CPSC 4240/6240 Discovery 4 50 points Ashlyn Cooper

This homework is done in *individually*. You are allowed to use search engines, textbook/s, lecture notes, and any other sources you wish. But you are *not* allowed to copy paste from Internet, or help other teams with their work, either by giving them hints or solutions.

What and how to submit

Since this is an editable word document, you can make space between the questions and type your answers here. You can also make additions to the "map" at the end. Please do not type in red, but any other color is fine. I read everything you write, so I will not miss your answer ☺
Save as pdf and submit to Canvas.

Grading and Points

Every question indicates how many points it is worth. 4000-level and 6000-level are graded differently, with points indicated as (x/y), where x is 4240 and y is 6240.

Exercises

1. We have talked about storage devices. Please research Linux partitioning scheme. Which scheme is used? How many partitions are supported in that scheme? Explain what are primary, extended, and logical partitions are and how many can you have under that scheme? (10/10points)

   Linux gives the user several options for their partitioning scheme, but in general Linux uses a GPT scheme where the user can then define as many partitions as they want to best suit their needs. At a minimum, Linux operating systems need 1 partition for the OS itself. However, most of the time 2 primary partitions are sued with one being for the OS and one being for the swap area. The Linux partitioning scheme can support as many partitions as desired through the use of logical partitions.

   Primary partitions hold the OS and it holds the master boot code. There can only be 4 primary partitions on one disk. An extended partition is a special partition that contains "free space" where more than 4 primary partitions can be created. There can only be 1 extended partition on a system and if 4 primary partitions exist, you must delete one of the primary partitions to create an extended partition. Logical partitions are partitions created within an extended partition. There is no limit to the number of logical partitions allowed and they can be formatted with any filesystem.

2. System administrators are often tasked with selecting and even installing the proper video surveillance system for the organization. Please do an online research and find two candidate video security systems. The cost of the system should be no more than $600 USD. The motion activated system should have recording capabilities, night vision, and other useful features. It should be accessible for monitoring over the internet via a

phone or laptop. Ease of installation should also be considered. Justify why you are recommending your selected systems. Which one is the best of the two? (12/12).

- The first system is the Hiseeu 4K PoE Security Camera system. This system costs around $400 when not on sale. The system allows for motion detection as well as AI human and facial detection. The camera's AI can determine whether a human as be detected so as to limit false alarms that are triggered by animals. The camera system also has night vision and 1 TB of storage that is good for 30 days of recording. Without an internet connection, the system can be monitored locally on a screen plugged into the system, but with an internet connection, a live feed can be viewed from an PC or mobile device anywhere in the world. The system also has a 2-way audio feature, so not only can the users of the system hear what is being recorded by the cameras, but they can also speak or transmit recorded audio through the camera, so they can speak to whoever they see in the camera. Lastly, the system is easy to install. The system uses PoE or Power over Ethernet, so only one cable connection is needed for power, video, and audio transmission. They are also suitable for indoor and outdoor use.
- The next option is the Night Owl 4K 4-Cam Camera System. This system comes with 4 wired 4K cameras that can work indoors and outdoors. It also comes with a DVR that has a 1 TB hard drive for local storage. The system can also be easily expanded to 4 cameras. The cameras have night vision with a range of up to 100 feet as well as human detection to reduce false alerts. The cameras also have a motion activated spotlight. When connected to the internet, the camera feed can be viewed remotely. The system costs around $375 dollars. For installation, the cameras also come with all necessary cables.
- Both of these options offer good security capabilities for a very entry level price; however, I think the first system, the Hiseeu, is slightly better. This is mainly due to ease of installation. The HIseeu only needs one cord to be installed and connected to a network and the reviews for the Night Owl says that it is not quite as easy to install. I also think that the 2-way audio feature of the HIseeu is a nice addition and the Night Owl lacks audio entirely.

3. Design a security system for a small company. The map of the property is shown below. You have to address physical, operations security and equipment/OS security. (28/28)

A small privately owned company manufacturing custom computer components has just moved into a corner lot of a quiet residential neighborhood. The one-story building is about 2000 sq. feet. The land lot is 1 acre with trees on the two back sides. The building has three entrances. There is a small shed with valuable components in the corner of the lot. The company has 3 offices for employees and a freshly installed computer system with 3 laptops running Ubuntu Linux 20.04. They have hired you to design a security system that includes both the exterior and the interior physical security. You were also asked to secure the computer system that contains some intellectual property from possible cyber attacks. The owner also requested some security cameras, so they can monitor the area around the building at all times. Since the company is located in the residential neighborhood, the owner wants to blend-in with the surroundings and does not want to attract attention with barb-wire fences or ferocious guard dogs. Write a small

