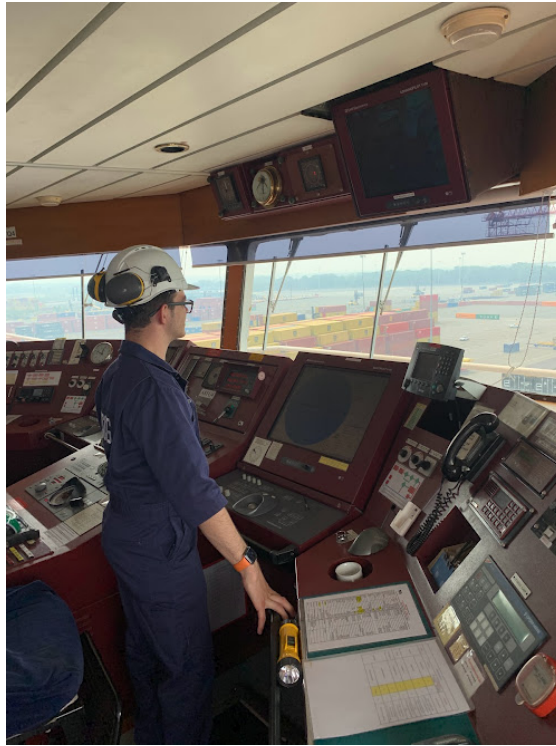Coutz's Final Briefing of USCG Sector New York

Name: Caden William Coutz

Hosting Site: United States Coast Guard Sector New York

Mentor: Mr. John Hillin, Mr. Brendan Dolan

One of the big components of my research this summer was gathering different information about cyber hygiene of ships. One of my mentors, Brendan Dolan was able to take the photo above as we were on a container ship. This information was being gathered to have a better understanding of how cyber security is conducted in the Maritime. The information was being used in order to develop a full scale cyber attack on USCG Sector New York and their area of responsibility. The facilities were the main target for the Cyber Security exercises, that is being conducted in October of 2023, but it is also important for the Coast Guard and the other ports in the harbor because a port can. Only be as safe as the vessel that is coming in. My research and findings lead to a real life modeled cyber attack scenario which is leading or has lead to a successful cyber security exercise. Essentially all of the USCG Sector New York is benefiting from this as well as the whole harbor of New York, all the way up to Albany, NY.

Coutz's Final Briefing of USCG Sector New York

Introduction

As an individual deeply committed to safeguarding my country, I have recognized a tremendous opportunity in utilizing my skills to protect national assets. In my dedicated efforts to contribute to the protection of our nation, one of my significant endeavors involved conducting extensive research on the cybersecurity vulnerabilities pertaining to the Harbor New York. This comprehensive study has enabled me to develop a highly sophisticated mock cyber attack, designed specifically for the Coast Guard of Sector New York, with the intention of facilitating an impactful Cyber Security Live Exercise scheduled for October 2023.

Driven by an unwavering passion for working with computers, I have come to understand that the safety of working on a computer is only as strong as the security measures that ar in place. Consequently, I have immersed myself in exploring the most effective mitigations to implement in order to fortify computer systems against potential threats. Additionally, I have dedicated considerable effort to gaining insights into the factors that render computers vulnerable to attacks.

The Research

During the first week of my internship I was brief by a couple different people on the their objective for a cyber security exercise. The exercise has been called "Operation Shuteye". They told me that I was going to be put in charge to create the mock cyber attacks for the exercise. As technology is evolving more and more of the Maritime industry is getting replaced or expanded with it. Technology has allowed industry to start replacing people having to patrol

and watch over grounds with CCTV Cameras. This now allows one person look over enough areas that may have taken.

With this all being said, Mr. Hillin wanted me to based the mock cyber attack around the CCTV cameras systems getting jammed or hacked, which leads the cameras to getting shut down. Along with this, I was also tasked with exploring other cyber vulnerabilities within the Port of NY, and target those, as well so that everyone can get multiple ideas on how their systems can be infiltrated.

A lot of the beginning of my research involved learning everything I could about CCTV Camera Systems. Prior to starting this internship I did not know anything about CCTV excepts for they are use for security. Various aspects of the research to trying to understands how and why the cameras can be venerable to hacking and how to mitigate it. This lead to a lot of other research on how to get access to the cameras. I had to understand how an attacker might work so I could better understand hoe to develop and build the attack scenario.

Along with doing research on the CCTV Cameras I also worked with by Cyber Specialist Brendan Dolan to create a cyber questionnaire to further understand how CCTV Systems are being used with in Sector NY AOR.

Contributions Made

As written above my main contribution this pas summer was building a highly sophisticated mock cyber attacks. This was the most important thing because they relied on it for a full scale cyber security exercise that they are conduction in October of 2023. Another part of the cyber exercise is that it is going to be one of the first of its kind. Meaning, once the exercise

has been performed and worked through, it is going to be used as a model for the rest of the United States Coast Guard to build off of and implement in other Sectors and districts.

With all of the research I am doing within cyber security, it piled up into a lot of different categories. Half way through my internship Mr. Hillin found a wind farm learning tool made by Stevens Institute. I took some time to build a small html website equivalent for cyber security. This is going to be a tool that can be given to anyone interested and will make learning about different aspects of cyber security more approachable rather than reading some boring document.

