Reflection Essay

Cameron Waddy

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Andrews

June 21st, 2024

Introduction

As an Old Dominion University student, I am enrolled in the Bachelor of Science: cybersecurity program. Throughout my college career I have exposed to and accumulated a wide variety of skills. This ranges from the very fundamental principles of information technology to intricate concepts and disciplines of cybersecurity. Each of these information technology disciples further roll into more refined skills that I have continuously refined over the years. These skills range in variety, however there are three that are the core of my knowledge and supersede the rest. My top three skills are cloud security, networking, and programming which will be discussed throughout this essay. Furthermore, I will be referencing artifacts that are displayed on my electronic portfolio that work towards supporting my competency in these skills. These artifacts are composed of research essays, scenario-based reports, and lab projects.

My most prevalent skill is cloud security. It is also important to note that this skill is a compilation of many other important attributes. The main attribute is having a strong foundational knowledge in cybersecurity. There is a strong similarity between on-premises (on-prem) cybersecurity and cloud security, however the main differences lye within the responsibility, focus, and scope. Essentially, cloud offerings are hosted on public servers by companies such as AWS (Amazon Web Services) and Microsoft. Your on-premises offerings are more private as they are owned and maintained privately by companies or organizations. To put more light on this, the responsibility aspect for a cloud security environment relies mainly on the cloud service provider whereas on-prem cyber security relies on themselves for owning the servers. Of course, this can vary depending on how the environment is set up and any service agreements that are set. The next attribute, focus, refers to the main priority difference between cloud and on-prem security professionals. Cloud security's main focus is on securing any and all

cloud-based services and data. In contrast, on-prem security professionals have a more holistic approach to securing data and information systems whether for their customers or the organization itself. Finally, we reach the scope of responsibilities. Cloud security's main scope is within the cloud environment itself and it's limiting any exposure to the public internet. Cyber security has the main focus of protecting their data over the internet.

Cloud Security

Spyware Investigation

My first artifact is a research paper into the Pegasus Spyware. Being in the cloud security space, you need to understand any threats that could pose a risk to your environment. This includes how the software can be used against targets to then exploit companies and wreak havoc. The best approach to take is a very methodical one. You must understand the underlying foundations of malicious software and viruses and how they can be used to exploit systems. This can range from just data collection to taking control of the environment and holding it for ransom. Regardless of the purpose, this can cause huge financial and reputational losses to companies, and they must be safeguarded against. Next, you need to investigate how the malicious software works and what it aims to accomplish. It is very important to understand the full-scope of its capabilities as you may be able to protect one aspect of your environment while still leaving another part exposed to penetration. Finally, you need to create a comprehensive understanding of the hacking process that it takes to help your upper management or peers understand the capacity of the spyware. Then, it is important to identify your security gaps and cost of securing your environment so that you can properly protect the organization.

Information Assurance

One of the most core essential pieces of cloud security is information assurance. This next artifact is an investigative essay that addresses the responsibility of responding to a security incident. We were presented with being in the role of a chief information assurance officer who has to complete a investigative report into a security incident where the network was breached and sensitive information was collected by the instigating adversary. A cloud security analyst needs to be able to complete security incident reports to present to the environment stakeholders. Being able to logically report the intricate details of the incident in a language that is understandable to non-technical management is extremely important. This allows them to understand the full capacity of the attack while also ensuring they know the severity or lack-there-of. Additionally, proposing and proactively implementing security protocols or programs to help ensure incidents are not repeated is essential to help retain your position should there be any lack of confidence from management.

Cyber Technology

Having a baseline understanding of cybersecurity and the impact that it has on society is extremely important. All technology is connected and securing it is the responsibility of all individuals. This responsibility ranges from those who design the system to the user's and their password usage and storage. Understanding that malicious actors will exploit anyone to gain an advantage in leveraging your bank accounts or stealing your identity is the only way to help drive individuals protect their PII (personally identifiable information). In this artifact, I work to help bridge the gap in this regard. I further discuss the importance of being proactive in technological security and what can happen to you should a malicious actor gain access to your

PII. Additionally, I discuss the important of cyber technologies in corporations and the obligation that they have to themselves and their customers.

