**Chapter 11 Problems and Exercises Tips**

**1) Many of the threats to enterprise networks are also threats to personal computing devices. For example, you may be targeted in a phishing attack by intruders who want to install malware (e.g., viruses and ransomware) and/or compromise your device for botnet attacks on other networks. Also, if you have important files stored on your device, a hard drive failure could make them inaccessible. Your life could also be impacted if your device was stolen. Given these everyday realities, do an abbreviated threat analysis for a personal device such as a laptop.**

**A) Identify at least five major threats, existing safeguards to protect your device from the threats, and additional security controls that could be added to provide further protection or to mitigate attack damage.**

**Consider using the following table to organize this information.**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Existing Safeguards** | **Additional Security Controls** |
|  |  |  |
|  |  |  |

**Part A Tips for Success:** This part of the exercise enables you to develop a better understanding of threat analysis and how it may be applied to personal devices. Threat and risk analysis are discussed in section 11.3.2; Tables 11-6, and Figures 11-5 and 11-6 are relevant. Section 12.1.1 and 12.1.3 may also be useful.

Be sure to identify at least five threats or vulnerabilities for the device; some of these may need brief descriptions. Strive to focus on critical and medium-level risks and avoid low-level risks. Be sure to specify what is being done to protect the device against each threat; if there are no current safeguards in place, say so. Also, be sure to identify and briefly describe at least one additional safeguard that could be used to protect your device from the threat. Here, content from Chapters 11 and 12 in the book can be helpful. Keep in mind that you are being asked to complete all five rows and all three columns of the table. Proofread your completed table to ensure that it is free from spelling and grammatical errors.

**B) Consider how you would arrange current and additional security mechanisms for your personal device in a layered manner, such as defense in depth (DiD). Identify the layer at which the security mechanism is used (e.g., physical, perimeter) and briefly describe how it deters intruders from reaching the next layer.**

**Part B Tips for Success**: In this part of the exercise, you should consider the security safeguards identified in the existing and additional columns of the table you developed for part A from a DiD perspective. Consider using a table like the following to organize the security safeguards from your part A table.

|  |  |  |
| --- | --- | --- |
| **DiD Layer** | **Security Safeguard(s)** | **How Safeguard Deters Intruders** |
| Physical |  |  |
| Perimeter |  |  |
| Network |  |  |
| Endpoint |  |  |
| Application |  |  |
| Data |  |  |

Because you are using safeguards from your part A table, the part B table may have some rows with several safeguards and other rows with none. Keep in mind that the purpose of part B is to get you thinking about how safeguards for personal devices map to DiD layers. Be sure to proofread your part B table or narrative to ensure that it is free of spelling or grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with format specifications | 10 |
| Identifies at least five potential threats | 10 |
| Identifies existing safeguards for each threat | 10 |
| Identifies at least one additional security control for each threat | 10 |
| Identifies appropriate layering for current and additional security controls | 20 |
| Briefly describes how each security control deters intruders from reaching next layer | 20 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |

**2) You have been hired as a security analyst by a start-up that creates, hosts, and maintains websites for clients. The company’s 15 web developers generate an average of 250 Gigabytes of content per person every month, and most of this is shared with clients over the Internet before being added to their websites. As the company’s client base continues to grow, so does its processing and storage requirements and its reliance on cloud services. The company’s founders want to ensure that adequate security controls are in place for the cloud layer of DiD.**

**A) Identify and briefly explain what the company should know about the physical security of the cloud data centers that it uses to host its clients’ websites and storage. Ideally, what physical security controls should be in place?**

**Part A Tips for Success:** This exercise provides a vehicle for demonstrating some of the things that you have learned about the DiD’s physical layer, cloud layer, and perimeter layers and how they apply to a case scenario. Section 11.6 and Table 11-9 are relevant to this part of the exercise.

**B) Identify and briefly describe the digital security controls that should be in place at the cloud layer of DiD to ensure that the company’s clients’ websites and storage are adequately protected.**

**Part B Tips for Success:** Section 11.7 and Table 11-10 are relevant to developing a response to this part of the exercise.

**C) The company’s founders have asked you whether remote access VPNs should be used for communicating with clients. Would you recommend them? Why or why not?**

**Part C Tips for Success**: The VPN Monitoring section of section 11.8 and Figure 11-16 are relevant to this part of the exercise, but you are encouraged to also review Chapter 8’s discussion of extranet VPNs.

