Final Paper

Elijah Gartrell

Old Dominion University

CYSE 368 Summer 2024

Professor Duval

Cybersecurity Infrastructure Security Agency

Table of Content*s*

Pages:

Final Paper

This summer I've had the amazing opportunity to be a penetration testing intern with the Cybersecurity Infrastructure Security Agency(CISA). I am a Scholarship for Service(SFS) student as well and I joined CISA through their SFS pipeline. I wanted to work at CISA this summer because of the opportunity to work with the federal government before I start my service commitment as part of the scholarship agreement.This internship allowed me the opportunity to get the inside view of what it is truly like working for the federal government and has been a great learning experience.

Three main learning objectives that I wanted to focus on as I took this internship were : expanding my cyber knowledge, learning the ins and outs of federal government work, and what it actually meant to be a penetration tester. These were my main objectives for a multitude of reasons. Within this world of cyber you have to know the current landscape in order to succeed because of how fast the cybersecurity world is moving. Although the government is typically behind it would be great to actually see where they are within it as well. Old Dominion does not do the best job at keeping up with the current landscape so being able to learn it here will be amazing. Learning the ins and outs of federal government work helps me to understand what I am getting myself into before I start my first full time job with an agency after graduation next year. This internship will also help me to know whether CISA is the right agency for me or should I look elsewhere and see where else within the federal government would be the best for me to work in.

Before this internship I have not had any pen testing experience and truly wanted to see what the work was like. I believed that it was an over saturated market and that most people who want to get into cybersecurity choose those fields. So because of those reasons I shied away from this field mainly because I wanted to be different. So I focused my studies elsewhere and still got to do pen testing so I was absolutely excited to get to learn what that is like and for it to be at America's Cybersecurity Agency.

The Beginning of My Internship

The federal agency I am currently interning with is the newest federal agency in the government. CISA is a subset of the Department of Homeland Security(DHS) which was created back in 2018. CISA's mission is "We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." CISA has a multitude of different divisions and different focuses for each division.

There are divisions that handle infrastructure, emergency communications and even the national risk management division. CISA also handles the Common Exploited Vulnerability(CVE) along with MITRE and prides themselves with being America's Cybersecurity Agency. This CVE list helps everyone see different vulnerabilities, whether they've been patched and is poured into by everyone in industry. I believe it is amazing how CISA handles something so important to the world of cybersecurity. CISA is interesting because most of their work is public and they work with both federal agencies and private companies. The team I am on in CISA offers free penetration tests to state & local governments which is just one of their many features that CISA has. Protect2024 is one of CISAs main focuses this year within this big presidential election cycle. They want to strive for secure elections and ensure trust within the American people to know that they can go and vote in peace. Protect2024 is an amazing project that I hope I get to work on as my internship continues. There is much more that

CISA handles and DHS as a whole. My initial orientation mainly focused on the history of the DHS and how/why it was created. Then it followed with the creation of CISA and why CISA is needed within the federal government. We got to speak with the Deputy Chief of CISA and he talked about his path to the agency and what his plans were in his short term left with the agency since they are appointment-based from the administrations. We had security briefs and equipment set ups well within this time. All CISA employees interns and high GS levels go through the same long orientation which I thought was fairly interesting. Those were both within the first week and then following I had to do my division's orientation which is the Cybersecurity Division(CSD). This orientation was just covering CSDs mission and the point of CSD and how they work with the different offices within CISA and different subdivisions within CSD as well.

The subdivision I am in is Vulnerability Management(VM) and even though I will be almost 5 weeks within my internship I still have to complete VM orientation in August. Initial training was mainly HR based, sexual harassment training, workplace readiness, workplace fatigue etc. This was easy and tedious because there was so much training to complete and once you're starting you just really want to get into your work. The cyber training was all hosted on the platform HackTheBox academy. The HackTheBox training had two focuses on knowing computer systems all around a more technical path that focused on red teaming. I received my equipment fairly quickly so I did not get to do much HackTheBox and I was able to get right into my project.. My initial impressions of CISA in the first few weeks was not much since it was slow and I had no idea what I would be doing.

