CompTIA Security+ Study Guide (SY0-501)

Syllabus

Session 1

At the end of this session, students will understand what risk is and the basics of what it means to have security in an organization. This includes the following concepts:

Risk management, covering CompTIA objectives:

5.2 Summarize business impact analysis concepts

5.3 Explain risk management processes and concepts

Book Chapter: Chapter 1

Ancillary Lab 1

Session 2

At the end of this session, students will understand how security is implemented in a workplace environment. This includes the following concepts:

Architecture and design, covering CompTIA objective:

3.8 Explain how resiliency and automation strategies reduce risk

Risk management, covering CompTIA objectives:

5.1 Explain the importance of policies, plans, and procedures related to organizational security

5.2 Summarize business impact analysis concepts

5.3 Explain risk management processes and concepts

Book Chapter: Chapter 1

Ancillary Lab 2

Session 3

This session describes some of the issues that many security professionals face when dealing with security postures and network monitoring. This includes the following topics:

Architecture and design, covering CompTIA objectives:

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides

3.2 Given a scenario, implement secure network architecture concepts

Book Chapter: Chapter 2

Ancillary Lab 3

Session 4

This session starts looking at secure systems design. This includes the following topics:

Architecture and design, covering CompTIA objectives:

3.3 Given a scenario, implement secure systems design

3.4 Explain the importance of secure staging deployment concepts

Book Chapter: Chapter 2

Ancillary Lab 4

Session 5

This session looks at infrastructure and the devices that are used to build and secure it. This session includes the following:

Technologies and tools, covering CompTIA objective:

2.1 Install and configure network components, both hardware- and software-based to support organizational security

Book Chapter: Chapter 3

Ancillary Lab 5

Session 6

This session concludes the look at infrastructure ways to deal with network issues. This session includes the following:

Technologies and tools, covering CompTIA objective:

2.1 Install and configure network components, both hardware- and software-based to support organizational security

Book Chapter: Chapter 3

Ancillary Lab 6

Session 7

In this session, students will learn about the basics of access control. This session includes the following:

Technologies and tools, covering CompTIA objectives:

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

2.3 Given a scenario, troubleshoot common security issues

2.4 Given a scenario, analyze and interpret output from security technologies

Book Chapter: Chapter 4

Ancillary Lab 7

Session 8

In this session, students continue learning about the basics of access control, authentication, and authorization. This session includes the following:

Identity and access Management, including CompTIA objectives:

4.1 Compare and contrast identity and access management concepts

4.2 Given a scenario, install and configure identity and access services

4.3 Given a scenario, implement identity and access management controls

Book Chapter: Chapter 4

Ancillary Lab 8

Session 9

In this section, students will learn about wireless network security. Topics include the following:

Threats, attacks, and vulnerabilities, covering CompTIA objective:

1.2 Compare and contrast types of attacks

Book Chapter: Chapter 5

Sample Lab 9

Session 10

In this session, students will learn about cloud computing and security issues related with it, including such topics as:

Architecture and design, including CompTIA objective:

3.7 Summarize cloud and virtualization concepts

Book Chapter: Chapter 6

Sample Lab 10

Session 11

In this session, students will learn about host, data, and application security. Topics covered include the following:

Threats, attacks, and vulnerabilities, including CompTIA objectives:

1.3 Explain threat actor types and attributes

1.6 Explain the impact associated with types of vulnerabilities

Book Chapter: Chapter 7

Sample Lab 11

Sample Lab 12

Session 12

In this session, students will continue the discussion about host, data, and application security. Topics covered include the following:

Architecture and design, including CompTIA objectives:

3.5 Explain the security implications of embedded systems

3.6 Summarize secure application development and deployment concepts

Book Chapter: Chapter 7

Sample Lab 13

Session 13

Cryptography is one of the largest parts of communications security. In this chapter, students will learn about different types of attacks that are used to try and break cryptography. Topics include the following:

Threats, attacks, and vulnerabilities, covering CompTIA objective:

1.2 Compare and contrast types of attacks

Cryptography and PKI, including CompTIA objective:

6.1 Compare and contrast basic concepts of cryptography

Book Chapter: Chapter 8

Sample Lab 14

Session 14

In this session, students will continue learning about cryptography and how it is used. Topics include the following:

Cryptography and PKI, including CompTIA objectives:

6.2 Explain cryptography algorithms and their basic characteristics

6.3 Given a scenario, install and configure wireless security settings

Book Chapter: Chapter 8

Sample Lab 15

Session 15

In this session, students will finish learning about cryptography and how it is used. Topics include the following:

Cryptography and PKI, including CompTIA objectives:

6.3 Given a scenario, install and configure wireless security settings

6.4 Given a scenario, implement public key infrastructure

Book Chapter: Chapter 8

Sample Lab 16

Session 16

In this section, students will learn about malware, vulnerabilities, and threats to security. Topics include the following:

Threats, attacks, and vulnerabilities, including CompTIA objectives:

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware

1.2 Compare and contrast types of attacks

Book Chapter: Chapter 9

Sample Lab 17

Session 17

In this section, students will continue to learn about malware, vulnerabilities, and threats to security. Topics include the following:

Threats, attacks, and vulnerabilities, including CompTIA objectives:

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware

1.2 Compare and contrast types of attacks

Book Chapter: Chapter 9

Sample Lab 18

Session 18

In this section, students will learn about physical security, environmental controls, social engineering, and other foes. Topics include the following:

Threats, attacks, and vulnerabilities, covering CompTIA objective:

1.2 Compare and contrast types of attacks

Architecture and design, including CompTIA objective:

3.9 Explain the importance of physical security controls

Book Chapter: Chapter 10

Sample Lab 19

Sample Lab 20

Session 19

In this section, students will continue to learn about social engineering and the need for appropriate controls. Topics include the following:

Risk management, including CompTIA objectives:

5.7 Compare and contrast various types of controls

5.8 Given a scenario, carry out data security and privacy practices

Book Chapter: Chapter 10

Sample Lab 21

Sample Lab 22

Session 20

In this section, students will learn about common security administration issues, policies and procedures. Topics include the following:

Technologies and tools, covering CompTIA objective:

2.5 Given a scenario, deploy mobile devices securely

Identity and access management, including CompTIA objective:

4.4 Given a scenario, differentiate common account management practices

Chapter 11

Sample Lab 23

Session 21

In this section, students will continue to learn about common security administration issues, policies and procedures. Topics include the following:

Technologies and tools, covering CompTIA objective:

2.5 Given a scenario, deploy mobile devices securely

Identity and access management, including CompTIA objective:

4.4 Given a scenario, differentiate common account management practices

Chapter 11

Sample Lab 24

Sample Lab 25

Session 22

In this section, students will discuss disaster recovery and incident response policies and procedures. Topics include the following:

Threats, attacks, and vulnerabilities, covering CompTIA objectives:

1.4 Explain penetration testing concepts

1.5 Explain vulnerability scanning concepts

Chapter 12

Sample Lab 26

Session 23

In this section, students will finish discussing disaster recovery and incident response policies and procedures. Topics include the following:

Risk management, covering CompTIA objectives:

5.4 Given a scenario, following incident response procedures

5.5 Summarize basic concepts of forensics

5.6 Explain disaster recovery and continuity of operation concepts

Chapter 12

Sample Lab 27

Sample Lab 28

Optional Labs

Included in the labs are three optional ones that can be used to round out sessions as needed:

Sample Lab 29

Sample Lab 30