Cybersecurity Internship Final Paper

E.J. Corpus

Research Security at Old Dominion University

Old Dominion University

CYSE 368: Cybersecurity Internship

Spring 2024

April 2nd, 2024

Table of Contents

Introduction

Undertaking a full-time job at Old Dominion University marked a pivotal moment in my journey toward professional growth and development within the cybersecurity domain. Motivated by the desire to apply the theoretical knowledge gained from my studies at Old Dominion University (ODU) to practical scenarios, I embarked on this job with clear objectives in mind. Primarily, I aimed to deepen my understanding of cybersecurity practices in a professional setting, enhance my technical skills, particularly in areas such as Linux administration and physical security management, and gain hands-on experience in implementing security measures within an organizational framework.

Reflecting on the experiences documented in the reflection papers, it becomes evident how each facet of this internship journey contributed to the attainment of these overarching objectives. From the initial days of orientation and training, where I familiarized myself with Old Dominion University's operations, culture, and management environment, to the culmination of projects such as the Linux Learning Project and the Containers Project, each phase presented unique opportunities for learning and growth. Moreover, the integration of theoretical concepts from ODU's curriculum with practical applications in the workplace highlights the relevance and effectiveness of academic preparation in real-world scenarios.

Throughout the internship, I experienced various challenges and encountered both motivating and discouraging aspects. However, each obstacle presented an opportunity for learning and development, reinforcing my determination to succeed and contribute meaningfully to the organization. As I navigated through tasks ranging from Linux server administration to physical security management, I witnessed firsthand the importance of cybersecurity in safeguarding organizational assets and maintaining operational resilience.

I intend to bring together the lessons learned from the reflection papers in this paper. I'll explain how what we learned in our studies connects with what we did in real-world situations. I'll also talk about what went well and what was difficult during the internship. Lastly, I'll give some advice for future interns who might be starting similar projects. Through this comprehensive reflection, I aim to express how the internship has deeply influenced my personal and professional development. I will explain how it has shaped my path toward a career in cybersecurity.

Internship Beginning

Old Dominion University, located in Norfolk, Virginia, stands as a distinguished institution renowned for its commitment to academic excellence, research innovation, and community engagement. Established in 1930 as the Norfolk Division of the College of William & Mary, ODU has since evolved into a comprehensive public research university, serving as a beacon of higher education in the Hampton Roads region and beyond.

Brief History of the Organization:

ODU's journey traces back to its humble beginnings as a two-year extension division offering evening classes to a small cohort of students in the heart of Norfolk. Over the decades, the

institution experienced exponential growth, expanding its academic offerings, campus infrastructure, and student body to meet the evolving needs of the community. In 1962, ODU gained independence as Old Dominion College and achieved university status in 1969, officially becoming Old Dominion University.

Major Products and/or Services:
As a comprehensive research university, ODU offers a diverse array of academic programs spanning undergraduate, graduate, and doctoral levels across various disciplines. From business and engineering to arts and humanities, ODU's curriculum reflects a commitment to interdisciplinary learning and academic excellence. Additionally, the university includes cutting-edge research facilities and centers of excellence, driving innovation and discovery in fields such as marine science, cybersecurity, and healthcare.

Major Customers or Demographics Targeted:
ODU's clientele encompasses a broad spectrum of individuals, including traditional college-aged students, adult learners, military personnel, and working professionals seeking to advance their education and career prospects. With a diverse student body from different backgrounds, cultures, and experiences, ODU fosters an inclusive and supportive learning environment conducive to personal and intellectual growth.

Initial Orientation and Training:
Upon joining Old Dominion University, I underwent a comprehensive orientation program to familiarize new employees with the company's operations, policies, and culture. The training sessions provided insights into the organization's mission, values, and expectations from employees. Additionally, I received specialized training in cybersecurity protocols, including data protection measures, network security fundamentals, and incident response procedures. My initial impressions of the company were positive, with a strong emphasis on employee development and a supportive work environment.