Coming into this internship with a little Banking IT Experience I was able to gain ideas of implementation of cyber security. One of my big projects last summer, 2022, I converted a bank of about 300 employees to a dual authentication login on all work stations. This gave me more insight on how secure a work station or computer can be. This allowed me insight needed to give feedback on possible insertions of cyber security checks into their vessel inspection routines. A lot of it was directed towards the bridge of the vessels. As someone whom has never looked or worked with these inspection manuals, I was able to look at them with a completely different perspective than what they had.

Within an exercise there is a few different handouts that people get. These handouts involve some different aspects of graphic design. I also was given the opportunity to work on some of the designs for the handouts. There was really no one sleaze working on them, so I was able to fully design a double sides placemat and the front and back cover of a short packet containing information having to do with the exercise. To the right is the front cover of the packet handout as a sample of the work I did.
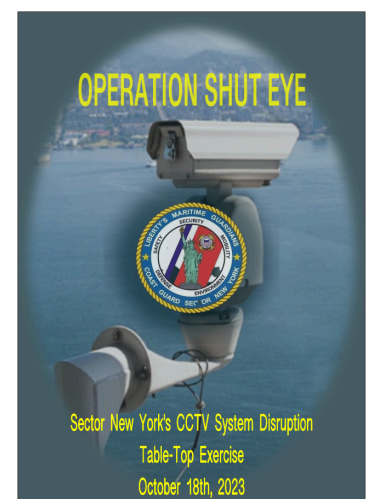
Skills and Knowledge Gained

As stated before I did not have really any understanding of how CCTV Camera Systems work and what attackers are capable of doing with them. I now have a better understanding of what needs to be done to ensure they are safe. Through the research of CCTV System hacks and vulnerabilities, I also gained more of an insight that even though commercial CCTV has more a of a value to hack, the amount of residential CCTV Cameras getting hacks is just has much as commercial is or can be.

Referring back to my IT Help desk at the bank last summer. I also got a experience in many ways dealing with software as well. The experience comes from installing, uninstalling, updating and doing other maintenance to software. From that work I gained a good understanding of how software is handled or works, but it was not until this years that all the knowledge of software got plugged into being understood within a cyber security understanding. I understand now why it is important to install software a specific way and why it is even more important to update software as soon as you can. Once a piece of software has been given an update there are no longer people looking at the outdated software, trying to find bugs and vulnerabilities they would make the software not as strong. This is the whole reason software updates and patches are released, and why it is very important to implement any updates or patches are given by reputable sources.

I learned a lot about cyber security mainly through legit application of what the Coast Guard does. In order to understand how cyber security procedures and policies are applied I got to go on a lot if different kinds of vessel exams. Before this internship, I heard of the Coast Guards, but I never knew what they actually did.

During my internship, USCG Sector New York was audited by a cyber security auditing team from the Department of Homeland Security. Mr. Hillin let me go with the cyber auditing teams for the three days they were here, and we basically shadowed Andre interviewed every department that Sector New York had. This helped to further my knowledge of what each p[art of a Coast Guard Sector unit, as well as how much cyber security relates to them.

Even by shadowing around the cyber auditing teams for only 3 days. I got a taste of other jobs involving cyber security. The field of cyber security is not only just about working to prevent or4 fix attacks. Rather there is a whole other side to it. Being able to have people, from an outside perspective, looking at the work you are doing can be very helpful. It is the same concept when Mr. Hill wanted me to look at the vessel inspection procedure. With a fresh perspective it is easier to give feedback on improvement.

This opportunity has also taught how valuable past skills and lessons learned can be. Going into the internship I thought that I was mainly going to be doing stuff that I have never done before. For a big portion of the time, this was the case, but there was also a lot of things I did and agreed to help with that would not have been as successful without the experience that I came in with.

As I was working through building the mock cyber-attack, some of the concepts I got and developed from working IT at the bank, made connecting some dots quicker and more efficient. Reading about some of the cyber vulnerabilities within reports made complete sense to me after I remembered what I did last years with. Also at the same time after understanding the vulnerabilities, I also have a further understanding of why what I did last year was and is still so important to the bank and companies in general. Once I was able to understand both sides of

vulnerabilities and the work of an IT help, the need to implement updates as soon as they are released became so much more important to me.

Research Experience Impact on My Academic and Career Planning

This internship has opened up a lot for me. Growing up one of my. Big dreams for work was being in the military. Being a person with a mild case of Cerebral Palsy, serving in the armed forces was not going to be a possibility for me, after talking with several different recruiters. Going into this internship, I did not know how many civilians actually also worked along side of active duty personnel. Through working this summer I got to talk to a lot of different people, all with different perspectives. I was able to learn and gain some very good advices as far as career paths within both the military for civilians, as well as career paths in the federal government, as well as a combination of both career paths intertwined that have worked out for others.

Along with this internship also brought a whole new perspective to living and transportation. As someone who has not tried to drive before and certain circumstances, driving and getting around my own, outside of walking, is a bit of a challenge. Living in Staten Island there is a lot more access to public transportation. After a couple of weeks I got pretty comfortable riding public transportation, so I did not have to worry about getting around. I learned that there is a lot of people who could drive but don't because they take public transportation. This will help to better understand where to move to when I move into my own place and what things to look for when finding a job.

- Not completely confident I wanted to do cyber security

- Also opene4d up interest in other parts

    - Hearing abbot other things they do container dashboard and data science

- Learned about master's education opportunities

-

-