



Lesson Plans

Systems Security Certified Practitioner (SSCP)

Version 2.0

Table of Contents

Course Overview	3
Introduction to SSCP	5
Section 1.1: Access Control	6
Section 1.2: Access Control Models	7
Section 1.3: Authentication	8
Section 1.4: Authentication Administration	9
Section 1.5: Administration	10
Section 2.1: Cryptography	11
Section 2.2: Symmetric Cryptography	12
Section 2.3: Asymmetric Cryptography	13
Section 2.4: Signatures and Hashing	14
Section 2.5: Public Key Infrastructure	15
Section 2.6: Cryptographic Uses	16
Section 2.7: Cryptographic Attacks	17
Section 3.1: Networking	18
Section 3.2: Local Area Networking	19
Section 3.3: Wide Area Networking	20
Section 3.4: Protocols	21
Section 3.5: Network Devices	22
Section 3.6: Packet Filters	23
Section 3.7: Firewalls	24
Section 3.8: Network Address Translation (NAT)	26
Section 3.9: Remote Access	27
Section 3.10: Virtual Private Networks (VPN)	29
Section 3.11: Wireless	30
Section 4.1: Malicious Code and Attacks	31
Section 4.2: Reconnaissance Attacks	32
Section 4.3: Social Engineering Attacks	33
Section 4.4: Network Attacks	34
Section 4.5: Password Attacks	35
Section 4.6: Availability Attacks	36
Section 4.7: Application Attacks	37
Section 4.8: Web Server Attacks	38
Section 4.9: Browser Security	39
Section 4.10: Communication Attacks	40
Section 4.11: System Hardening	41
Section 5.1: Auditing	42
Section 5.2: Audit Trails	43
Section 5.3: Intrusion Detection	44
Section 5.4: Penetration Testing	45
Section 6.1: Risk Management	46
Section 6.2: Risk Analysis	47
Section 6.3: Business Continuity and Disaster Recovery	48
Section 6.4: Incident Response	49

Section 7.1: Security Administration	50
Section 7.2: Trusted Computing	51
Section 7.3: Development	52
Section 7.4: Employee Management	53
Practice Exams	54

Course Overview

This course prepares students for the Systems Security Certified Practitioner (SSCP) certification exam by International Information Systems Security Certification Consortium, Inc. (ISC)2. It focuses on how to design and maintain security programs. A security program defines what security is for an organization and the procedures for implementation.

Introduction to SSCP

This video introduces the prerequisite to this course, areas of knowledge that will be discussed in this course, and the (ISC)2 Code of Ethics.

Module 1 – Access Control

This module discusses different aspects of access control. Students will learn about access control entities, processes, policies, measures, and models. They will learn about authentication and administration methods to increase security.

Module 2 – Cryptography

In this module students will learn how cryptography is used to store and transmit information in a format that is unreadable to unauthorized individuals. Students will become familiar with symmetric and asymmetric cryptography, signatures and hashing, and public key infrastructure. They will also learn about cryptographic technologies to protect commerce and information in LAN and Web-based environments. Methods of cryptographic attack and countermeasures are also presented.

Module 3 – Networks and Communications

This section covers several elements of networks and communications. Concepts covered about networking include; networking concepts, local area networking, and wide area networking. Concepts covered about managing traffic include using; packets filters, firewalls, and Network Address Translation (NAT). Concepts covered about communications include; configuring remote access, using Virtual Private Networks (VPN) to allow IP traffic to travel securely over a TCP/IP network, and wireless networking technology.

Module 4 – Malicious Code and Attacks

In Module 4 students will learn about malicious code and attacks. They will become familiar with the following types of attacks and countermeasures for; reconnaissance attacks, social engineering attacks, password attacks, availability attacks, application attacks, Web server attacks, and communication attacks. This module also examines securing the browser and hardening a system.

Module 5 – Analysis and Monitoring

Module 5 teaches students the tools that can be used to analyze and monitor a system. This includes tools used for; auditing, creating audit trails, monitoring frames using

intrusion detection, and implementing penetration testing to verify the security of an organization.

Module 6 – Risk, Response, and Recovery

Module 6 discusses elements of risk, response, and recovery. Students will be presented with information about developing plans for risk management and risk analysis, business continuity and disaster recovery, and incident response.

Module 7 – Operations and Administration

In Module 7 students will learn about administration of security management, implementing trusted computing, using a systematic approach to software development to protect security, and managing employees to protect company assets.

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.

