**Learning Tips for Chapter 11**

This chapter discusses several network security topics introduced in previous chapters and provides additional clarity on others.

Numerous important terms are described in the chapter’s opening pages including network vulnerabilities, attack surfaces, and attack vectors. It is valuable to have a clear understanding of these.

Common vulnerabilities and attacks are identified in the chapter’s early pages. The contents of the lists are unlikely to be surprising, but it is important to know what is common and what is not. It is also important for you to be aware of how organizations usually respond to cybersecurity attacks.

The CIA triad is widely used to focus attention on the overarching goals of network security, and it is something that you should focus on.

It is important for you to understand that organizations use threat analysis and the assignment of risk values to pinpoint network assets whose security warrants prioritized attention. These are important risk management activities.

It is valuable for you to understand the differences between security plans, policies, and procedures. It is also valuable for you to have a general understanding of what security policies typically include and to realize that security plans, policies, procedures, and user training are included in the outermost layer of defense in depth (DiD).

It is important for you to understand the rationale behind layered defenses and DiD and to realize that DiD continues to guide the deployment of network security defenses, despite the emergence of zero trust security.

It is valuable for you to realize that DiD is an example of network security architecture and that network architectures, including zero trust architecture, typically have layers.

The last half of the chapter focuses on security issues and defenses associated with the physical, cloud, perimeter, and internal network layers of DiD. Here it is important to have a general understanding of the major threats and issues associated with each layer and a more detailed understanding of the defenses used at the layer.

DiD is a useful vehicle for better understanding the wide array of security mechanisms used to protect today’s networks. Considering security issues and defenses layer-by-layer makes it easier to see that security defenses are deployed in a systematic rather than haphazard fashion.

It is valuable for you to understand that physical security is important with computer rooms and facilities that include network infrastructure, but often extends outside the buildings/facilities, especially for data centers.

A cloud security layer has been added to some recent depictions of DiD. This makes sense since enterprise networks routinely include cloud infrastructure and services. Hence, it is important to have a general understanding of security defenses for cloud resources and data traffic to/from the cloud.

Perimeter security has been a traditional network security concern, and a wide range of perimeter defenses are common including firewalls, DMZ networks, IDSs, and IPSs. This and the internal network security sections warrant more attention than the other sections in the last half of the chapter.

APTs are among the most concerning internal network security threats, and it is important for you to have a good understanding of what they are, how they begin, and why lateral movement controls are used to detect and combat them.

Encryption has been mentioned countless times in previous chapters without being fully explained. This makes the cryptography section and its descriptions of symmetric and asymmetric encryption and PKI especially important.

Having a good grasp of the DiD layers described in this chapter provides a good foundation for understanding the other three layers, which are the subject of Chapter 12.

Do not ignore the Key Concepts in Chapter 11 Presentation.

You are also encouraged to leverage the supplement videos and readings for this chapter.

Use the Chapter 11 Problems and Exercises tips to assist with any problems and exercises that you may be assigned.

The appendices for Chapter 11 provide additional information on numerous topics in this chapter.

**Especially Important Sections**

Sections 11.1.1 and 11.1.2

Sections 11.2.1 and 11.2.2

Sections 11.3.1 and 11.3.2

Section 11.4

Section 11.5.2

Section 11.5.3

Sections 11.6 and 11.7

Section 11.8 and each of its subsections

Section 11.9 and each of its subsections

**Especially Important Figures and Tables**

*Note:* It is important to read/study the discussion related to each figure and table that is identified.

Figure 11-1

Tables 11-1 and 11-2

Table 11-3

Table 11-4

Figure 11-4 and Table 11-5

Table 11-6

Figure 11-5

Figure 11-6

Table 11-7

Table 11-8

Figure 11-11

Figure 11-12

Table 11-9

Table 11-10

Table 11-11

Figure 11-14

Figures 11-15 and 11-16

Table 11-12

Table 11-13

Table 11-14

Figures 11-17 and 11-18

Figure 11-19

Figures 11-20, 11-21, and 11-22

**Especially Important Key Terms**

Asymmetric encryption algorithms

Certificate authority (CA)

DMZ network

Encryption

Internet Key Exchange (IKE)

Intrusion detection system (IDS)

Intrusion prevention system (IPS)

Lateral movement

Network attack surface

Network perimeter

Network vulnerability

Public key infrastructure (PKI)

Secure access service edge (SASE)

Secured web gateway (SWG)

Symmetric encryption algorithms

Unified threat management (UTM) systems

**Especially Important Review Questions**

Questions 1-7, 9-11, 13-29

**Especially Valuable Problems and Exercises**

Exercises 11-1, 11-2, 11-5