Old Dominion University

Internship Reflection Paper

National Security Agency

Kobe Coleman

CYSE 368

Summer 2024

Table of Contents

Introduction

My decision to intern with the National Security Agency was motivated by my interest in cybersecurity as well as the practical skills and information I gained during my academic studies. The government, with its essential role in national security and sensitive information protection, provides a unique opportunity for me to apply and enhance my cybersecurity skills. This opportunity completely coincides with my professional goals and personal ideals of preserving the public and national interests. Throughout my academic career, I have been immersed in a curriculum that focuses on both theoretical and practical aspects of cybersecurity, computer science, and information technology. Network security, cyber fundamentals, and introductory programming courses have given me a solid basis for understanding the complexity of cybersecurity and the need of protecting digital infrastructure. In addition, my participation in numerous school projects, hackathons, and cybersecurity competitions has refined my technical, analytical, and problem-solving abilities—all of which are necessary for a successful career in cybersecurity. Among the learning outcomes I aimed to attain were increased Linux proficiency, collaboration with workers in various job areas, and improved time management abilities. Linux proficiency is required for a cybersecurity expert because it is widely used in the business for server management, network security, and scripting. During my internship, I hope to broaden my knowledge and improve my technical skills by immersing myself in real-world Linux applications. Working in a diverse setting will also provide significant opportunity to collaborate with professionals from many disciplines, encouraging a multidisciplinary approach to problem solving and widening my perspective on how different jobs contribute to accomplishing common goals.

History of the Business and What the Organization Does

The mission the NSA provides is “The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) insights and cybersecurity products and services and enables computer network operations to gain a decisive advantage for the nation and our allies. Throughout the site, NSA/CSS will be referred to collectively as NSA.” (NSA.com) They also provide combat support “NSA is part of the U.S. Department of Defense serving as a combat support agency. Supporting our military service members around the world is one of the most important things that we do. NSA analysts, linguists, engineers and other personnel deploy to Afghanistan and other hostile areas to provide actionable SIGINT and cybersecurity support to warfighters on the front lines. We provide intelligence support to military operations through our signal’s intelligence activities, while our cybersecurity personnel, products and services ensure that military communications and data remain secure, and out of the hands of our adversaries. We provide wireless and wired secure communications to our warfighters and others in uniform no matter where they are, whether traveling through Afghanistan in a Humvee, diving beneath the sea, or flying into outer space. Our cybersecurity mission also produces and packages the codes that secure our nation's weapons systems. Additionally, we set common protocols and standards so that our military can securely share information with our allies, NATO and coalition forces around the world. Interoperability is a key to successful joint operations and exercises”

(NSA.com). My organization pen tests systems that are requested from various organizations in order to be compliant with the rules and standards set by the NSA. When you first start in this organization it is required to be familiar with Linux OS and Windows OS. You are then to read the rules and regulations that are required to be followed when conducting a Pen Test on a system. After this you are thrown into your first Test as a secondary tester and from then you are to learn how to do the job from scratch. This job is mostly for self-starters and people who are willing to learn outside of work to get the most from this opportunity. Setting up a meeting with the owner of the system to decide what we might test was the first step in this test. Pen testers are prevented from testing areas of the system that were not meant to be inspected by doing this. Before starting the hands-on part of the test, we first performed passive reconnaissance on the system to see what we might find and exploit. We used Nmap, or Network Mapper, to scan the system for the second part of the test. It is an open-source Linux command-line tool that finds installed apps and searches a network for IP addresses and ports. Network administrators can use Nmap to find out which devices are connected to their network, find open ports and services, and find vulnerabilities (FreeCodeCamp). Nessus Scans is another program that's frequently used in the field of cyber security and security testing for vulnerability scanning purposes. Tenable created the Nessus platform, which checks for security flaws in hardware, software, operating systems, cloud services, and other network resources (Geeks for Geeks).

The Managerial Culture

The managerial culture here is very amazing. My immediate supervisor stands out for his exceptional assistance and advice. They continually maintain an open and friendly environment and are always willing to answer any questions I may have, particularly about testing. Their willingness to share knowledge and provide clear explanations has been beneficial to my learning experience. This encouraging environment has not only improved my comprehension of the exam procedure, but it has also given me more confidence in tackling difficult assignments. Furthermore, the management team's collaborative and inclusive culture promotes a sense of belonging and continual improvement, making it a perfect environment for professional growth and development.

