking sometimes lead to problems in query processing?
- When using transactions, what conditions must be met before changes are committed?
- How does Java use the sandbox to provide security?
- How do cookies pose a security threat? Which CIA triad component can be compromised by cookies?

Time

About 55 minutes

Section 7.1: Networking Models and Standards

Preparation

In this section students will review the basics of the OSI model, TCP/IP model and the IEEE 802 standards.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- What functions are performed by the Data Link layer?
- Which devices operate at the Network layer?
- How does the TCP/IP Network Access layer relate to the OSI model?
- What are the differences between TCP and UDP? How are they the same?
- What function is performed by the Address Resolution Protocol (ARP)?
- Which IEEE committee defines standards for Ethernet? Wireless networking?

Time

About 35 minutes

Section 7.2: Network Technology

Preparation

This section overviews networking technologies. Topics include presentations on signaling, media access methods, networking components, and topologies. Students must have a basic and broad understanding of networking technology to plan adequate security measures to protect an information system.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- What is the difference between wave frequency, amplitude, and phase?
- How are synchronous and asynchronous communication different?
- What are the main types of weaknesses involved in networking?
- Which twisted pair cable rating(s) are appropriate for 100 megabit Ethernet?
- Which media type is most resistant to EMI and eavesdropping? Which media type is the most susceptible?
- How does a plenum area pose a safety risk in the event of a fire?
- How does CSMA/CD differ from CSMA/CA?
- What two features are provided by the dual rings of FDDI?
- How many devices are affected by a cable break in a physical bus topology? Physical ring? Physical star?
- How are physical and logical topologies different?

Time

About 75 minutes

Section 7.3: Network Devices

Preparation

This section covers the network devices and systems that establish the information systems infrastructure. Topics include common internetworking devices, the function of Network Address Translation (NAT), Intrusion Detection Systems (IDS), and Intrusion Protection Systems (IPS).

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- How are hubs and switches different?
- What are the differences between collision domains and broadcast domains?
- How many collision domains are on a switch? How many broadcast domains?
- What is a multi-homed firewall?
- Which firewall type can examine the entire contents of a message?
- What type of devices should be placed inside a demilitarized zone (DMZ)?
- How does NAT provide a measure of security to network devices?
- What is the difference between IDS and IPS?
- How are network-based IDS and host-based IDS different?
- How is a honey pot used?

Time

About 75 minutes

Section 7.4: Fault Tolerance

Preparation

In this section the students will review redundant information systems and methods of backup to protect the availability of valuable information assets.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- What is the difference between RAID 1 and RAID 5?
- Which RAID level does not provide fault tolerance?
- Which RAID level does not provide an increase in performance?
- What is the difference between a cold spare and a hot spare?
- What is the difference between a full + incremental backup and a full + differential backup?
- Why can't you combine incremental and differential backup methods?
- Which backup methods do not reset the Archive bit?
- Where should backup media be stored for maximum security?
- Why should you test your restore methods?

Time

About 55 minutes

Section 7.5: Internetworking

Preparation

This section discusses internetworking using Wide Area Network (WAN) technologies and Remote Access. Common WAN transmission media types are discussed and service options. Also discussed, are the basics of remote access including protocols and centralized remote access.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- Which WAN services use analog connectivity?
- What is the difference between basic rate and primary rate ISDN?
- What are the functions of a remote access server?
- How are SLIP and PPP different?
- What advantages are provided by EAP over other forms of authentication?
- How can caller ID and callback be used to improve remote access security?
- In a RADIUS system, which component provides authentication for remote access clients?

Time

About 40 minutes

Section 7.6: Transmission Security

Preparation

In this section students will learn the basics of security for both LAN-based and Web-based transmissions. VPN technology is used for a LAN-based information flow and uses common tunneling protocols and IPSec for encryption. SSL and TLS are used to provide security for data in transit for Web-based applications.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- Which VPN technologies operate at OSI model layer 2?
- What is the difference between AH and ESP?
- What is the function of IKE in IPSec?
- What is the difference between IPSec tunnel mode and transport mode?
- How can you tell that a session with a Web server is using SSL?
- Why are server certificates required in SSL and TLS?
- What additional benefit is provided by requiring client certificates in TLS?