Introduction to SSCP

Summary

This video introduces the prerequisite knowledge a student should have before attempting this course. They include knowledge of:

- Network Configurations
- Network Security
- Network Protocols

The instructor also gives an overview of the Common Body of Knowledge (CBK) domains (areas of knowledge) that will be discussed in this course:

- Access Control
- Cryptography
- Networks and Communications
- Malicious Code and Attacks
- Analysis and Monitoring
- Risk, Response, and Recovery
- Operations and Administration

The instructor explains that (ISC)2 requires all candidates that become certified to accept and agree to the (ISC)2 Code of Ethics:

1. Protect Society
2. Act Honorably
3. Provide Competent Services
4. Advance the Profession

The instructor also discusses that individuals who are certified must submit Continuing Education Credits every 3 years.

Time

About 10 minutes

Section 1.1: Access Control

Summary

In this section students will learn how information security is based upon a secure approach which determines what should be accessed, by whom and at what level. To accomplish this, the instructor discusses:

- Access control entities.
- Access control processes.
- Access control policies.
- Access counter measures.

Students will view demonstrations on:

- Managing Microsoft networks using Active Directory.
- Managing Novell networks using eDirectory.

SSCP Exam Domains

- 1. Access Control

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 do preventive access controls differ from deterrent access controls?
- How do directory services benefit a computer network?
- What services do most directory services perform?

Time

About 35 minutes

Number of Exam Questions

5 questions

Section 1.2: Access Control Models

Summary

In this section students will become familiar with commonly used access control models. Concepts covered include the:

- Types of access control models.
- Trusted Computer Security Evaluation Criteria (TCSEC).
- Academic security models.

Students will learn how to:

- Change and configure NTFS permissions.
- Set and modify NetWare file rights.

SSCP Exam Domains

- 1. Access Control

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?
- How does role-based access control differ from rule-based access control?
- How does explicit deny differ from explicit allow?

Time

About 75 minutes

Lab/Activity

- Change NTFS Permissions
- Configure NTFS Permissions
- Modify File System Rights
- Add a Trustee and Rights

Number of Exam Questions

14 questions

Section 1.3: Authentication

Summary

This section discusses using authentication to prove a subject's identity. Concepts covered include:

- Types of authentication.
- Combinations of authentication methods.
- Measuring authentication solutions.
- The role of Single Sign-on (SS) solutions.

SSCP Exam Domains

- 1. Access Control

Lecture Focus Questions:

- Which form of authentication is generally considered the strongest?
- 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 are the components of a strong password policy?
- What additional benefits does SESAME provide over Kerberos?
- What are the main advantages of SSO authentication? Disadvantages?
- What is the relationship between *keys* and *subjects* in Kerberos?

Time

About 60 minutes

Number of Exam Questions

20 questions

Section 1.4: Authentication Administration

Summary

In this section the students will learn administration methods to protect password authentication. Concepts covered include:

- Improving password authentication.
- Controlling password requirements on Microsoft computers.
- Using account lockout to disable a user account.

Students will learn how to:

- Configure Windows account policies to enforce strong password.
- Configure account lockout.
- Configure eDirectory password settings and account restrictions.

SSCP Exam Domains

- 1. Access Control

Lecture Focus Questions:

- What characteristics typically define a strong password?
- When is salting useful in passwords? What advantages does it provide?
- 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?

Time

About 40 minutes

Lab/Activity

- Enforce Password Settings
- Configure Account Lockout
- Modify Password Properties
- Restrict Logon Hours

Number of Exam Questions

7 questions

Section 1.5: Administration

Summary

This section discusses administration precautions to protect information from creeping privileges which allows a user to accumulate privileges over time that are not necessary for their current work tasks. Concepts covered included:

- Precautions to protect against administration creep and corruption of information.
- End-of-life procedures to prevent sensitive data from being accessed by unauthorized users.

Students will learn how to:

- Create and manage domain user accounts.
- Create an eDirectory user.

SSCP Exam Domains

- 1. Access Control

Lecture Focus Questions:

- What are creeping privileges? How can they be prevented?
- What security precautions should be made during the creation phase of the account life cycle?
- What is the best way to clean magnetic data from media so it can be reused?
- What are the approved methods to destroy optical media?

Time

About 40 minutes

Lab/Activity

- Create a Domain User Account
- Disable a User Account
- Reset the Password
- Create a User

Number of Exam Questions

5 questions

Section 2.1: Cryptography

Summary

In this section students will learn about cryptography, which is a method of storing and transmitting information in a format that is unreadable to unauthorized individuals. Cryptography is used by governments, militaries, industries, and individuals to protect data. Concepts covered include:

- Security services provided by cryptographic systems.
- Concepts, terms, and services of cryptography.
- A review of historical ciphers.

