CYSE 368

Term Fall 2022

Professor Thorbjorsen / C2 Management

Mario Villatoro-Molina

During my search for an internship or entry-level position, many places were asking for experiences in the field, your education in the IT world, certifications, clearances, and multiple skills that you need to know. For example, in skills, many places ask for experience in Office 365, VMware, group policies, coding languages, and many more. I have applied to multiple companies from ODU handshake since July 2022. Some places I have applied to still haven't received any notice of acceptance or declined the internship. So, I talked to Professor Thorbjorsen if she can help me with my internship course but she says “Continue applying to different internships and if I wasn’t able to find one she can help.” Professor Thorbjorsen also told me that if I can find a job that is related to my degree, I can use it for my internship while exampling my process of getting a certificate. There were three objectives that I want to achieve during my time on the internship. The first objective is to get experience for me to go up in my career, the second one is to know what certifications I should get soon, and lastly what knowledge I should expand or increase for future job offers.

I have also applied to entry-level jobs and some replied saying "We like your resume and education, but you don't fit the requirements that we are asking." Then I asked myself how a person with a degree in the IT world is supposed to get experience. I started researching what types of certificates I should get to help in my career. While I was researching several questions came to me. The questions were while I was studying for my associate’s degree and now my bachelor's degree, why have my professors over the year never told me that you have to get a certificate to get into an entry-level position? Most of the professors said "You can get this certificate at the end of this course, but you have to pay for the exam. The second question was how I will get experience in the IT field if entry-level jobs and even internships want students to already have two to three years of experience. so, I decided to research some entry-level certificates for students show to get. Certificates are highly respected by IT companies. They are the CompTIA Security + and GIAC Information Security Fundamentals (GISF).

When I finished researching there was one certificate that stood out and it was the CompTIA Security +. The exam cost was $352 on Professor Messer’s website, and the original price is $392 on the official CompTIA website. I bought my material to study from the website for $10 with a practice exam. When anyone is ready to take a test, they must get a voucher or pay for the exam on Pearson Vue and can find the local locations to take the exam in person or you can take it online with strict guidelines. When I began studying, I also learned that CompTIA Security + is the basic information for someone pursuing a cybersecurity career. Students can use information from the past course to help them understand the information more quickly and effectively. While studying I learn the CIA triad and the AAA of security in depth. During my time studying, I also applied to multiple internships without hearing anything in return and many other entry-level jobs gave me the response that they like my resume, but I haven’t reached the qualifications they are searching for. Expected one job from a small company that gave me a chance to start my career.

The company name is C2 Management and the job title I applied for is Secure IT Technician. During the interview process, I had an interview by phone with Jay Pastor from HR if I was still interested. Jay also asked me if I had experience in PCs, laptops, servers, and switches. He also asked if had any experience in refurbishing computers and laptops. Jay also asked about my experience in driving forklifts due to becoming a trainer and about the experience I gain that will help the company improve. I responded that I had experience in building a computer and refurbishing laptops. By building my computer and by getting experience in refurbishing in high school. I also told Jay about my experience in server admin and making sure vulnerabilities are patched and updated. Jay then told me when it is a date and time that is good for me for a second interview. The second interview was in person. While I was there, I couldn’t bring my phone inside the building due to security reasons. I had a walk through the Department of Secure and talk to Brooke who was using the command line on a switch. I had a chance in asking what type of technology she has run into and she replies that a lot of different or new technology comes inside the company. Such as phones, different types of switches or servers, etc. Brooke also told me that the company gets technology from a lot of government facilities and companies. She also told me that the department usually deletes data and resales the item but sometimes has to research to erase the data.

