**Chapter 4 Problems and Exercises Tips**

**1) Explain how (and why) an organization’s technology architecture is influenced by its business architecture, data/information architecture, and application architecture.**

**Tips for Success**: This problem/exercise promotes better insight into how/why an organization’s enterprise network should align with its business, data/information, and application needs/requirements. You are encouraged to revisit Section 1.3 in Chapter 1 which provides an overview of the different layers of EA and how they interrelate.

Ideally, your answer will note that the technologies and networks used by an organization should support its operations, core business requirements, and strategic initiatives. These should also facilitate the use of strategically and operationally relevant data/information and mission-critical applications.

You are encouraged to provide a response that is professionally formatted and include references in an appropriate reference format. A grading rubric like the following may be used by your instructor to evaluate your work.

|  |  |  |
| --- | --- | --- |
| **Criterion** | **Description** | **Points** |
| On time? | Is document/presentation submitted on or before its due date | 5 |
| Error Free? | Is submission free of spelling errors, formatting inconsistences, grammatical, and syntax shortcomings? | 5 |
| Business architecture influence | Does student explain how the organization’s technology architecture id influenced by its business architecture? | 30 |
| Data/information architecture influence | Does student explain how the organization’s technology architecture id influenced by its data/information architecture? | 30 |
| Application architecture influence | Does student explain how the organization’s technology architecture id influenced by its application architecture? | 30 |

**2) Wireshark is a widely used packet sniffing tool that is used to capture and analyze data traffic in TCP/IP networks. It can be downloaded from the Wireshark.org website (**[**https://www.wireshark.org/download.html**](https://www.wireshark.org/download.html)**) for installation on personal computers and laptops with Ethernet or Wi-Fi adapters.**

* **If you lack access to Wireshark in a campus lab, download and install the current version on your personal computer or laptop.**
* **Learn Wireshark basics, navigation, and uses from online or printed tutorials such as the following:**
  + **Sunny Dimalu the Cyborg. (2020). Wireshark Tutorial for Beginners (2022): From Absolute Basics | Packet Capture | Kali Linux [Video].** [**https://www.youtube.com/watch?v=DCqbOhWSFus**](https://www.youtube.com/watch?v=DCqbOhWSFus)
  + **Vinsloev Academy. (2020). Learn Wireshark in 10 minutes—Wireshark Tutorial for Beginners [Video].** [**https://www.youtube.com/watch?v=lb1Dw0elw0Q**](https://www.youtube.com/watch?v=lb1Dw0elw0Q)
  + **Viatto. (2019). How I Use Wireshark [Video].** [**https://www.youtube.com/watch?v=7CYpjf19GkA**](https://www.youtube.com/watch?v=7CYpjf19GkA)
  + **Orgera, S. (2020). How to Use Wireshark: A Complete Tutorial. Lifewire.** [**https://www.lifewire.com/wireshark-tutorial-4143298**](https://www.lifewire.com/wireshark-tutorial-4143298)
  + **Neasbitt, C. (n.d.). Wireshark Tutorial [Slideshow]. University of Georgia.** [**https://cobweb.cs.uga.edu/~perdisci/CSCIx250-F15/Slides/wireshark\_lecture.pdf**](https://cobweb.cs.uga.edu/~perdisci/CSCIx250-F15/Slides/wireshark_lecture.pdf)
* **Launch Wireshark and capture packets going through your network adapter for 20 to 30 seconds.**
* **Click Protocol ( ) to sort your captured packets alphabetically by protocol. (Note: Clicking Time will restore the packets to their original order.)**
* **List all the protocols included in your set of captured packets, associate each with its TCP/IP model layer, and identify protocols that were not mentioned in this chapter.**

**Tips for Success**: Wireshark enables you to observe firsthand the incoming and outgoing data traffic through your computer’s network adapter conforms and that the data traffic conforms to the layers of the TCP/IP model.

If you lack prior experience with Wireshark, the tutorials are helpful for learning Wireshark navigation basics and understanding what is included in packet capture display screens. It is not necessary for to complete all tutorials, but their contents vary, and some provide very good guidance for completing the activities for this exercise.

Your instructor may require you to submit screenshots or snips to document the exercise’s activities.

For the last activity, it can be useful to summarize your work in tabular form, such as the following:

|  |  |
| --- | --- |
| **TCP/IP Layer** | **Protocols in Capture List** |
| Application |  |
| Transport |  |
| Network |  |
| Data Link |  |

Most listed protocols in Wireshark display screens will be Application or Transport layer; Network and Data Link protocols are typically only revealed by exploding (clicking on the layers of) individual packets.