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- What two values are used by a cryptographic algorithm to encrypt data?
- What characteristics of the key contribute to the security of encrypted data?
- What are two legitimate uses for cryptanalysis?
- What is the difference between a transposition cipher and a substitution cipher?
- What is the difference between encryption and steganography?
- What is a legitimate use of steganography?

Time

About 35 minutes

Number of Exam Questions

8 questions

Section 2.2: Symmetric Cryptography

Summary

Students will learn the basics of symmetric cryptography which involves using a secret key that is shared between two communication partners. Concepts covered include:

- The role of symmetric cryptography.
- Issues with implementing symmetric key cryptography.
- Common symmetric block cryptography methods.
- The role of symmetric key stream ciphers.

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- Why are symmetric key stream ciphers considered to be stronger than symmetric key block ciphers?
- How does an initialization vector work?
- What is the main disadvantage of symmetric key cryptography?
- What are the four primary modes of DES?
- What advantage does cipher block chaining have over other cipher block encryption methods?
- What advantages does AES have over Triple DES?

Time

About 40 minutes

Number of Exam Questions

18 questions

Section 2.3: Asymmetric Cryptography

Summary

This section examines how asymmetric cryptography is used to communicate securely without having prior access to a shared secret key. Concepts covered include:

- The role of asymmetric cryptography.
- Implementing asymmetric cryptography.
- Common asymmetric key cryptography systems.
- Using a hybrid cryptography system.

SSCP Exam Domains

- 2. Cryptography

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?
- How does RSA work?
- What are the strengths of elliptic curve cryptography?
- How are both symmetric and asymmetric cryptography used in practical applications?

Time

About 15 minutes

Number of Exam Questions

7 questions

Section 2.4: Signatures and Hashing

Summary

In this section students will learn the basics of using digital signatures and hashing to ensure the confidentiality and integrity of data. Concepts covered include:

- The role of hashing.
- Hashing algorithms.
- Digital signature or signing.
- Creating a digital envelope.

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- What service or function is provided by hashes?
- 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 are hashes used in digital signatures?
- How do digital signatures provide confidentiality, integrity validation, strong authentication, and non-repudiation?

Time

About 25 minutes

Number of Exam Questions

11 questions

Section 2.5: Public Key Infrastructure

Summary

This section discusses Public Key Infrastructure (PKI), which is a system that provides for a trusted third party to vouch for user identities and allows binding of public keys to subjects. Concepts covered include:

- Digital certificates.
- X.509 certificates.
- PKI system.
- Public Key Cryptography Standards (PKCS).
- The certificate management process.
- The key management process.

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- How do distribution methods vary for symmetric and asymmetric keys?
- Who authorizes subordinate CAs? Why is this important?
- What does a template standard include?
- What is included in a X.509 certificate?
- How are revoked certificates identified?
- What precautions should be exercised when disposing of private keys?

Time

About 30 minutes

Number of Exam Questions

14 questions

Section 2.6: Cryptographic Uses

Summary

In this section students will learn cryptographic technologies used to protect commerce and information in LAN- and Web-based environments:

- Secure Electronic Transaction (SET).
- Secure Sockets Layer (SSL).
- Transport Layer Security (TLS).
- Secure Hyper Text Transport Protocol (S-HTTP).
- Hyper Text Transport Protocol Secure (HTTPS).
- Secure Shell (SSH).
- Internet Protocol Security (IPSEC).
- E-mail encryption solutions to secure e-mail messages.

Students will learn how to:

- Encrypt a file.
- Encrypt a folder and its contents

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- What are the differences between SSL and TLS?
- Which port is used by IPsec?
- Which protocol is a replacement for S-HTTP?
- How are PGP and S/MIME similar?

Time

About 25 minutes

Lab/Activity

- Encrypt a File
- Encrypt a Folder and Contents

Number of Exam Questions

8 questions

Section 2.7: Cryptographic Attacks

Summary

This section examines cryptographic attacks. Concepts covered include:

- Methods of attack.
- Countermeasures to strengthen the cryptosystem.

SSCP Exam Domains

- 2. Cryptography

Lecture Focus Questions:

- How does a dictionary attack differ from a brute force attack?
- How does having chosen plaintext enhance an attacker's chances of breaking the code over having known plaintext only?
- Why are strong passwords a good countermeasure for a dictionary attack?
- When is the most probable time for a chosen plaintext attack to occur?
- What is the goal of a replay attack?

Time

About 20 minutes

Number of Exam Questions

12 questions

Section 3.1: Networking

Summary

This section discusses networking. Concepts covered include:

- The Open System Interconnection (OSI) model.
- TCP/IP model layers.
- Common TCP/IP protocols.
- Network models.
- Network types.