Management Environment:
Old Dominion University maintains a structured management environment, characterized by clear lines of supervision and effective communication channels. Each department is led by experienced managers who oversee daily operations and provide guidance to team members. The management structure fosters collaboration and innovation, allowing employees to contribute actively to the company's success. Throughout my internship, I found my supervisors to be approachable and supportive, offering valuable feedback and mentorship as I navigated through various tasks and projects.

Major Work Duties and Projects

Description of Tasks and Projects:
During my internship, I was assigned a diverse range of duties and projects, each contributing to the organization's cybersecurity initiatives and operational efficiency. One of the primary tasks assigned to me was the Linux Learning Project, aimed at enhancing my skills in Linux administration. This project involved configuring and managing Linux servers, troubleshooting system issues, and implementing security measures to safeguard against potential threats. After

completing the Linux Learning Project, I was tasked with a Containers project where I would utilize Podman to create rootless containers to fully understand how they operate. Additionally, I was responsible for managing physical security measures, including monitoring access logs, implementing door alerts, and operating the loaner laptop program.

Importance to Business:
Each of my internship duties and projects played a crucial role in supporting Old Dominion University's cybersecurity objectives and overall business operations. The Linux Learning Project, for instance, can help strengthen the organization's IT infrastructure by improving the efficiency and security of Linux-based systems. My involvement in physical security management ensured the safety and integrity of company assets, which led to mitigating risks and enhancing organizational resilience.

Use of Cybersecurity Skills

Prior Knowledge and Learning on the job:
Before starting the internship, I possessed foundational knowledge in cybersecurity acquired through coursework at Old Dominion University (ODU) and certifications that I have achieved. This included an understanding of basic security principles, network protocols, and risk management frameworks. However, the internship provided me with opportunities to apply this knowledge in a practical setting and acquire new skills tailored to industry requirements. In particular, I sharpened my expertise in Linux administration, building containers, and security compliance through hands-on experience and mentorship from senior colleagues.

Impact on Understanding:
The on-the-job experience gained during the internship significantly enhanced my understanding of cybersecurity practices and their real-world applications. By working on diverse projects and tackling complex challenges, I gained insights into industry best practices, emerging threats, and effective mitigation strategies. Moreover, exposure to practical scenarios helped bridge the gap between theoretical concepts learned in school and their implementation in professional settings. As a result, I developed a more comprehensive understanding of cybersecurity's role in safeguarding organizational assets and maintaining business continuity.

Connection with ODU Curriculum

Preparation from School:
The curriculum at ODU provided a solid foundation in cybersecurity principles, equipping me with the essential knowledge and skills required for the internship. Courses such as Network Security, Cyber Defense, and Cyber Strategy and Policy laid the groundwork for understanding key concepts related to threat detection, vulnerability management, and security controls. Additionally, practical lab exercises and projects offered hands-on experience in configuring firewalls and analyzing security incidents, preparing me for the challenges encountered during the internship.

Connections with School Learning:
Throughout the internship, I found several connections between my coursework at ODU and the skills utilized in the workplace. Concepts learned in classes, such as encryption techniques, firewall rules, and security policy frameworks, directly informed my approach to tasks and projects undertaken during the internship. For instance, knowledge of access control models helped me create firewall rules and implement effective security measures for controlling user access to sensitive systems and data. Likewise, familiarity with encryption algorithms facilitated the deployment of encryption protocols to secure communications and data storage within my projects.

New Concepts or Skills:
Despite the strong foundation provided by the ODU curriculum, the internship exposed me to new concepts, techniques, and skills not covered in academic settings. For example, hands-on experience with Linux administration deepened my understanding of server management, package deployment, and system hardening strategies beyond what was taught in coursework. Similarly, involvement in physical security management introduced me to surveillance systems, access control technologies, and regulatory compliance requirements, expanding my knowledge beyond traditional cybersecurity domains. Overall, the internship complimented my academic learning by exposing me to practical scenarios and industry-specific practices, enhancing my skill set and professional development.