Be sure that your address all Part A, Part B, and Part C questions/requirements. Proofread your responses to ensure that each is professionally formatted and free of spelling and grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with format specifications | 10 |
| Identifies what company should know about cloud data center security | 10 |
| Identifies physical security controls for cloud data centers | 10 |
| Identifies appropriate digital security controls for cloud services | 10 |
| Briefly describes each cloud security control | 20 |
| Includes VPN recommendation for client communications | 10 |
| Includes justification for VPN justification | 10 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |

**3)** **After taking a computer networking course at your university, you have grown more concerned about securing the Wi-Fi network in your residence. Review the section of Chapter 7 that focuses on Wi-Fi security and use it to identify potential threats and the security mechanisms that could or should be used to protect your Wi-Fi network from potential intruders/attackers. Consider how these security mechanisms could be arranged in layers (e.g., perimeter, internal network, endpoint/device) to deter attackers/intruders from reaching deeper layers.**

**Tips for Success**: This exercise provides an opportunity to revisit security issues and mechanisms for residential Wi-Fi networks within the context of DiD. In addition to discussion in Chapter 7, additional relevant information is included in the Chapter 7 appendices. Consider developing a table like the following to organize and summarize your work.

|  |  |  |
| --- | --- | --- |
| DiD Layer | Security Controls | Provided Deterrence |
| Physical |  |  |
| Perimeter |  |  |
| Internal Network |  |  |
| Endpoint |  |  |
| Application |  |  |
| Data |  |  |

Be sure to proofread your work to ensure that it is free of spelling and grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with format specifications | 10 |
| Identifies multiple potential security threats for residential Wi-Fi networks | 20 |
| Identifies multiple security controls for residential Wi-Fi networks | 20 |
| Identifies appropriate arrangement of security controls by DiD layers | 30 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |

**4) Authy (from Authy.com) is a free app for mobile devices, laptops, and desktops that provides two-factor authentication. Many popular websites use Authy to authenticate visitors. It is also being increasingly adopted by individuals to protect their personal devices and their online interactions with Internet sites. Do some online research on Authy and compose a brief report on how it works and how it can be used to protect businesses and individuals from security breaches. Summarize the results of your research in a 150- to 300-word report.**

**Tips for Success**: This exercise enables you to explore how multifactor authentication services work in greater detail. Strive to identify one or more substantive online articles that focus on Authy and MFA services and how they work. Consider including an image, diagram, or sketch in your report that illustrates how Authy works. Be sure that your report addresses how Authy can be used to protect businesses and also how it can be used by individuals. Be sure to proofread your report to ensure that it is professionally formatted and free of spelling and grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with length specifications | 5 |
| Includes explanation of how Authy works | 30 |
| Describes how Authy can be used to protect businesses | 20 |
| Describes how Authy can be used to protect individuals | 20 |
| Includes at least the specified minimum number of online sources | 5 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |

**5) CORE Credit Union has two branches in Statesboro, Georgia; two branches in Savannah, Georgia; and a branch in Brooklet, Georgia. It has 46 employees across these different locations and uses extensive electronic communication between its locations and to communicate with its members. The NCUA requires credit unions to document how data and applications are secured by cloud and other third-party organizations that provide them with services (e.g., online banking, bill pay, credit card transaction processing, remote deposit capture, ATMs, cloud storage, firewall monitoring, etc.). There is much that needs to be protected, and employees are the first line of defense. If you were responsible for overseeing security training for new employees, what topics would you include in their training? Develop a list of at least 10 required security topics that should be included in the training program and briefly describe why each topic is important.**

**Tips for Success**: This exercise enables you to apply your understanding of security policies and user training to a case scenario. Section 11.4, Table 11-7, and Figure 11-7 are relevant to this exercise. Consider summarizing your recommendations in a table like the following.

|  |  |
| --- | --- |
| Security Topic | Importance |
|  |  |

Be sure that you identify at least 10 security training tops and that you provide a brief explanation for why it should be included. Be sure that your table or description is professionally formatted and free of spelling and grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with length and format specifications | 10 |
| Identifies at least 10 relevant employee training topics | 20 |
| Provides a reasonable description for why each training topic is important | 50 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |

**6) Do some online research on Pretty Good Privacy (PGP). Develop a 300- to 500-word report on PGP, what it is used for, and how it works. Your report should also describe how/where you can acquire PGP tools, how you generate public-private key pairs, and how/where you can share your public key to enable others to send you encrypted messages that only you can decrypt.**

**Tips for Success**: This exercise enables you to develop a deeper understanding of public key encryption and PKI. The Asymmetric Encryption section of section 11.9.2 and Figure 11-21 are relevant to this exercise. Strive to identify one or more substantive online articles/sources that focus on PGP and address the issues required for your report. Be sure to address all required topics and be sure to proofread your report to ensure that it is professionally formatted and is free of spelling and grammatical errors.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Complies with format specifications | 10 |
| Identifies how PGP is used | 10 |
| Describes how PGP works | 20 |
| Describes how/where PGP tools can be acquired | 10 |
| Describes how public-private key pairs are generated | 20 |
| Identifies how/where public key can be shared | 10 |
| Submitted content is free of spelling errors and formatting and syntax shortcomings | 10 |
| Total | 100 |