Management

The management structure and interaction within my internship have provided me with a diverse experience, particularly in terms of communication and hierarchy. Initially, I had regular check-ins with my supervisors every few days to discuss the progress of my project and any ongoing developments. This consistent interaction was crucial at the outset as it helped clarify expectations and provided a clear direction for my tasks. Over time, the management approach within my department has demonstrated a relaxed yet effective style, largely influenced by the high demands and busyness of the department. Despite this relaxed atmosphere, the entire team has been incredibly supportive and approachable, which has made the work environment very positive.

A notable aspect of the management style is the periodic update system I've established with my project coordinator. Each morning, I provide a detailed update addressing the following points:

- **What was accomplished yesterday?** This helps in tracking progress and understanding the outcomes of previous efforts.
- **What are you planning on working on today?** This sets clear expectations and ensures alignment with the project goals for the day.
- **Are there any blockers or issues you are having?** Identifying obstacles early on allows for timely intervention and problem resolution.
- **What do you need from me to succeed today?** This fosters a collaborative approach, ensuring I have the necessary support to achieve my objectives.

This structured communication has significantly enhanced the openness and effectiveness of our interactions. It ensures that everyone is on the same page and facilitates smoother workflow management. The hierarchical structure within the department, ranging from interns up to the

associate director, reflects a clear chain of command. However, due to the high volume of meetings that 90% of this hierarchy is involved in, direct contact with higher-ups can be infrequent. Nonetheless, when interaction does occur, the guidance and support received are highly valuable. The upcoming lunch with the chief of my department exemplifies the approachable nature of the management team and their willingness to foster relationships with interns.

Work Duties

In my role as a penetration testing intern, my primary responsibility revolves around the automation of virtual machine (VM) creation, specifically tailored for penetration tests. This task involves utilizing a set of Packer and Ansible scripts to streamline the deployment process of two distinct VMs. These scripts are designed to output an Open Virtual Appliance (OVA), encapsulating all necessary configurations for the machines. The automation process is executed through a series of commands:

1. packer init template.pkr.hcl
2. packer validate template.pkr.hcl
3. packer build template.pkr.hcl

By automating the creation of these VMs, my work significantly benefits the department during Risk and Vulnerability Assessments (RVAs). The automated process eliminates the need to manually build the VMs each time they are required for testing, thus saving valuable time and ensuring consistency. Instead, the scripts allow for quick deployment and readiness of the VMs with minimal manual intervention.

Additionally, I have the opportunity to observe RVAs, which provides valuable insight into the penetration testing process. Although my role does not typically involve active testing, I can execute commands under supervision, gaining practical experience and understanding of the testing environment. While my official title is PenTest Intern, much of my work focuses on scripting, which is a critical component of the role.

Looking ahead, I am preparing to take on a new project related to the President's Cup challenges. This Capture The Flag (CTF) competition, designed for federal employees, presents an exciting opportunity to further develop my skills. Engaging in this project will enhance my abilities in creating cybersecurity challenges, navigating complex systems, and managing hosting environments on servers. These experiences will contribute to a well-rounded skill set in cybersecurity, equipping me with both theoretical knowledge and practical expertise.

Prior Knowledge & Skills

Prior to embarking on this internship, my experience with penetration testing was limited to casual experimentation within my home lab and participation in Capture The Flag (CTF) competitions. While these activities provided a foundational understanding, they did not fully prepare me for the complexities of professional penetration testing. Navigating a Linux environment and engaging in theoretical exercises are only a small part of the broader skill set

required for effective penetration testing. The discipline itself is akin to an art form, requiring a deep understanding of various attack vectors and system vulnerabilities.

One of the most striking realizations from this internship has been the sheer expertise of the operators in problem-solving. In penetration testing, encountering attacks that do not succeed is a common scenario. Observing how seasoned professionals quickly pivot to alternative strategies and adeptly maneuver through an array of tools was enlightening. This ability to troubleshoot and adapt rapidly is a crucial skill in penetration testing, and it underscored the sophisticated nature of the work involved.

Before this internship, I considered problem-solving to be one of my strengths, but the level of problem-solving demonstrated by the operators here has elevated my understanding of what it means to think critically under pressure. Additionally, my familiarity with different types of scans, acquired through my prior experiences, offered some assistance during Risk and Vulnerability Assessments (RVAs). However, the real depth of penetration testing became apparent as I delved deeper into the practical aspects of the field.