At the very end, Jay asks me if I was interested. I replied “Yes, I am very interested in the department and looking forward to improving the department. I had a last interview with the department manager Rhett, Rhett asked questions about my knowledge of basic computer repair, the command line for switches, and my willingness to adapt. I answered the question by using my knowledge in building my personal computer and using my knowledge in my four years of studying in college. Such as using the command lines on Windows and Linux, how to install OS, and updating patches so there will be no vulnerabilities. Eventually, I got a call saying that I got the job and I also told Professor Thorbjorsen. She told me that I can use the hours of the job towards the internship. On my first day of work on February 1, I had to fill out paperwork and talked about a lot of procedures all about servers, blade servers, how to dismantle a server, and pc/laptops. On my second day of work, I finish up my courses and then officially started my hands-on experience with Pcs then Rhett introduced me to the Aikens workshop. During orientation, some of the policies are very weird such as the hurricane policy, tornado policy, and the policy about Spotted Lanternflies. When Rhett was explaining how to use Aiken by plugging in an ethernet cable to the laptop or computer to boot up to Aiken. Rhett then told me that I must audit the Pc first and erase all the information from the previous company and make sure the computer has the right parts to start up the pc (rams and a CPU). We go to the bios to make sure the legacy boot is turned on and turn off the secure boot. Then we grade the pc and if I find a hard drive, we erase the date by using Aiken and scrap it. Rhett also made me an account for Aiken to save all the information that Aiken provides. Aiken gathers the model number, model name, ram size, processor, serial number, etc. All the information you need to list is on eBay but when we list something we list it as not containing data. Rhett also explains to me how to process a pallet in Listapp and make a pallet that goes to valley tech with its license for transport. When the pallet is completed I use the license a measure the weight of the pallet on the license.

The pallet that I was working on for the first day was all the same model and goes straight to valley tech. On my third day of work, I continued auditing Pcs, making sure it has the right parts to start up the pc, making sure it doesn't have any data storage, and grading the pc. If it had any data, we just erase it and destroy the hard drive, and depending on the previous company we can also sell the computer parts if permitted. Then we just grab the make, model, and serial number and save it on a sheet. I also need to check sometimes the type of processor the Pcs or laptops have because if it has a Core 2 or lower, we automatically scrap it. Scraping a Pc or laptop is when it is destroyed and can’t turn on. Then put it in a separate pallet and we also put the laptops or pcs on a separate pallet that is still functional. I completed my first pallet and had to weigh the pallet with functional pcs to send it outbound for another company named Valley Tech. Then my manager wants me to grab another pc pallet with a couple of laptops on the pallet. With laptops, I must do the exact way I did with the Pcs but every time we get a new pallet, we have to check every item if we can resell it on eBay. The pallet originally came from the government but for some reason, they drilled the motherboards of the laptops, so it was automatically scrapped. All the Pcs had no hard drives because they came from the government. On the weekend I keep on studying the different types of hackers and threats. The following week I kept getting the same old pc that goes to Valley Tech till Thursday, February 9 when I first started a whole pallet of servers. With the servers, if it contains hard drives, we have to use an application name Wipe Drive to erase the data and then audit the server with Aiken. After finishing auditing, I need to reboot to go to the bios to reset the idrac for Dell mostly due to having data on it and also reset the setting to default. I also needed to check if the servers’ cost anything so on February 13 it was my first time listing one server that cost more than $150 on eBay. But the rest goes to Valley Tech due to not costing much on eBay. During the weekend I started studying security threats such as malware for example. Most of the information I already know is due to the past course I took for my associate degree in cybersecurity. I also learned about mitigating threats which was also familiar to me. Eventually, I started to learn about the different types of hackers. Two hackers were completely new to me. Blue hats are hackers who attempt to hack into a network with the permission of the company but are not employed by the company. Elite hackers are who find and exploit vulnerabilities before anyone else does, which is a very rare hacker.

On February 14 I finished the server quickly due to not having any issues and due to not having to delete data because none of the servers have hard drives. Then my manager Rhett told me I can do any pallet I saw. Then I took advantage of the opportunity because I saw a pallet full of Apple iMac so Rhett to it down for me with a forklift. Rhett told for iMac we have to check the model number and check if boots. When I researched the model number on eBay it showed that it is a valuable asset to sell. I have a total of 24 iMacs to erase data from and reinstall an operating system. To delete that data from the iMacs I used Aiken to erase that by overwriting the data in 1s and 0s. After it was completely erased, I plugged in a USB that contained macOS Mojave. When the macOS installation wizard pops up I need to erase the data in the hard drive because it only contains 1s and 0s. After I agreed the agreement to install the operating system and waited for almost one hour. While I was the operating system to download I grabbed two other iMacs to overwrite the data on the hard drive. I continued that process till February 16 when I completed erasing the data contained on the iMacs and reinstalling the operating system. I had to see if the iMacs were remotely managed by going through the process of making an account and connecting the Wi-Fi. If a popup did not show saying that it has remote management on the system, then it is not remote manage. Then it was my first time cleaning up a computer to look good in the pictures. Plus, the company (Shenandoah University) that had the iMacs wrote numbers behind the iMacs. After cleaning up the iMacs I had to measure the height, length, and width of the iMacs for Listapp. I also gathered the weight and took pictures of the iMacs. Then the process of listing it on eBay was completed. On February 18 I started working on storage arrays that contain a lot of hard drives sadly and a couple of phones. For each storage array, I had to take out one hard drive and check if it can resell on eBay but luckily it was not worth reselling. During the next two, I continued studying for CompTIA Security +. The following that was interesting to me was advanced persistent threats that are Highly trained and funded groups of hackers often by nation-states with covert and open-source intelligence at their disposal. APT has the highest skill levels for all the threat actors. I also learn in-depth about threat intelligence and sources. For example confidence level, closed source, and extra. On February 20 I return to work to continue taking out the hard drive from the storage array and stacking up all the phones from the pallet. On February 21, I finished taking all the hard drives into the storage. After that, I check if the company wants us to erase the hard drive or just shred them. The original company want us to shred all their hard drives so at the end of the day I decided to shred them all after making a document with all the hard drives’ serial numbers.