SSCP Exam Domains

- 3. Networks and Communications

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 three categories of port ranges?
- How do peer-to-peer networks differ from client/server networks? What are the strengths of each?

Time

About 40 minutes

Number of Exam Questions

4 questions

Section 3.2: Local Area Networking

Summary

This section discusses details about local area networking. Concepts covered include:

- Network topologies.
- Networking issues.
- Types of media.
- Susceptibility of media to transmission problems.
- Countermeasures to minimize emanations.
- Signaling systems.
- Network architecture.
- Forms of media access.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- 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?

Time

About 45 minutes

Number of Exam Questions

7 questions

Section 3.3: Wide Area Networking

Summary

This section examines the basics of Wide Area Networking (WAN). Concepts covered include:

- WAN transmission media.
- Service options.
- Additional technologies.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- Which WAN services use analog connectivity?
- What is the difference between basic rate and primary rate ISDN?
- Which WAN service provides the highest bandwidth?
- How does MPLS work?
- What benefits does VoIP provide?

Time

About 20 minutes

Section 3.4: Protocols

Summary

In this section students will learn about protocols for sending data across a network.

Concepts covered include:

- Common protocols.
- The role of Secure Sockets Layer (SSL).
- The role of Transport Layer Security (TLS).

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- What is the drawback to using UDP over TCP? What is one advantage of UDP over TCP?
- What is the main function of ARP?
- How does SSL verify authentication credentials?
- 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 50 minutes

Number of Exam Questions

15 questions

Section 3.5: Network Devices

Summary

This section discusses network devices used to establish the network infrastructure. Concepts covered include:

- Common internetworking devices:
 - Network Interface Card (NIC)
 - Hub
 - Wireless Access Point (WAP)
 - Switch
 - Bridge
 - Router
 - Gateway

Students will learn how to:

- Create a VLAN and assign ports.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- How are hubs and switches different?
- At what OSI layer do switches operate?
- How can VLANs be used to improve security?
- How are MAC addresses used by switches?
- How are bridges different from switches?

Time

About 35 minutes

Lab/Activity

- Create a VLAN and Assign Ports
- Exploring VLAN Communication

Number of Exam Questions

8 questions

Section 3.6: Packet Filters

Summary

This section discusses managing traffic with packet filters. Students will become familiar with defining an inbound filter and an outbound filter.

Students will learn how to:

- Create and configure packet filters.
- Configure and apply ACLs to router interfaces.

SSCP Exam Domains

- 3. Networks and Communications

Time

About 40 minutes

Lab/Activity

- Create a Packet Filter 1
- Create a Packet Filter 2
- Apply Access Lists to Interfaces
- Restrict Traffic from Specific Hosts
- Restrict Traffic from Specific Networks

Section 3.7: Firewalls

Summary

This section examines using firewalls to protect a trusted private network or separate one private network from another. Concepts covered include:

- The role of firewalls.
- Types of firewalls.
- Methods of deploying firewalls.
- Categories of ports specified by Internet Corporation of Assigning Names and Numbers (ICANN).
- Well known ports that correspond to common Internet services.

Students will learn how to:

- Enable Internet Connection Firewall on a Windows XP system.
- Open and close ports in ICF.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- What is a multi-homed firewall?
- Which firewall type can examine the entire contents of a message?
- What is the difference between an application layer firewall and a circuit proxy filter?
- How many firewall devices are used to create a typical demilitarized zone (DMZ)?
- What type of devices should be placed inside a demilitarized zone (DMZ)?
- What port numbers correspond to HTTP traffic? Common e-mail traffic?

Time

About 50 minutes

Lab/Activity

- Enable ICF
- Open ICF Ports
- Close Open Ports
- Prevent ICMP Events

Number of Exam Questions

19 questions

Section 3.8: Network Address Translation (NAT)

Summary

This section covers the basic concepts of using Network Address Translation (NAT) to connect a private network to the Internet without obtaining registered addresses for every host. The private address ranges for two addressing methods are presented:

- IP version 4
- IP version 6

Students will learn how to:

- Configure Internet Connection Sharing (ICS) on a Windows XP system.
- Configure NAT on a Windows router.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- How does NAT provide a measure of security to network devices?
- What should be combined with NAT to increase security?
- What address ranges should you use on private networks connected to the Internet using NAT?
- How does NAT provide two way traffic flow?

Time

About 25 minutes

Lab/Activity

- Share an Internet Connection
- Configure NAT

Number of Exam Questions

4 questions

Section 3.9: Remote Access

Summary

In this section students will learn about configuring remote access. Concepts covered include:

- Remote access protocols.
- Protocols to deploy centralized authentication.