One of the key areas of learning for me has been the use of GitHub tools that are essential for penetration testers. At one point, I had up to 20 GitHub repositories open simultaneously on my computer, each representing different tools and scripts used in penetration testing. The process of learning about these tools and understanding their applications was both challenging and rewarding. It provided me with a practical perspective on how these resources are utilized in real-world scenarios.

My experience has significantly reshaped my view of penetration testing. What I once saw as a set of discrete activities now appears as a complex, integrated field requiring a high level of skill and adaptability. This newfound appreciation extends to the broader field of cybersecurity, where the depth of expertise and dedication required is truly impressive.

In terms of my specific project, prior to this internship, I had no experience with tools like Packer or the automation of Virtual Machine (VM) creation. Learning to use Packer to automate VM setup has been an enjoyable and educational experience. The process of mastering these tools and applying them effectively has not only been fun but has also sparked a desire to continue exploring automation techniques independently. I plan to further develop my skills by experimenting with different VMs and automation strategies at home, building on the knowledge and experience gained through this internship. This ongoing learning process will undoubtedly enhance my proficiency in the field and contribute to my growth as a cybersecurity professional.

Did ODU Prepare me?

Unfortunately ODU's curriculum did not prepare me at all for this internship nor the things that I would be doing within this internship. ODU does not have much practical experience within the classes and the hands-on within the classes are dated. This is not to say our curriculum is bad and it helps you to learn plenty of the basics. But as far as what is actually going on in industry we do not learn it. Nothing of what we learned is something I did within my classes besides nmap scans. Metasploit is something great that we learned but we end up not actually using them within actual pentest.

Since I am taking higher level classes these next two semesters it would be interesting to see whether these actually help or not far as what is going on but ODU does give you a great understanding of the fundamentals. I think ODU would benefit from classes that are more on the current landscape of cybersecurity so students actually know what is going on within the world of cybersecurity because there are many of our students who do not know the current landscape of cybersecurity and who do not get the essential skills that employers are looking for currently. I do not think there are any classes within the cybersecurity or computer science departments that are teaching automation with Hashicorp Packer. I would love to see blue team courses at ODU as well since that is an area that is not taught at all.

Did I Meet My Objectives

I fully met one of my objectives and I slightly met the other two. The objective that was fully met was deepening my cybersecurity knowledge. I have been able to learn more about the current landscape of cybersecurity and the current threat landscape as well which has been super interesting. Going into this internship I knew a great amount of cybersecurity, just not much of the "nitty gritty" as people would say.

I have been very happy and grateful to have learned different attack vectors and paths that threat actors use. I've also learned more of what people in cybersecurity are actually looking for in new hires and what skills/knowledge that they prefer us to have. I have semi been able to understand federal work seeing as most of the federal employees I only somewhat know what they do. This is because we are often unable to speak with them as much as I'd prefer and it has been difficult connecting with alot of them since they work remote. My direct supervisor works in California so that has been a struggle trying to genuinely understand his job and what he does. For the majority of my department I do not know what their actual jobs are nor what they do.

Same with the penetration testing I have very little experience with and not being hands on with the assessments has been harder to learn the actual ins and outs of an assessment. It is one thing to sit over an operator's shoulder and shadow but it is completely different being able to look, process and think for yourself within an assessment. But I understand why we cannot do assessments as interns as well since they are very sensitive processes, but a crash course on certain orders of operations that they take would be amazing.

Motivators, Discourages, & Challenges

The biggest motivator within this internship was not knowing much and feeling behind the curve within this specific field of cybersecurity(pentesting) and wanting to actively learn and be better at what I am doing. This lit sort of a fire under me to learn more and be better within pentesting and have made me start to do more within my homelab based on what I have been learning at work. Being young was also motivating, knowing that the operators were several years older it made me feel better about everything. Initially I was worried because I thought the operators were closer in age to me opposed to what is actually the case. I was very confused when they would call me young and say I am in a great position because I wouldn't feel so. But I guess federal work keeps you looking young! There were some interns that understood different things that the operators were doing within the internship & RVAs and I didn't understand much and that was a big motivating factor as well. Knowing that there were students who were in similar age to me and at a certain level in cyber makes me want to learn more and develop more within the field, especially pentesting. I had to tell myself several times that it was only my first experience with pentesting and it should not end all be all.