On February 22, I started the process of disposing of multiple phones. Some of the phones were Blackberry, I also had some flip phones and iPhones. For the Blackberry and flip phones, I just need to take out the SIM cards and then grab their serial numbers to make and model to put in the scrap sheet. After that, I threw it in a bin full of scrap phones. For iPhones and smartphones made by Samsung, we must use an application named Phone Check. The application grabs their serial numbers, IMEI, model, and if the phone has been jailbroken. After that I factory reset the phone which takes up to 25 minutes. When it is done the application automatically down their app to test the phone. Then I must do one more factory reset so the phone can be thrown away in the scrap bin or to be sold on eBay. On February 23 I started on a new pallet which involved taking out hard drives with different Pcs, laptops, Apple products, etc. The company wants to get rid of some pallets that have been in the building for almost 8 months. Most of the pallets had no hard drives but I had to check it with another person. We also had to separate Chromebook that automatically goes to scrap and put them in the scrap pallet. We also separate computers and laptops that have core 2 or less because they automatically go to scrap as well. Computers that are not scrap go to a separate pallet to go to Valley Tech. Phones, apple products, valuable computers, valuable switches or servers, and laptops that have onboard hard drives such as the Surface Pro have to go to a separate pallet to go to the Secure department. C2 management was doing this fast process to make space and to get ready for my manager that will leave to pursue his career in FEMA. When I heard about it, I volunteered so I could help the department out and show the owner of the company that I am serious about learning everything in this department to help me advance in my career. I also asked Rhett if I could get his information to add him as a professional reference. Rhett agreed and I am still in touch with him till this day. I continue this process till March 1 for 8:30 hours. During the weekend on February 26, I studied for 4 hours for CompTIA Security+. I learned about threat hunting, which is a cyber security technique designed to detect the presence of threats that have not been discovered by normal security monitoring. I also learned about the kill chain model that was created by Lockheed Martin. I also heard about the MITRE ATT&CK framework which is a knowledge base maintained by the MITRE Corporation for listing and explaining specific adversary tactics, techniques, and common knowledge or procedures. I also learned about different types of malware which was a great refresher for me. I also had to learn about malware infections such as botnets and zombies. On March 1 I went back to the secure area after cleaning up the area where me and another person did the fast process from the last reflection. When I came back, I had to finish up some desktops and laptops that need to be finished so we can send them to Valley Tech. As usual, I had to use Aiken Workshop to audit the computer and make sure it is in working condition. I also had to check that the computer is valuable. Luckily all the desktops and laptops were not valuable so I can send it to Valley Tech. On March 3, the operations manager named Nick told everyone to stop what they are doing and focus on getting the make, model, and serial number to sell some pallets that are full of switches in GovDeals. GovDeals is a website that sells cheap IT types of equipment. Spend a couple of hours getting all the make, model, and serial numbers in the worksheet I had to send it to a co-worker named Brooke due to not having the credentials of putting materials in GovDeals. After getting the switch out of my way I proceed to the last computer and laptops to send it to Valley Tech. On March 4 I started studying for Security+ again and learned about something interesting. I learned about the topic of active interception and privilege escalation. Been discovered by normal security monitoring when a computer is positioned between the sender and receiver and can record or alter the traffic between them, this is known as active interception such as sniffing. Privilege escalation occurs when you can utilize a system's design defect or bug to access resources that a regular user isn't allowed to access. I also learned about backdoors and logic bombs again but the easter egg was a topic that was new to me. Easter egg is a non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature. An occurrence to the secure coding standards logic bombs and easter eggs should not be used. On March 6 I finished up the last couple of desktops that I had on my station and began to clean up my station due to having a lot of iPhones on this pallet. For iPhones, I need to factory reset the phones to make sure it is not iCloud lock or remote manage. During my procedure of erasing iPhones, I came to the problem of how to go to recovery mode due to having different types of models. Each iPhone model has a different layout and buttons to press to go to recovery mode. Multiple phones were an iCloud lock, so I just had to scrap them, and all the iPhones were not valuable to list on eBay. I continue with this process and checked if they had a sim card till March 8. On March 9 I started on a new pallet that was full of Apple laptops. I had to use Aiken Workshop to audit the laptop, erase the hard drive and make sure it is in working condition. But before I connected it to Aiken, I checked the back of the laptops due to some of the laptops being inflated. When I open the back, it shows that the battery is inflamed, and for that, I had to check all the batteries to see if they were inflamed. Almost half of the Apple laptops had inflamed batteries. What I had to do for the inflamed batteries was to take them out and tape up the connector just in case it causes a spark. After that we scrap it, but we take out the screen if it is in working condition. I also had some brand-new Apple laptops but the original company who had the laptop took out the motherboard and broke the screen, so I had to scrap it. I also notice that this particular company drilled some of their hard drives into the motherboard and screen. So, most of the laptops had to go to scrap due to the condition of the laptops. The laptops that are working 100% had their hard drive erased then I listed the laptops after cleaning them up, measuring them, and weighing the item. I did this procedure till March 14. On March 11 I study the steps of how to remove malware and how to prevent Malware. I also explore the different types of malware exploitation. On March 15 I start a new pallet full of HP and Apple laptops. First, a separated all the computers into different model numbers, then I started focusing on the HP laptops because most of them were inflamed. When I boot up most of the laptops it show that the CMOS battery was not functioning, so I decided to look up the error code and if the battery is inflamed. When I researched the error code it said that the main cause of the error is by the main battery not holding up or the bios needing an update. The function of Hp laptops is I process it through Aiken and erase the data. After that, I made a stack of all the good laptops to list on eBay. This process continued till March 17 and on March 20 started on the Apple laptops.