Students will learn how to:

- Configure a remote access server, including remote access policies.
- Configure a remote access client connection.
- Customize remote access authentication protocols.
- Configure RADIUS clients and servers.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- 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?
- How does TACACS implement multi-factor authentication?
- How is TACACS an improvement over RADIUS?
- What are the main benefits of DIAMETER?

Time

About 75 minutes

Lab/Activity

- Configure a Remote Access Server
- Create a Remote Access Policy
- Create a Dialup Connection
- Configure Advanced Authentication
- Configure Smart Card for Authentication
- Configure a RADIUS Server
- Configure a RADIUS Client

Number of Exam Questions

11 questions

Section 3.10: Virtual Private Networks (VPN)

Summary

This section examines using a Virtual Private Network (VPN) to allow IP traffic to travel securely over the TCP/IP network. Concepts covered include:

- Common tunneling protocols.
- Using IPSec to provide encryption.
- IPSec protocols.
- IPSec modes of operation.

Students will learn how to:

- Configure a VPN server.
- Configure a client VPN connection.
- Configure specific VPN protocols.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- 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?
- Which VPN technologies operate at OSI model layer 2?
- How is L2TP an improvement over PPTP and L2F?

Time

About 65 minutes

Lab/Activity

- Configure a VPN Server
- Disable PPTP Ports
- Create a Client VPN Connection
- Customize the Tunneling Protocol

Number of Exam Questions

10 questions

Section 3.11: Wireless

Summary

This section provides a basic overview of the wireless networking technology. Concepts covered include:

- Wireless transmission technologies.
- Common wireless standards.
- Wireless networking standards.
- Configuring a wireless LAN.
- Methods to provide authentication on a wireless network.
- Security for wireless networking.

SSCP Exam Domains

- 3. Networks and Communications

Lecture Focus Questions:

- How are FHSS and DSSS different?
- How does the BSSID differ from the SSID?
- 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?
- What is the function of the MIC with WPA and WPA2?
- Which encryption mechanisms are used by WEP, WPA, and WPA2?

Time

About 30 minutes

Number of Exam Questions

17 questions

Section 4.1: Malicious Code and Attacks

Summary

This section discusses malicious code and attacks. Students will become familiar with the following concepts:

- Defining attackers.
- Examples of common malware.
- Countermeasures for malware attacks.
- Historic malware events.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What's the difference between a hacker and a cracker?
- Which types of malware can self replicate?
- 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 attacks?
- How did the ILOVEYOU virus propagate?

Time

About 50 minutes

Number of Exam Questions

16 questions

Section 4.2: Reconnaissance Attacks

Summary

This section provides an overview of reconnaissance used to plan a mode of attack. Concepts covered include:

- The basic stages of reconnaissance.
- Countermeasures for preventing reconnaissance.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What types of activities are considered passive reconnaissance?
- What are popular network scanning tools?
- How does a Christmas tree scan work?
- How can reconnaissance be prevented?

Time

About 15 minutes

Number of Exam Questions

2 questions

Section 4.3: Social Engineering Attacks

Summary

This section examines using social engineering attacks to exploit human nature by convincing someone to reveal information or perform an activity. Concepts covered include:

- Defining social engineering.
- Main types of social engineering attacks.
- Specific social engineering attacks.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What human traits are exploited in a social engineering attack?
- What is the best defense against a social engineering attack?
- A caller tells you he is a network administrator and needs information about the computer on your desk. What type of social engineering attack is he using?
- How does a phishing attack work?

Time

About 15 minutes

Number of Exam Questions

9 questions

Section 4.4: Network Attacks

Summary

This section discusses common attacks that exploit network communications. Network attacks and countermeasures for each are presented:

- Spoofing
- Sniffing
- Hijacking
- Man-in-the-middle
- Replay

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What is the main purpose of a replay attack?
- How does spoofing work? How can it be prevented?
- Which protocols typically transfer data in clear text? What does this mean for the security of the information?
- How are hijacking and man-in-the-middle attacks related?

Time

About 25 minutes

Number of Exam Questions

14 questions

Section 4.5: Password Attacks

Summary

In this section students will learn about attacks that are directed at passwords. Concepts covered include:

- Common password attacks
- Collecting hashed passwords
- Cracking hashed passwords.
- Countermeasures for password attacks

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- How does a dictionary attack differ from a brute force attack?
- How can hashed passwords be collected?
- How does a rainbow table speed up the password cracking process?
- What are the best countermeasures for attacks against passwords?