Time

About 60 minutes

Section 7.7: Wireless

Preparation

This section discusses the major concerns of wireless devices and wireless architecture. Wireless networks are inherently insecure and require much attention regarding security. 802.11x standards are presented as well as the transmissions technologies they employ. Common security implementations to protect a wireless network are discussed.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- How are FHSS and DSSS different?
- What are the different frequency ranges for ISM and UNIBAND?
- Which wireless standards use frequencies in the ISM range?
- How does the BSSID differ from the SSID?
- How does key rotation improve wireless security?
- How are a groupwise key and a pairwise key different?
- What improvements did WPA make to overcome the weaknesses of WEP?
- Why shouldn't you use shared secret authentication with WEP?
- Why is a RADIUS server required when using 802.1x authentication?
- How can you add pairwise key rotation when using WEP?
- What is the function of the MIC with WPA and WPA2?
- What encryption mechanisms are used by WEP, WPA, and WPA2?
- How do disabling SSID broadcast and using MAC filtering add security to wireless networks?

Time

About 60 minutes

Section 8.1: Cryptosystem Attacks

Preparation

This section discusses different types of attacks on cryptosystems: cipher text only, known plaintext, chosen plaintext, iterative chosen plaintext, and chosen cipher text. The general methods hackers use for attacking are discussed and the countermeasures to strengthen the cryptosystem.

CISSP Objectives

5. Cryptography

Lecture Focus Questions:

- How does a dictionary attack differ from a brute force attack?
- How is the statistical incidence of two people with the same birthday in a room relevant for cryptography?
- How does having chosen plaintext enhance an attacker's chances of breaking the code over having known plaintext only?
- How is having strong passwords a countermeasure for a dictionary attack?
- What effect does redundant encipherment have on a statistical attack?

Time

About 15 minutes

Section 8.2: Access Control Attacks

Preparation

This section discusses twenty-three different attacks and attack vectors that could be used against network confidentiality and integrity. Students must understand these to adequately protect their information systems. Discussions include access control to protect the components of the CIA Triad, attacks on integrity, attacks on confidentiality and countermeasures.

CISSP Objectives

1. Access Controls

Lecture Focus Questions:

- How are inference and aggregation attacks similar?
- What is the difference between a cracker and a white-hat hacker?
- For what attacks will disabling backdoors be most effective?
- How are spoofing and DNS poisoning similar?
- How does a data diddling attack differ from a salami attack?
- What is the best protection against social engineering attacks?
- What is the main purpose of a replay attack?

Time

About 40 minutes

Section 8.3: Availability Attacks

Preparation

In this section students learn about Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Fifteen common types of DoS and DDoS attacks are presented, as well the countermeasures to protect an information system from these forms of attack.

CISSP Objectives

2. Telecommunications and Network Security
3. Security Management

Lecture Focus Questions:

- How are DoS and DDoS attacks similar?
- What is the difference between a DoS and a DDoS attack?
- How does a Fraggle attack differ from a Smurf attack?
- How are a Land attack and a Teardrop attack similar?
- What attacks are reverse DNS lookups a countermeasure for?
- How can hashes help prevent data loss from DoS or DDoS attacks?
- What is the role of a *zombie*?

Time

About 35 minutes

Section 8.4: Trusted Computing Base Attacks

Preparation

In this section the students will learn about additional attacks, these include attacks on the trusted computing base, malware attacks, common exploitation methods, database threats and vulnerabilities, and attacks on Web servers. Countermeasures for each are explained.

CISSP Objectives

4. Applications Security
6. Security Architecture

Lecture Focus Questions:

- What type of files do anti-virus software need to be able to identify known viruses?
- What must you do to make anti-virus software effective?
- What countermeasures are recommended for Trojan horse and backdoor attacks?
- What is the difference between a buffer overflow attack and a pointer overflow attack?
- What countermeasures do database attacks and Web server attacks have in common?
- Why are cookies a vulnerability?
- How are a covert timing channel and a storage channel similar?

Time

About 60 minutes

Section 8.5: Communication Attacks

Preparation

This section discusses threats to a Private Branch eXchange (PBX) system connecting T1 lines to a phone system and the countermeasures to protect it. Also discussed are the specific security attacks that can be implemented against wireless communications and the countermeasures.

CISSP Objectives

2. Telecommunications and Network Security

Lecture Focus Questions:

- What are two potential effects or costs to businesses from PBX vulnerabilities?
- What is the difference between war dialing and war driving?
- How are replay attacks and man-in-the-middle attacks similar?
- What vulnerability does The Gap in the WAP expose?
- What are effective countermeasures for inbound fax exposure?
- How do strong password policies deter PBX attacks?

Time

About 30 minutes

Summary

Preparation

The summary is a brief review of the major concepts of the CISSP objectives:

- The security program must be senior management driven and fully supported.
- There must be budget justifications for deploying countermeasures.
- Security objectives for the protection of your information system must provide confidentiality, integrity and availability.
- User training and penalties for non-compliance to security policies must be in place.
- Adhere to the ethics of a Security Professional.

Time

About 2 minutes