Fulfillment of Internship Goals

Achievement of Objectives:
Reflecting on my internship experience, I am pleased to note that the objectives outlined at the beginning of the internship have been largely achieved. Firstly, the internship provided valuable insights into cybersecurity practices in a professional environment, allowing me to witness firsthand the implementation of security measures and protocols within an organization. Secondly, I successfully enhanced my technical skills, particularly in areas such as Linux administration, containers, and physical security management, through hands-on experience and mentorship from experienced professionals. Lastly, the internship afforded me opportunities to contribute to meaningful projects and tasks that directly supported Old Dominion University's cybersecurity objectives, which allowed me to gain practical experience and refine my expertise in cybersecurity.

Motivating or Exciting Aspects of the Internship:
One of the most motivating aspects of the internship was the opportunity to work on projects that directly contributed to the organization's cybersecurity objectives. Being entrusted with tasks such as the Linux Learning Project and the Containers Project provided a sense of purpose and accomplishment, as I could see the tangible impact of my efforts on enhancing the company's security posture. Additionally, the supportive and collaborative work environment created a sense of shared purpose among team members, creating an inspiring atmosphere helpful to innovation and professional growth. Moreover, the exposure to cutting-edge technologies and industry best practices ignited my passion for cybersecurity and fueled my desire to excel in the field.

Discouraging Aspects of the Internship:
Despite the many positive aspects of the internship, there were moments of frustration and obstacles, particularly when facing technical challenges or encountering setbacks in projects. Dealing with complex issues, such as troubleshooting system errors or resolving configuration issues, could be mentally difficult and demoralizing at times. Balancing multiple responsibilities and deadlines could lead to feelings of overwhelm and stress, especially when confronted with unexpected obstacles or competing priorities.

Challenging Aspects of the Internship:
The internship presented several notable challenges that tested my resilience, adaptability, and problem-solving skills. One of the primary challenges was the steep learning curve associated with mastering new technologies and tools, such as Linux administration and containerization. Overcoming this challenge required dedication, perseverance, and a willingness to seek guidance from mentors and colleagues. Additionally, managing time effectively to juggle multiple projects and tasks proved challenging, especially when faced with tight deadlines or unforeseen complexities. Communicating effectively with team members highlighted the importance of clear and concise communication skills in a professional context.

Recommendations for Future Interns:
For future interns in this internship, I recommend the following preparations to maximize their success and effectiveness:

Familiarize Yourself with Key Concepts:
- **Cybersecurity Fundamentals:** Understand basic principles of cybersecurity such as encryption, network security, threat detection, and incident response.
- **Linux Administration:** Gain familiarity with Linux operating systems, including common commands, file systems, user management, and basic system administration tasks.
- **Containerization:** Learn about containerization technologies like Docker and Podman, including container orchestration, networking, and security best practices.

Brush Up on Technical Skills:
- **Scripting Languages:** Enhance proficiency in scripting languages like Python, Bash, or PowerShell for automating tasks, analyzing data, and scripting security-related functions.
- **Command-Line Interfaces (CLI):** Practice navigating and using command-line interfaces efficiently for tasks such as system administration, network troubleshooting, and security operations.
- **Virtualization Technologies:** Familiarize yourself with virtualization concepts and tools such as VMware, VirtualBox, or KVM to understand virtual machine deployment, management, and security implications.

Develop Time Management Strategies:
- **Task Prioritization:** Learn to prioritize tasks based on importance and urgency to ensure critical objectives are met on time.
- **Setting Goals:** Set clear, achievable goals for each day or week, breaking down larger projects into manageable tasks to maintain progress and momentum.

- **Time Tracking:** Utilize tools or techniques to track time spent on different tasks, identifying areas for improvement and optimizing productivity.

Embrace a Growth Mindset:

- **Learning from Mistakes:** Embrace failures as learning opportunities, reflecting on mistakes to identify areas for improvement and growth.
- **Continuous Learning:** Stay curious and proactive about expanding your knowledge and skills, seeking out new challenges and opportunities for development.
- **Resilience:** Cultivate resilience in the face of setbacks, maintaining a positive attitude and perseverance to overcome obstacles and achieve goals.