Time

About 30 minutes

Number of Exam Questions

9 questions

Section 4.6: Availability Attacks

Summary

This section teaches the students about availability attacks, which consists of Denial of Service (DoS) attacks and Distributed Denial of Service attacks (DDoS). Concepts covered include:

- Common forms of DoS attacks.
- Common forms of DDoS attacks.
- Countermeasures for DoS and DDoS attacks.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- How are DoS and DDoS attacks similar? How are they different?
- How does a Fraggle attack differ from a Smurf attack?
- How are a Land attack and a Teardrop attack similar?
- Which attacks can be prevented with reverse DNS lookups?
- What is the role of a zombie?

Time

About 40 minutes

Number of Exam Questions

15 questions

Section 4.7: Application Attacks

Summary

This section discusses common application exploitation attacks. Concepts covered include:

- Backdoor attacks.
- Buffer overflow attacks.
- Pointer overflow attacks.
- Salami attacks.
- Data diddling.
- Excessive permissions.
- Unprotected temporary files.
- Directory traversal.
- Covert channels.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- How are backdoors most commonly exploited?
- How does a data diddling attack differ from a salami attack?
- How do excessive permissions affect the vulnerability of an application?
- How does directory traversal work? How can it be prevented?
- What is the difference between a buffer overflow attack and a pointer overflow attack?
- How are a covert timing channel and a storage channel similar?

Time

About 20 minutes

Number of Exam Questions

9 questions

Section 4.8: Web Server Attacks

Summary

This section teaches students how to secure a Web site from Web server attacks.

Concepts covered include:

- Applications commonly used for Web-based applications or scripting programs.
- Countermeasures for Web server-based attacks.

Students will learn how to:

- Configure authentication for Web sites and Web folders.
- Configure IIS permissions.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- How does Java use the sandbox to provide security?
- How does client-side scripting differ from server-side scripting?
- How is ActiveX vulnerable to attacks?
- What are the best countermeasures for Web server attacks?

Time

About 30 minutes

Lab/Activity

- Configure Web Site Authentication
- Configure Web Folder Authentication
- Configure IIS Permissions

Number of Exam Questions

5 questions

Section 4.9: Browser Security

Summary

This section examines securing the browser from attacks. Concepts covered include:

- Indications of an unsecured connection or attack.
- Preventing browser attacks.

Students will learn how to:

- Clear the Internet Explorer cache.
- Configure security zones in Internet Explorer.
- Configure cookie and security settings for Internet Explorer.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- How do cookies pose a security threat? Which CIA triad component can be compromised by cookies?
- How is cache used on the Internet? How does it make a system vulnerable?
- What are the different Internet Explorer zones? Which has the highest security settings?
- What can you look for that may indicate an unsecured connection or an attack?

Time

About 60 minutes

Lab/Activity

- Clear the Browser Cache
- Add a Trusted Site
- Add a Restricted Site
- Customize Zone Settings
- Change the Cookie Level
- Customize Cookie Handling
- Configure Browser Security
- Clear Temporary Internet Files

Number of Exam Questions

5 questions

Section 4.10: Communication Attacks

Summary

This section provides information about wireless, phone, and cell phone attacks.

Concepts covered include:

- Wireless networks vulnerabilities.
- Measures to protect a wireless network.
- Common phone exploitation attacks.
- Common cell phone exploitation attacks.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What is the purpose of warchalking?
- How are rogue access points used in man-in-the-middle attacks?
- How does MAC address filtering and disabling DHCP on a wireless access point provide some measure of security?
- What are the different methods used for wireless authentication? Which is the most secure?
- How does a site survey impact wireless security?
- How is cramming different than slamming?
- What are the most common types of cell phone exploitation attacks?

Time

About 35 minutes

Number of Exam Questions

10 questions

Section 4.11: System Hardening

Summary

This section provides recommendations and the processes to harden a system. Concepts covered include:

- Hardening devices.
- Hardening individual services or applications.

Students will learn how to:

- Disable and uninstall networking components.
- Download and apply Windows operating system updates.
- Manage services on a Windows system.
- Identify excess services and software running on a system.

SSCP Exam Domains

- 4. Malicious Code and Attacks

Lecture Focus Questions:

- What is system hardening? How does it benefit the security of an organization?
- What is a security baseline?
- How do system updates relate to system security?
- What are the vulnerabilities of FTP? DNS?

Time

About 40 minutes

Lab/Activity

- Disable File and Printer Sharing
- Disable NetBIOS over TCP/IP
- Stop and Disable Services

Number of Exam Questions

8 questions

Section 5.1: Auditing

Summary

In this section students will learn how to use auditing to ensure that the current implementation meets the security goals of the organization. Concepts covered include:

- The role of auditing.
- Audit domains.
- Methods auditors use to gather information.
- Types of auditors.
- Applying due care and due diligence.
- Preventing creeping privileges.
- Post audit activities.
- Standardized auditing models
- Auditing methods and tools.