Work Duties and Projects

As a penetration tester, my primary responsibilities include conducting comprehensive security assessments to detect vulnerabilities in an organization's digital infrastructure. This procedure starts with intensive planning and reconnaissance, in which I collect information on the target systems, networks, and applications. Using this information, I plan and carry out a series of simulated cyberattacks, using a variety of tools and methodologies to assess the target environment's resistance. These tests involve exploiting flaws in online applications, network setups, and user credentials. Throughout the process, I painstakingly document my findings, including the nature of each vulnerability, the methods utilized to exploit it, and the possible impact on the company. After the testing phase, I create a detailed report that emphasizes the detected security weaknesses and provides practical solutions for. As a penetration tester, my primary responsibilities include conducting comprehensive security assessments to detect vulnerabilities in an organization's digital infrastructure. This procedure starts with intensive planning and reconnaissance, in which I collect information on the target systems, networks, and applications. Using this information, I plan and carry out a series of simulated cyberattacks, using a variety of tools and methodologies to assess the target environment's resistance. These tests involve exploiting flaws in online applications, network setups, and user credentials. Throughout the process, I painstakingly document my findings, including the nature of each vulnerability, the methods utilized to exploit it, and the possible impact on the company. Following the testing phase, I created a complete report outlining the detected security flaws and making practical recommendations to mitigate these risks. I frequently work with the organization's IT and security departments to explain my discoveries, demonstrate exploitation tactics, and help install the necessary security measures. Staying up to date on the newest cybersecurity trends, emerging threats, and new testing tools is also an important element of my position, as it allows me to effectively safeguard the firm from growing cyber threats.

I have finished three penetration tests successfully since beginning this internship. Every test is a drawn-out procedure that usually takes two weeks to finish. The length of time covers every phase of the evaluation, from preliminary planning and reconnaissance to carrying out the mock assaults and recording results. The schedule is meticulously planned so that, in the two weeks allocated, every component of the test is completed. This phase, which includes everything from information gathering and assault strategy development to result analysis and recommendation formulation, is crucial. Following this roadmap will let us produce comprehensive and useful information on the security posture of the company on time, while also preserving the efficacy and efficiency of the testing process.

Penetration testing is crucial for government systems because it proactively identifies and addresses vulnerabilities that could be exploited by malicious actors, potentially compromising sensitive national security information and critical infrastructure. Ensuring that governmental functions, such as military, intelligence, and public services, are safeguarded against cyber threats is of utmost importance due to the significant risks involved. Penetration tests mimic actual attacks to find vulnerabilities before attackers can take use of them, allowing for prompt patching and enhancing overall security posture. This preventive strategy guards against potentially disastrous breaches that could jeopardize public safety and national security, preserves operational continuity, and preserves public trust.

Skills Used and Acquired from Internship

I was able to improve my cybersecurity knowledge throughout my internship, especially with regard to Linux-based tools and commands. I knew a lot about Linux systems and fundamental cybersecurity concepts before I started the internship, but I didn't have much hands-on experience with particular tools. I concentrated on honing my abilities with commands and penetration testing tools, like Nmap and MSFconsole, during the internship. For example, Nmap made it possible for me to carry out thorough network scans in order to find open ports and services, which was essential for laying out the target environment. I was able to practice sophisticated exploitation techniques firsthand by simulating real-world attacks and exploiting vulnerabilities using MSFconsole, a component of the Metasploit Framework. One of the most important abilities in penetration testing is undoubtedly the ability to understand and analyze scan findings, which is something I greatly enhanced. Finding potential vulnerabilities that could otherwise go overlooked can be greatly aided by knowing what to look for in scan outputs. Because it requires differentiating between discoveries that are benign and those that could point to significant security issues, this ability is crucial. I now know how to carefully examine scan data, spot trends or abnormalities that point to vulnerabilities, and rank them according to possible effect. This improved capacity to evaluate scan results has improved my overall competence in identifying and resolving security concerns and has made me more skilled at locating important vulnerabilities that are essential for system security. During my internship, I also learned how to do open-source research, which proved to be quite helpful when looking for Common Vulnerabilities and Exposures (CVEs) and spotting potential security holes in out-of-date software. Using publicly accessible resources, such vulnerability databases, security forums, and documentation, to learn about known vulnerabilities and security issues is the expertise at hand. As an example, I used CVE databases and related repositories to find known vulnerabilities that might impact the target system when evaluating an earlier version of a software program. This procedure was helpful in locating possible security holes and gave important background information on how these flaws might be used in practical situations (Imperva).