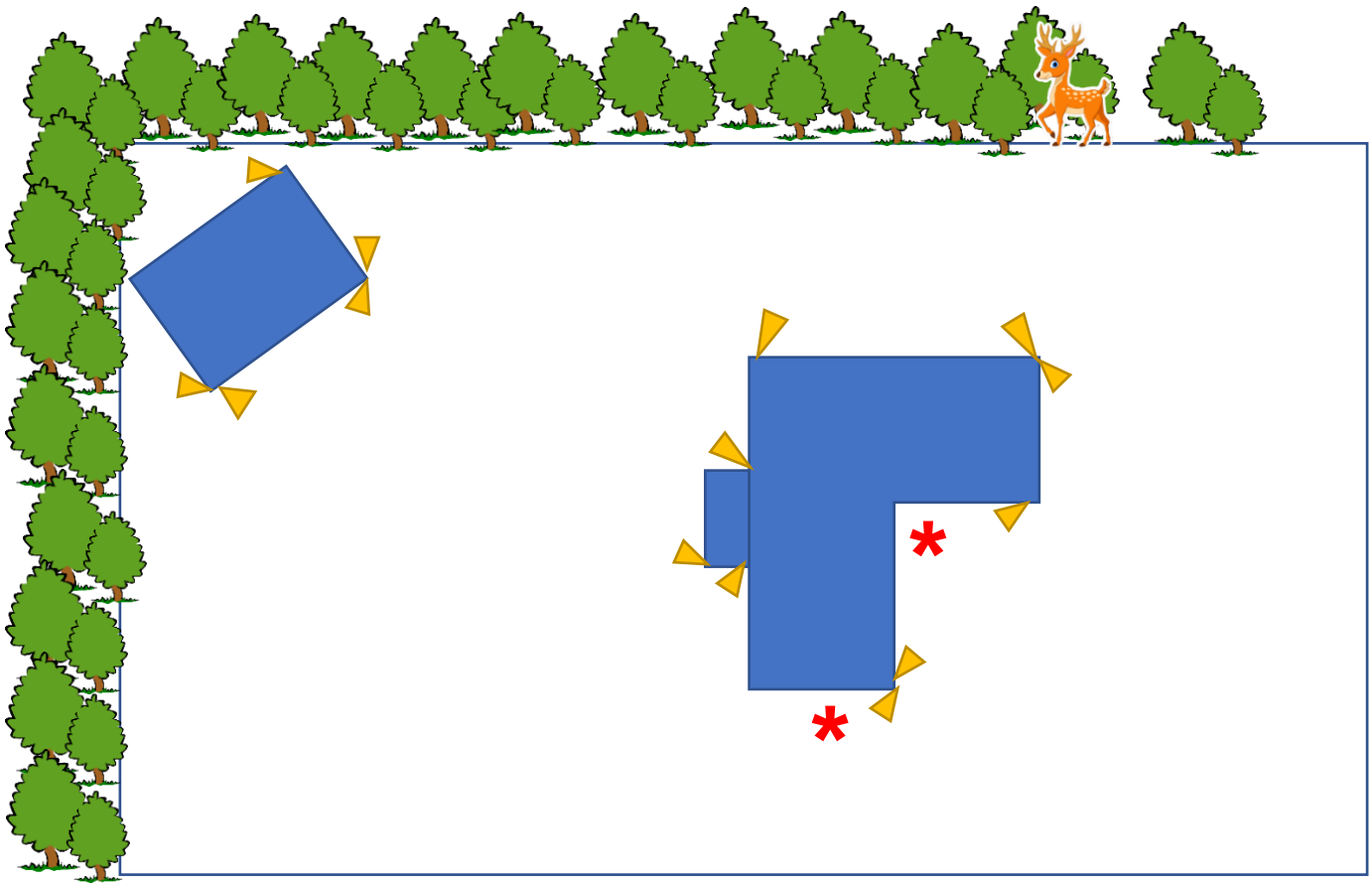
proposal for the owner where you will outline all the security mechanisms (from door locks and cameras to firewalls and IDS) that you recommend implementing. Be specific while recommending certain features. For example, recommend a specific firewall product, etc.

Proposal:

For the physical security, I would first make sure that there are locks on all entrances to the main building itself as well as locks on the entrance to the shed. These locks could either be normal deadbolts that are locked and unlocked with a physical key or digital combination locks in which a pin code must be entered, optimally each employee would have a unique pin code to enter so that who enters the building could be tracked. I would also make sure that any and all windows lock and that it is only management/ownership that has the access codes or keys to the buildings. Next, I would select the Hiseeu camera system described above to monitor the exteriors of the buildings. I would make sure there is at least one camera recording every entrance, with the camera locations and views marked by the yellow triangles on the map below.

For the interior of the building and laptops, I would make sure that only employees that need to use the laptops have access. The employees with access to the laptops would also have their own personal logins, so it can be easier to track who was using the laptops when. At the end of the day, management should then lock the laptops in one of the office room before leaving for the night. Also, for any digital connection to the company's servers, sites, or systems, I would recommend the use of a two-factor authentication program for added security.

For the company network and system, I would recommend two things, a firewall and an intrusion detection system. For a firewall product, I would recommend the Fortinet Security Fabric. The Fortinet is well respected in the industry and allows for easy scaling as the business grows. Also, the system is easy to manage as it takes place through a singular console and it can be managed through the cloud, so remote management is possible. The Fortinet also runs at an affordable price for a small business, starting at around $400 from Walmart. The Fortinet's Security Fabric package offers comprehensive endpoint device protection, a strong firewall, and improved security for individual devices. Lastly for an IDS, I would recommend Snort. Snort is an IDS that is compatible with the Linux laptops that is a network intrusion detection system or NIDS. Snort is highly rated and offers packet sniffing, packet logging, signature blocking, in depth reporting, real-time updates, and the ability to detect events like OS fingerprinting, buffer overflow attacks, and stealth port scans.



2-lane local road