SSCP Exam Domains

- 5. Analysis and Monitoring

Lecture Focus Questions:

- How is an audit benchmark used?
- What are the benefits of internal auditors? External auditors?
- What are methods an auditor can use to gather data?
- What is the importance of a clearly defined audit scope?
- How can creeping privileges be avoided?
- How can you benefit from applying a standardized model when performing an audit?

Time

About 35 minutes

Number of Exam Questions

3 questions

Section 5.2: Audit Trails

Summary

This section discusses using audit trails to trace the cause of events and provide problem resolution. Concepts covered include:

- The role of an audit trail.
- Components of an auditing subsystem.
- Types of events the audit trail should include.
- The role of logging.

Students will learn how to:

- Enable system auditing
- Save audit logs
- Change audit log properties

SSCP Exam Domains

- 5. Analysis and Monitoring

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 50 minutes

Lab/Activity

- Enable Auditing 1
- Enable Auditing 2
- Save the Audit Log
- Change Log Properties
- Configure the System to Shut Down

Number of Exam Questions

10 questions

Section 5.3: Intrusion Detection

Summary

This section examines using intrusion detection to detect and protect the network from suspicious activity by monitoring frames on the network. Concepts covered include:

- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- Honeypot
- Padded cell (also referred to as a tar pit or honey net)

SSCP Exam Domains

- 5. Analysis and Monitoring

Lecture Focus Questions:

- What is the difference between IPS and IDS?
- How are network-based IDS and host-based IDS different?
- What are clipping levels and thresholds?
- What are the strengths and weaknesses of anomaly recognition? Signature recognition?
- How is a honey pot used?

Time

About 30 minutes

Number of Exam Questions

15 questions

Section 5.4: Penetration Testing

Summary

In this section students will learn how penetration testing can be used to assure the effectiveness of an organization's security implementations and countermeasures. Concepts covered include:

- Defining the Rules of Engagement (ROE).
- Defining the penetration testing teams.
- Types of penetration testing.
- Levels of knowledge the attack and system personnel have prior to the attack.
- Stages of penetration testing.

SSCP Exam Domains

- 5. Analysis and Monitoring

Lecture Focus Questions:

- Why are physical penetration and operation penetration tests valuable to system security?
- What boundaries should be defined 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?

Time

About 45 minutes

Number of Exam Questions

8 questions

Section 6.1: Risk Management

Summary

This section discusses risk management for an organization. Concepts covered include:

- Sources of threats.
- An organization's approach to risk.
- The processes involved in risk management.

SSCP Exam Domains

- 6. Risk, Response, and Recovery

Lecture Focus Questions:

- What are the sources of threats?
- How does the threat source affect the countermeasures you might put in place?
- How is the proactive approach to risk different than the reactive approach?
- What approach to risk demonstrates due care and due diligence?

Time

About 10 minutes

Number of Exam Questions

1 question

Section 6.2: Risk Analysis

Summary

This section discusses using risk analysis to protect assets. Concepts covered include:

- The terms related to risk analysis.
- The general steps to perform a risk analysis and develop a plan to respond to the risk.
- Selecting and deploying countermeasures.
- Acceptable responses to risk.
- Asset analysis theories.
- Quantitative risk analysis formulas.

SSCP Exam Domains

- 6. Risk, Response, and Recovery

Lecture Focus Questions:

- What is the difference between a *threat* and a *threat agent*?
- What is the difference between asset exposure and asset vulnerability?
- How do tangible assets differ from intangible assets?
- How can an organization transfer risk?
- When should a countermeasure *not* be implemented?
- When is risk acceptance appropriate? When is risk rejection appropriate?
- What is the relationship between the control gap and residual risk?
- How does the single loss expectancy affect the annualize rate of occurrence?

Time

About 40 minutes

Number of Exam Questions

12 questions

Section 6.3: Business Continuity and Disaster Recovery

Summary

In this section students will learn about planning for a disruptive event. Concepts covered include:

- Disaster Recovery Planning (DRP).
- Business Continuity Planning (BCP).
- Incident recovery.
- The Business Impact Analysis (BIA).
- Guidelines for plan testing.
- Backup methods and strategies.
- Redundancy solutions.

SSCP Exam Domains

- 6. Risk, Response, and Recovery

Lecture Focus Questions:

- What is the primary difference between disaster recovery and business continuity planning?
- What are the objectives of security planning?
- How do the primary tasks of the recovery team differ from the primary tasks of the salvage team?
- What are the major stages in the Business Impact Analysis (BIA)?
- What are the differences between compliance and substantive testing?
- Which backup options reset the archive bit?
- Why are hot sites typically not implemented? Why might cold sites be of little use when recovering from a disaster?
- What are the drawbacks to a mutual aid agreement?