During the first couple of weeks, I was a lot of information about what I learned where companies do with the technology they don’t need anymore. I also learned how to erase data to make sure no information is leaked. Rhett explains the process of everything very well and very straightforwardly. That I just grab a pallet and complete it promptly. Some of my courses in ODU such as Linux and Windows course help me a lot by using the command line frequently for assignments. Also, one of the penetration courses from Lord Fairfax Community College helped me a lot to get past admin privileges from server computers that are worth a lot. Some things that were new to me was the amount ram sticks need to turn on a server. You only need 2 ram sticks in the slot of A1 and A2. If the server has two processors, then you can also add two more ram sticks to B! and B2 but it can still turn on with only two ram sticks. Something that I had learn during my almost three months is to get involved with switches. How to reset the admin or root password to erase all the data. I mostly have to research how to erase the data for all of the switches because they are not the same all the time. Especially the Cisco switches and the brocades switches. I also didn’t know that dell sometimes sell the chassis and parts to other companies to rebranded it to their company such as Netapp and Forecast. I was able to complete all my objectives for this internship. I was able to find the correct certification for me to continue on my path for my career and it was to study for my CompTIA Security +. Even though I failed my first try by missing a couple of questions I’m going to continue studying and grab some practice exams for Udemy that cost $20 dollars. I achieved on getting experience in multiple types of technology in C2 Management. I was able to completely refurbish a computer for a customer, manage a switch and install a printer by Wi-Fi. Lastly in what knowledge I show expand on for my career. I need to focus on different types of switches and there different types of command lines such as brocade and Cisco that none of past courses has prepare me. The only thing that past courses have helped me a lot was to use the command line and to be patience. I should get more use to group policies in a system to add users to new hires. I should as broaden my scope on how to manage licenses in switches and how to reset the ports on a switch.

References

<https://www.comptia.org/blog/what-are-the-best-cybersecurity-certifications>