How Old Dominion Prepared me for this Internship

My preparation for my penetration testing internship was greatly aided by Old Dominion University's (ODU) curriculum, especially with courses like CYSE 301—Cyber Techniques and Operations and CYSE 270—Linux for Cybersecurity. My work in the internship required me to have a strong foundation in Linux systems, which CYSE 270 offered. During the course, I gained actual expertise with Linux commands and administration, which I used to my internship by using programs like Nmap and MSFconsole. My familiarity with Linux environments and command-line interfaces helped me to operate these tools for penetration testing effectively. In a similar vein, CYSE 301 prepared me for my internship work by introducing me to fundamental cyber tactics and operational strategies. The cybersecurity best practices and approaches that were presented in this course were immediately applicable to the penetration testing procedures that I came across. For example, I was able to create and carry out successful simulated attacks as well as evaluate the findings of security assessments with the assistance of the knowledge I acquired from examining attack pathways and security measures in CYSE 301. Although the curriculum gave students a solid theoretical and practical foundation, the internship exposed them to novel ideas and sophisticated methods that were not fully covered in the classroom. I learned more in-depth information than what was covered in the curriculum, for instance, about the precise use of vulnerability scanning tools and the careful evaluation of scan results. In addition, the internship exposed me to practical situations and resources, like the utilization of sophisticated attack frameworks and open-source CVE research, which broadened my knowledge and skill set and enhanced what I had studied at ODU.

My internship with the government was greatly aided by Old Dominion University's (ODU) curriculum, which included essential courses like CYSE 250—Introduction to Programming—and CYSE 200T—Cybersecurity, Technology, and Society. A thorough grasp of the connection between cybersecurity, technology, and societal effects was given by CYSE 200T.

To understand the larger context of cybersecurity in a government setting, it was crucial to have an understanding of how technological improvements interact with security concerns and societal ramifications, which this course provided. My understanding of the value of securing sensitive data and the moral issues surrounding cybersecurity has grown because of the course, and it has been extremely helpful in navigating the challenges of working in a government setting. In a similar vein, CYSE 250 gave me the foundational programming abilities I needed for the internship. By learning to code, I was able to create custom scripts, examine software vulnerabilities, and automate several operations that are necessary for security assessments. The ability to program allowed for a deeper comprehension of the identification and resolution of technological problems, which was essential in advancing the security protocols and safeguards employed in government systems.

Fulfilling or Not Fulfilling my Learning outcomes

The internship made significant progress toward each of the objectives listed in my paper. I was able to achieve my goal of becoming more knowledgeable in Linux by using Linux systems extensively for a variety of jobs and tools. In addition to strengthening my theoretical understanding from CYSE 270—Linux for Cybersecurity—the practical experience with commands and tools like Nmap, MSFconsole, and dirb helped me to broaden and use these abilities in real-world situations, which improved my overall proficiency. In a similar vein, managing several projects with tight deadlines during the internship helped me accomplish my aim of improving my time management abilities. Managing the many penetration testing stages, from preparation and execution to documentation, improved my capacity for time management and work prioritization. Furthermore, the internship afforded numerous chances for collaboration with experts in various roles, such as cybersecurity analysts, IT specialists, and policy makers. My ability to communicate more effectively and comprehend how several departments work together to create a coherent security plan has increased as a result of this interdisciplinary engagement. My working experience was boosted by the collaborative environment, which also improved my capacity to function well in a variety of team settings. All in all, these encounters exceeded expectations and frequently exceeded the initial goals of the internship, greatly advancing my career and personal development.

Most Motivating Aspect of the Internship

The chance to continuously learn new things and put them to use via practical penetration testing experience was the most inspiring part of the internship. The dynamic landscape of cybersecurity, where new threats and vulnerabilities appear on a regular basis, has spurred my interest in keeping up with the newest methods and resources. Because there were new problems and learning opportunities every day, this drive for constant learning was energizing. The practical and engaging nature of the learning process was further enhanced by my direct engagement with real-world security concerns through the use of penetration testing tools and procedures. My enthusiasm for the topic was rekindled by the excitement of finding new vulnerabilities and seeing how they may be used against me. This gave me a sense of concrete success and a greater knowledge of the complexity of cybersecurity. The internship was very interesting and inspiring because of its unique combination of continuing education, real-world application, and the satisfaction of identifying and fixing security vulnerabilities.