The same last part that was motivating was also discouraging because I felt behind and I felt a bit of imposter syndrome along with it. But I learned and realized that everyone learns at

their own pace and I still know a great amount and worth a great amount as well. The most challenging part of this internship was probably getting people to talk and communicate with you. This was only challenging because of how busy everyone is but even the interns do not really communicate with each other. We each get our own project and go ahead and do our own work. Out of my department interns I have only had conversations with 3 of them, which is crazy to some people. You are thrown into the fire and told to figure it out so that was one of the hardest things, I initially got my project and had no idea what I was supposed to actually do with it until I asked more questions as to what I was supposed to be doing and the point and reason to doing what I was doing.

Recommendations

For future SFS scholars taking on an internship at CISA, there are several key strategies and insights that will better enhance your experience and success during the program. First and foremost, it is crucial to become comfortable with independent research and working autonomously. The ability to navigate and solve problems independently is a vital skill in the cybersecurity field. Often, you might find yourself needing to figure out solutions on your own, and being proactive rather than waiting for direct instructions will help somewhat.

One important aspect to be aware of is the sometime lack of immediate responses from internship coordinators. This is not uncommon in environments like CISA, where the workload is very heavy for the federal employees. So you should not be discouraged by delayed replies or the absence of direct guidance. Instead, be proactive. Take the initiative to seek out information, ask questions, and seek solutions independently. This self-reliance will be helpful, both in maximizing your learning and in demonstrating your commitment. Another piece of advice is to make the most of your time in the office. Actively speaking with your interns and supervisors by reaching out to colleagues and attending as many in-office events as possible. Unlike environments where management might seek out intern like my time at other internships, at CISA, it's often up to you to make those connections. Networking with the people around you, including those who might not be directly involved with your projects, can provide valuable insights and open doors to new opportunities. On my floor there is tons of different teams as well like threat hunting and it was great connecting with them.

Utilizing available training and resources is also crucial. CISA offers a wealth of educational materials and training sessions that can enhance your knowledge and skills. Even though the financial compensation is not much being a GS-4, the knowledge and skills you gain can be incredibly valuable. Attack your internship with the goal of enriching your expertise rather than focusing solely on financial gain. This mindset will help you fully appreciate the wealth of experience and learning opportunities available to you. Furthermore, actively seek out new projects and opportunities to broaden your skill set. The more proactive you are in exploring different aspects of the organization and its work, the more you will benefit from the experience. There is no guaranteed path to full-time employment at CISA, as job openings are subject to funding and organizational needs. Therefore, it's important to approach the internship with an open mind and a focus on learning rather than expecting a job offer at the end of your term.

Conclusion

The main takeaways I took from this internship would be that cybersecurity is truly such a big field and you're never going to fully know everything within it. It is truly astonishing how vast the cybersecurity world is because you could be in threat intelligence and never have to worry about reverse engineering, or work on IOT security and not have to worry about triaging. Knowing that the world of cybersecurity is fastly changing everyday, it is much better to be as well rounded as possible and not overwhelm yourself with trying to learn everything. Learning that not knowing everything was a big takeaway from this internship and I appreciate this internship for helping me with that . The best you can do is to continue to be a learner or pick your niche in cybersecurity and become really good at that. Because people who are really good at red teaming do not know much about other sides of cybersecurity, people who are talented in forensics are not the best cyber analysts because the scope of their jobs are so different. So learning to find a niche but also not confine yourself to it has also been a key takeaway. This internship will not affect the rest of my time at ODU much, it will make me more serious in making sure I am doing more home labs and additional learning on my own. There is nothing much that could happen at ODU for this to change. The most I can see changing is me helping out with our Cybersecurity Student Association(CS2A) and teaching the students within the club the new things I learned this summer. This will guide me within my future/professional path because depending on how the rest of the internship goes will determine whether I will work for CISA or another federal agency as I round out my last year of university. As an SFS scholar I can choose between federal agencies, state and local governments and FFRDCs. So this internship will be very important in what I will choose. So far I cannot say that I would choose to come back to CISA. There is a lot of reorganization going on within the divisions and for the majority of the employees I am still not 1000% sure of what their actual job is. Before I choose to land anywhere I want an honest review of what their work entails since I would be there very soon. In the next few weeks I hope that I am able to receive that knowledge and make a great decision on what to do. Overall I am very happy and grateful to CISA and all the employees there. I have grown and I have learned so much and I cannot wait to continue this internship.


CISA