Mark Moreno

Professor Karahan

CYSE 368

June 26, 2021

2nd Reflective Journal

Since my last journal entry, I have completed the Networking 1 learning project. This required a review of the OSI model, my refamiliarization of Cisco Packet Tracer and creating a network with a smaller number of IP addresses available so that none are wasted. I learned in this project about the CLI on Cisco devices so that I can configure a switch without using the GUI. I did get hung up for a second because I believed I needed to assign IP addresses not only to the switch, but to the ports on the switch. In the end I just configured the devices connecting to the switch with the specific IP addresses.

In the CLI portion, I learned that the configuration data including passwords for the management access is stored in plain text so that if someone were to access the configuration file, they could easily obtain the passwords to the switch. With commands like service password-encryption and enable secret it helps by either scrambling or encrypting the passwords. The obvious thing I see here is when you use the same passwords for multiple logins on the same device and scroll through the configuration file, it stands out that they are the same password. I also so the various connections available on the switch and how to secure them all with password protection. This includes the console and vty connections.

In my study of the OSI model and its comparison to the TCP/IP model I learned more about some items like Classful vs Classless subnetting. I was overthinking it but have come around to understand the difference. I have a good grasp on public vs private IPv4 addressing, I read a bit into IPv6 but what I saw online seemed to be generic and about the same information where I looked. The project had IPv6 as an extra credit item.

This was my first look at Cisco device hardening, it seems to be a best practices approach to lock down the device and protect from intrusion and misuse. There is a lot on the subject, and I covered the three planes a network device is categorized by, management plane, control plane, and data plane. This will be something I will have to investigate a lot more and have an opportunity here to learn more about should I decide to concentrate on networking in this job.

After completing the practical portion creating a subnet that had 16 IP addresses, 14 useable I answered a knowledge portion and had about four lookups. After a couple of days of review, I went back and had a follow-on conversation with my proctor. My first lookup included the difference between enable password and enable secret on the switch. The difference is one is stored in plain text, the other is encrypted using MD5. The second was how the TCP/IP model related to the OSI model, how they lined up with each other and the differences. Third was the specific make up and breakdown of a MAC address. I know how to identify one and I knew that a portion tells you who the manufacturer is, now I know specifically the breakdown and makeup. The last lookup was the broadcast domains which are broken up by routers and can be passed by a switch/bridge.

My follow-on project is Linux 1 which I had a day to review the project before we experienced the network issues in CS department. The project is on pause for the time being with most of my effort assisting the Runas and full times with task they need while they work to restore resources and services. We have switched to a new ticket system Zammad which I have become familiar with mainly through answering the reasonably expected backlog of tickets, one of my fellow consultants implemented it and has been very responsive to our issues in getting it to a smooth ticket experience for both root and the people we support. I have also been working on creating a Windows PXE boot image and imaging Ubuntu machines. The benefit of doing this to many machines is while the process is simple, the more computers we deal with, the various issues we run across, and I gain experience in solving those issues.