Time

About 50 minutes

Number of Exam Questions

21 questions

Section 6.4: Incident Response

Summary

Students will learn how to respond to a security incident. Concepts covered include:

- Incident response plans.
- Computer forensics.
- Ensuring evidence is admissible in court.
- The life cycle of evidence.
- The chain of custody.

SSCP Exam Domains

- 6. Risk, Response, and Recovery

Lecture Focus Questions:

- What are the responsibilities of the CIRT team?
- What is considered a security incident?
- How is computer evidence authenticated?
- What is required to ensure admissibility of evidence in court?
- What is the best method for duplicating hard drives?
- What is the purpose of the chain of custody?
- What precautions should be taken during the transportation and storage of evidence?

Time

About 40 minutes

Number of Exam Questions

12 questions

Section 7.1: Security Administration

Summary

This section discusses administration of security management to preserve the confidentiality, integrity and availability of all critical and valuable assets. Concepts covered include:

- Security management responsibilities.
- Operational security to establish defense and depth.
- Implementing a security policy.
- Protecting an organization with plans and policies.

SSCP Exam Domains

- 7. Operations and Administration

Lecture Focus Questions:

- How do the five components of a security policy document work together?
- In what situations would you use a security guideline instead of a security procedure?
- What is the importance of establishing baselines?
- What is defense in depth and how does it increase an organization's security?
- What are the steps in the change control process?

Time

About 20 minutes

Number of Exam Questions

15 questions

Section 7.2: Trusted Computing

Summary

In this section students will learn about using a trusted computing base to ensure that a system behaves properly and adheres to the organization's security policy. A trusted computing base is a combination of hardware, software, and all the controls that form the trusted computing base of that system. Concepts covered include:

- A Protection Profile (PP).
- Secure operating systems.
- Trusted Computing Base (TCB).
- Evaluation criteria standards.

SSCP Exam Domains

- 7. Operations and Administration

Lecture Focus Questions:

- 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 the four modes of security that should be included in a protection profile?
- What levels of access does a reference monitor use?
- How does layering provide security to an operating system?
- How does commercial classification labeling differ from military?

Time

About 40 minutes

Number of Exam Questions

20 questions

Section 7.3: Development

Summary

This section discusses software development. The System Development Life Cycle (SDLC) is a systematic method for design, development, and change management used for software development and implementation of system and security projects. Concepts covered include:

- The phases of the SDLC.
- The execution of change control.
- Standardized development models.

SSCP Exam Domains

- 7. Operations and Administration

Lecture Focus Questions:

- How does the spiral model combine the waterfall model and the prototype model?
- How should security be employed in the different stages of development?
- What does functional design entail?
- When is change control necessary?
- What are the responsibilities of developers after a product is released?

Time

About 25 minutes

Number of Exam Questions

11 questions

Section 7.4: Employee Management

Summary

In this section students will learn how to use employee management to ensure that employees play a major role in protecting company assets. Concepts covered include:

- Employee management principles.
- Employee-related security vulnerabilities.
- Employee security processes.
- Employment agreements.
- Setting employee expectations and responsibilities.
- Ensuring ethics.

SSCP Exam Domains

- 7. Operations and Administration

Lecture Focus Questions:

- How can pre-employment processing improve the security of an organization?
- What is the role of the policy handbook regarding security?
- What guidelines must be considered when monitoring employees?
- Why should employees be required to sign employment agreements?
- How are separation of duties and two-man control different?
- How can collusion be avoided?
- What is the importance of a clear job description?

Time

About 25 minutes

Number of Exam Questions

13 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 **Domain 1: Access Control** are grouped together and presented in practice exam *Domain 1: Access Control, All Questions*. Students will typically take about 60-90 minutes to complete each of the following practice exams.

Domain 1: Access Control, All Questions (52 questions)

Domain 2: Cryptography, All Questions (78 questions)

Domain 3: Networks and Communications, All Questions (98 questions)

Domain 4: Malicious Code and Attacks, All Questions (102 questions)

Domain 5: Analysis and Monitoring, All Questions (36 questions)

Domain 6: Risk, Response, and Recovery, All Questions (46 questions)

Domain 7: Operations and Administration, All Questions (58 questions)

The *Certification Practice Exam* consists of 125 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 180 minutes -- just like the real certification exam. A passing score of 90% should verify that the student has mastered the concepts and is ready to take the real certification exam.