**3) Network diagrams are useful for visualizing network topologies and other networking concepts. Visio is a widely used tool for creating network diagrams. If you have access to Visio through your university, consult one or more online tutorials to learn how to use Visio to create network diagrams:**

* **Video: Create a Network Diagram (**[**https://support.microsoft.com/en-us/office/video-create-a-network-diagram-a2360cd9-5c9d-4839-b4f6-17b485e02262**](https://support.microsoft.com/en-us/office/video-create-a-network-diagram-a2360cd9-5c9d-4839-b4f6-17b485e02262)**)**
* **Use Visio or another network diagramming tool to recreate Figure 4-37.**

**A computer screen shot of a cloud with a circular object

Description automatically generated**

**Figure 4-37: Internet connections between two networks.**

**Tips for Success**: This is a relatively simple and straightforward introductory network diagramming assignment. Creating network diagrams promotes understanding of how network infrastructure is deployed. If you have never used Visio or another network diagramming tool (there are several good alternatives), you are encouraged to take advantage of available online tutorials such as the one identified for Visio.

Be sure to compare the diagram you create to Figure 4-37 to ensure that it is not missing any of the components and labels.

**4) Create a table in a Word document that looks like the following:**

|  |  |  |  |
| --- | --- | --- | --- |
| **TCP/IP Model Layer** | **Security Controls** | **Brief Descriptions** | **Recommendations & Reasons** |
| **Application** |  |  |  |
| **Transport** |  |  |  |
| **Network** |  |  |  |
| **Data Link** |  |  |  |
| **Physical** |  |  |  |

**In the Security Controls column, list at least three security mechanisms identified in this chapter for each layer. In the Brief Descriptions column, provide a two- to three-sentence description for each security control in your list. In the Recommendations & Reasons column, identify which security control at each layer you think is the most important to deploy and provide a two- to three-sentence reason for each of your recommended choices.**

**Tips for Success**: This problem/exercise provides an opportunity to get a better understanding of how security technologies introduced in Chapter 4 map to the different layers of the TCP/IP model. This is an aggregation exercise that enables you to take a closer look at security technologies introduced in the chapter.

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

|  |  |  |
| --- | --- | --- |
| **Criterion** | **Description** | **Points** |
| On time? | Is document/presentation submitted on or before its due date | 10 |
| Error Free? | Is submission free of spelling errors, formatting inconsistences, grammatical, and syntax shortcomings? | 10 |
| Business architecture influence | Does the student identify two layer-appropriate security controls for each TCP/IP layer? Ideally from among those identified in the chapter. | 20 |
| Data/information architecture influence | Does student provide a brief and accurate description of each security control at each layer? | 40 |
| Application architecture influence | Does student identify a most important security control for each layer and provide a two- or three-sentence reason for recommending it? | 30 |

**5) Zero-trust security initiatives require authentication for every user and every device every time to grant access to the network or a network resource. Do some online research on zero-trust security that enables you to clearly describe how it works and how users and devices are authenticated. Map what you learn about zero-trust security to the layers of the TCP/IP model. Summarize the results of your research in a 500- to 750-word report or a four- to six-slide presentation. Specify a minimum of two online sources in a references section using APA or MLA format.**

**Tips for Success**: This exercise **e**ncourages you to learn more about zero trust security, especially user and device authentication, and how zero trust aligns to the TCP/IP model. Strive to identify two or more substantive online articles related to the topic, ideally articles that describe ZTA (Zero Trust Architecture) within the context of the TCP/IP model. Strive to find articles that are more general and less technical in tone in content.

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

|  |  |  |
| --- | --- | --- |
| **Criterion** | **Description** | **Points** |
| On time? | Is document/presentation submitted on or before its due date? | 10 |
| Length | 500- to 750-words or four to six slides? | 5 |
| References | Are references included? | 5 |
| Reference format | Are references in MLA or APA format? | 5 |
| Error Free? | Is submission free of spelling errors, formatting inconsistences, grammatical, and syntax shortcomings? | 10 |
| Zero trust understanding | Does student demonstrate understanding of how zero trust works? | 25 |
| User and device authentication | Is it clear that student understands how users and devices are authenticated in zero trust? | 20 |
| Zero trust and TCP/IP model | Does student map zero-trust to the TCP/IP model? | 20 |