(1)

To start off my reflection, I was hesitant at first if I thought that applying into a Cybersecurity program was where I wanted my career to go. I was hesitant because computers have always been a large hobby of mine where I liked the physical aspect of building a pc and understanding all the components and how they worked together, but then also on the software side with gaming and coding. I was worried that if I started to study a technology related field that I might not enjoy it as a hobby as well. I was completely wrong about that, and I am very glad that I was admitted into this program because I have been enjoying the learning much more than my undergraduate degree. All the content that I have learned in Cyber 701, along with my other classes so far, have given me a better understanding of the cybersecurity field. I thought that I was knowledgeable about computer systems, but after seeing what else there is to learn I realized that I am just scratching the surface and I am excited to see what else I will learn in this program.

Throughout the material that we have covered in this course, I’ve learned that there are a lot of different parts of having a properly secured system that need to work together to provide the best protection possible. Even then, there is still a risk of an attack that has not been prepared for. One of my biggest takeaways from this class has been the importance of having an Incident Response Plan. If there is a plan in place, that helps tremendously in the event of an attack. It will help to reduce the severity of the attack and have a step by step basis for how to deal with the aftermath of the attack rather than the organization panicking leading to poor choices. As an everyday user I always thought that having a quality antivirus software, the occasional VPN usage, and avoiding sketchy websites would allow my personal system to be secure. However, after learning about the material in this course it made me think that even by doing those steps there is still a risk of downloading a malicious file or an intrusion being undetected. I had a general understanding of binary, but never really understood exactly how it worked and what it represented. After reading through the textbook unit on binary and doing the exercises, I felt like I understood what binary was and how it could be used as an ordinary user or as a cybersecurity professional. As a cybersecurity professional throughout the semester I learned that creating and maintaining an effective defense system requires the user to consistently update and adjust that security system. Not every attack/attacker will be the same, which means that the system’s defense needs to change and evolve as the attacks change and evolve. I now view my system as a very powerful machine that can be used for a multitude of different exercises in the cybersecurity field. We are able to simulate certain attacks on a system through the use of Virtual Machines to understand how the attacks work. By understanding how an attack works, we are able to formulate a much better defense for the system to prevent a similar attack. I think my view has changed as a cybersecurity professional of computer systems that they aren’t quite as secure as I had originally thought and that they have the potential to be very secure if the proper systems are put into place such as having a properly configured firewall and something like NIDS/HIDS. Many times the cost of suffering a data breach could outweigh the cost of properly defending your system, you need to be proactive in these cases not reactive.

(2)

One way that I really want to start learning about more topics in general is to start working on completing some self-guided projects. They are not only great ways to figure out what I know and what I can still learn, but also is a great way to demonstrate my skills to future employers. One topic that I found interesting and that I want to learn more about is Module 12: Denial of Service Attacks. DoS attacks can be detrimental to a company when their service can no longer be provided, it can cause a loss of money, reputation, and customers. I think that DoS attacks are interesting because there is not just one given way to cause a denial of service, there are different ways that exploit different vulnerabilities. Additional, attackers are always looking for new ways to execute these types of attacks. DoS attacks can also be much more malicious than just looking for a sum of money to restore a system, they can target systems such as healthcare systems which could potentially cause many people to suffer. These are some examples of why DoS attacks are important to know about so that they can be prevented against. I can learn more about specific attack methods by researching them or reading news articles from past attacks to figure out how they were executed and how they were fixed. Similarly, I think that to a degree some of the attacks could be simulated using a VM setup to see how the attack is executed and then test different defense techniques. This would provide a chance to learn not only how the attack takes place, but also what steps need to be taken to defend against attacks of that nature. I could also learn by watching free online tutorials which could provide background information as well as troubleshooting tips if a simulation exercise is not working properly. I think that one of the best ways to prevent against DoS attacks is to stay up to date on the types of attacks that are emerging and being successful against victims.

Another topic that we learned about in the course that I found interesting was Module 7 where we learned about writing simple assembly programs. Previously I had known what assembly language was and that was the extent of my knowledge. It was interesting to see how high level code such as Java could then be also written as an assembly program. I really enjoyed that the process of learning assembly language starts out very simple with a few different instructions, but then can build upon itself to accomplish more complex tasks when adding in the input and output functions. While I do realize most of my time will probably consist of writing programs in a higher level code such as Java, it is still vital to know that at a base level a program can be written as an assembly program. I also found the Bash shell script part of this module interesting because it was another simple way of creating a script that could also be used to accomplish complex tasks resulting in being able to make powerful scripts. I think that the best way to learn more about these two topics would be through online tutorials and videos. These videos would be able to provide the background information about the different functions that can be carried out and how to do so. I also think that with the shell scripting especially I would also be able to complete self-guided projects where I could experience firsthand the different tasks that can be carried out through Bash shell scripting. This could be done through an idea that I would have myself, or I could find project ideas online and then try to carry them out by figuring out the process on my own. This would provide valuable learning through the process of creating the script and then also troubleshooting it.

For my next steps in the program and my future career, I am aiming to continue taking the classes available to deepen my knowledge but also to learn about different topics in cybersecurity that I may not have previously known much about. Starting this next year, I plan on starting some self-guided projects so that I can have proof of my skills for when I start trying to form my career in the cybersecurity field. I think that these projects will not only deepen my understanding and abilities, but also help me to determine what career I want to pursue as a cybersecurity professional.

As for my experience with this course, I found that the textbook was an effective style of learning using the Zybook platform. I was able to learn about the content in the given module, then test that knowledge through the questions asked in each section to see if my understanding was correct or not. I also feel that I learned a lot and enjoyed our exercises each week from the Linux Basics for Hackers book. It provided hands on learning throughout the chapters, and then checked our learning at the end through the exercises. Overall, I have enjoyed my time in this class and I can’t wait to continue extending my learning in this program as I plan out my career as a cybersecurity professional.