Seek Mentorship and Guidance:

- **Networking:** Build relationships with experienced professionals in the field through networking events, online communities, or mentorship programs.
- **Asking Questions:** Do not hesitate to ask questions and seek advice from mentors, supervisors, or peers to gain insights and perspectives on complex issues or tasks.
- **Feedback Loop:** Actively grab feedback on your performance, seeking constructive criticism to identify areas of improvement and refine your skills.

Communicate Proactively:

- **Effective Communication:** Practice clear and concise communication in both written and verbal formats, ensuring messages are understood and expectations are aligned.
- **Reporting:** Develop skills in reporting incidents, vulnerabilities, or project updates effectively to stakeholders, emphasizing key findings and recommendations.
- **Collaboration:** Foster collaboration with team members by actively participating in discussions, sharing ideas, and contributing to team objectives.

Stay Flexible and Adaptable:

- **Agility:** Adapt to changing priorities, technologies, or project requirements with flexibility and agility, adjusting strategies and approaches as needed to achieve objectives.
- **Continuous Improvement:** Embrace a culture of continuous improvement, actively seeking opportunities to innovate, streamline processes, and enhance efficiency in cybersecurity practices.
- **Resilience:** Maintain resilience in the face of uncertainty or challenges, remaining adaptable and resourceful to overcome obstacles and drive progress forward.

Preparing to be an effective intern in cybersecurity involves enhancing technical skills, continuous learning, gaining hands-on experience, and understanding compliance standards. Interns should focus on mastering programming languages, network protocols, and cybersecurity tools while staying updated with industry trends and certifications. Practical experience through hands-on work or internships is crucial for developing problem-solving abilities. Additionally, fostering soft skills like communication and teamwork, along with adopting a proactive mindset to identify vulnerabilities and propose improvements, enables interns to make valuable contributions to cybersecurity initiatives within the organization.

Conclusion

Main Takeaway Thoughts from Internship Experience:

Reflecting on my internship experience at Old Dominion University, several key takeaways were important to my journey. Firstly, the internship reinforced the importance of practical experience in complementing academic learning, underscoring the value of hands-on application in bridging theoretical concepts with real-world scenarios. Secondly, the exposure to diverse projects and tasks deepened my understanding of cybersecurity practices and instilled a sense of confidence in tackling complex challenges within the field. Additionally, the supportive environment and mentorship received during the internship underscored the significance of collaboration and continuous learning in fostering professional growth. Overall, the internship served as a transformative experience, shaping my perspective, refining my skills, and preparing me for a future in cybersecurity.

Influence on Remainder of College Time at ODU:

The internship experience at Old Dominion University will undoubtedly influence the remainder of my college time at ODU in several profound ways. Firstly, it has enriched my academic journey by providing practical insights and real-world applications of cybersecurity principles, enhancing the relevance and applicability of coursework. Secondly, the skills and knowledge acquired during the internship will inform my approach to subsequent courses and projects, allowing me to leverage hands-on experience in classroom discussions and assignments. The internship has reinforced the importance of networking and seeking mentorship, encouraging me to actively engage with faculty, peers, and industry professionals to foster ongoing learning and professional development.

Influence on Future Professional Path or Planning:

Looking ahead, the internship experience at Old Dominion University will greatly influence my future professional path and planning within the cybersecurity domain. It has provided me with invaluable insights into various facets of cybersecurity, from network security and system administration to incident response and compliance management, broadening my skill set and enhancing my versatility within the field. The hands-on experience gained during the internship has equipped me with practical expertise and industry-specific knowledge that will be instrumental in pursuing career opportunities in cybersecurity. The relationships forged and lessons learned during the internship will guide my professional trajectory, shaping my priorities, aspirations, and commitment to continuous learning and growth. As I embark on the next phase of my career journey, I am confident that the internship experience has laid a solid foundation for success and positioned me to make meaningful contributions to the cybersecurity landscape.

References

Linux Learning Project
https://drive.google.com/file/d/1Kui4KCnbcmfygn9rKcnV6Mu72D5Qzo1k/view?usp=sharing

Containers Project
https://drive.google.com/file/d/1ktHsLGW1R30lp4CB352YPMqrhB4xsePD/view?usp=sharing