Most Discouraging Aspect of the Internship

Long stretches of dullness during the internship, when the work felt monotonous and uninteresting, were among the most depressing aspects of the experience. These periods frequently required long hours of laboriously carrying out exhaustive scans or painstakingly evaluating data without seeing results right away, which might be quite taxing and discouraging. Furthermore, there were occasions when despite thorough testing and analysis, my attempts to locate vulnerabilities on a system produced no noteworthy results. It was discouraging to not find any new or exploitable vulnerabilities, especially after putting in a lot of time and effort. Since there was little visible progress, it was difficult to keep up motivation and enthusiasm because it occasionally seemed like the labor was not producing the desired results. Despite these depressing experiences, they served as a useful tool for instilling perseverance and resilience as well as highlighting the value of thoroughness and patience in cybersecurity work.

Most Challenging Aspect of the Internship

Keeping up with the quick growth of new exploits and vulnerabilities was one of the hardest parts of my internship. With new threats and exploits appearing often, the cybersecurity landscape is always changing and necessitates constant monitoring and response. It took a lot of time and energy to stay on top of these advancements since I had to constantly check security advisories, look for new vulnerabilities, and incorporate what I learned into my work. Another problem was making sure my technological abilities stayed up to date and useful. This required me to consistently practice and improve my current abilities in order to maintain proficiency, in addition to learning about new tools and techniques. It was difficult to manage both the short-term assignments and the long-term professional development while juggling these demands with the regular duties of the internship. These difficulties brought to light the dynamic and demanding nature of the cybersecurity industry and the necessity of continual learning and skill development in order to effectively address new security threats.

What I Recommend for Future Interns

Future interns should concentrate on a few essential areas in order to adequately prepare for a cybersecurity internship. First and foremost, it is imperative to finish pertinent courses like CYSE 200T—Cybersecurity, Technology, and Society, CYSE 250—Introduction to Programming, CYSE 270—Linux for Cybersecurity, and CYSE 301—Cyber Techniques and Operations," as these courses offer the fundamental knowledge and useful skills required for the position. Participating in Capture The Flag (CTF) events is another excellent way for interns to put their talents to use. CTFs imitate actual security scenarios and give participants a real-world setting in which to solve problems. Gaining expertise in open source research is also essential if you want to stay current on vulnerabilities and exploits. To do this, you must acquire the skills necessary to locate and evaluate data from sources such as CVE databases. Lastly, by building up a home lab or using virtual environments to obtain practical experience with penetration testing tools and procedures, interns may make sure they are familiar with the technologies they will use throughout their internship. The integration of academic preparation, real-world experience, and ongoing education will establish a strong basis for an effective and noteworthy internship.

Conclusion

In conclusion, my internship experience gave me priceless knowledge and useful skills that have profoundly changed the way I think about cybersecurity. The ability to use classroom knowledge in a professional setting, encounter real-world difficulties, and engage in hands-on work have enhanced my excitement for cybersecurity and increased my understanding of the industry. For the rest of my time at ODU, this experience will definitely have an impact on me because I will be approaching my coursework with a more focused and practical perspective and a desire to apply academic principles to real-world problems. In the future, my professional route will be guided by the skills and knowledge I have acquired, which will also inform my career plans and objectives. My career objectives have become clearer as a result of the practical experience, motivating me to pursue advanced cybersecurity responsibilities and never stop looking for chances to improve and specialize. In summary, the internship has enhanced my academic journey and established a clear path for my future profession, boosting my confidence and equipping me for the chances and difficulties that lie ahead.

Work Cited

“Cyse - Cybersecurity.” *CYSE - Cybersecurity &lt; Old Dominion University*, catalog.odu.edu/courses/cyse//. Accessed 29 July 2024.

“Explain Nessus Tool in Security Testing.” *GeeksforGeeks*, GeeksforGeeks, 11 Jan. 2024, www.geeksforgeeks.org/explain-nessus-tool-in-security-testing/.

“Home.” *National Security Agency Mission and Combat Support*, www.nsa.gov/About/Mission-Combat-Support/. Accessed 29 July 2024.

Shivanandhan, Manish. “What Is Nmap and How to Use It – a Tutorial for the Greatest Scanning Tool of All Time.” *freeCodeCamp.Org*, freeCodeCamp.org, 2 Oct. 2020, www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/.

“What Is CVE and CVSS: Vulnerability Scoring Explained: Imperva.” *Learning Center*, 21 Dec. 2023, www.imperva.com/learn/application-security/cve-cvss-vulnerability/#:~:text=CVE%20stands%20for%20Common%20Vulnerabilities,threat%20level%20of%20a%20vulnerability.