Artificial Intelligence

An extremely advanced technology known as artificial intelligence (AI) is becoming more and more prevalent in modern society. In this artifact, I dive into the implementation possibilities of artificial intelligence. The applicational purposes that I discuss can be used in positive influential ways. However, if implemented or cultivated incorrectly, this can lead to dire consequences such as how it is utilized in a military environment with drones. The implementation is important as you must weigh the benefits and costs of AI. One of the examples that I give within the artifact is that it can be used for agricultural purposes. This will without a doubt be a very expensive product that will only be available to large-scale farmers. This will allow these large farms to become more proficient and take markets away from smaller scaled farmers as they won't be able to afford or utilize the AI technology. Artificial intelligence as interdisciplinary from top to bottom which will require input from industry leaders across the market to develop it effectively and ethically. This project pushed me to explore many different disciplines to help properly discuss the pros and cons of AI.

Networking

Network Security Policy Review

The ability to review a security policy of an organization is a great skill in the course of an audit. Furthermore, it is important to be able to dissect a current policy to discover any gaps in security whether through networking or governance for insurance policies. Throughout this policy review, I discuss the oversight committees and their responsibilities for security implementations and network security policies. Having governing documents are extremely

important for insurance and customer review or regulations. Governing such a large organization, or university for this matter, is a very complex task to complete. Not only do you have to worry about personal devices connecting to university networks, but you also have students or professors connecting from all over the world. Additionally, ensuring the security of applications is essential as they contain PII and other private information. It is also important to ensure students understand their shared responsibility in protecting their login information to university owned sites or applications. Understanding how to review and comprise network security policies and how they govern an organization is a cornerstone of all cyber security professionals.

Digital Forensic Report

Every organization has s standard format in reporting incidents to ensure thorough documentation of events and data discovered. In this next artifact, I worked to complete an investigation that required web log analysis to complete a mobile device forensic investigation. Having a baseline understanding of networking is essential to every cyber professional. Additionally, the ability to analyze the web and network activities of a device or user is very important. This allows cyber professionals to find any malicious activity that is being conducted. While the investigation itself is very important, the tracking of such investigation is extremely important for audit and reporting purposes. This artifact works to demonstrate my capacity in both areas: investigation and reporting.

Zero Trust Strategy

Cyber strategies and policies are the cornerstone of governing documents and best practices in the security world. There are many different methods that organizations can take to secure their environments and users. However, specific strategies and policies have been

identified and documented for organizations to use as a baseline for integration with their systems. Understanding these are extremely important for those looking to break into the cyber security industry. You do not have to know every single word of these documents, although having some familiarity with the concepts is a good start to the journey. In relation to this artifact, I demonstrate the ability to break down the zero trust strategy and how you can work towards implementing it at your organization. This further demonstrates my capacity of understanding cyber security concepts that help guide companies towards a secure environment.

Programming & Scripting

Python Script

Having a baseline understanding of python is important in the world of cyber security as you are bound to interact with it at one point or another. This artifact is composed of a final project for a python script that I created. My goal of this project was to create a script that could be used by either cyber professionals or any day individuals who want to create more complex and safer passwords. After defining what the scope of the script was going to be, I started working on prototypes to allow user input and give responses based off certain criteria. Within the artifact, I describe the script and how it works and gives feedback based off of the user input. The feedback to be more specific would be a score out of 35. This 35 score would represent a very strong password that would provide them with the most security. The lower then number, the less secure the user's password would be. It also works to ensure that the user includes a variety of characters. These characters include upper and lowercase letters, numbers, and special characters such as a dollar sign or an exclamation point. This script helps demonstrate my capacity to write scripts and work towards creating a security solution that can be utilized by all.

Programming Project

This programming project was more than just contributing to a code base and walking away. During the summer of 2021, I returned for my second internship at a company called CloudFit Software. Over the course of this second internship, I had my first introduction to programming. The first programming language that I started to learn was "C#". As I came to find out, this was a very complex language that took a while to understand. But, through time and practice, I started to gain a firm understanding on how to read code proficiently and even begin to write code. Each individual journal represents a completed work during the internship in chronological order. It covers the project I contributed to with the internship team and any personal professions that I made. I not only learned how to write code, but also how to fix any bugs created throughout the coding process. This is also known as debugging. This is the process of fixing any inadvertent issues that are caused by conflicting or incorrect code. This task could vary between taking a few hours to a few days to solve. At the end of the day, debugging taught me the most important virtues of all: patience and persistence. This was my most pivotal point in my early career as it defined my work ethic and commitment to learning and growing.

Conclusion

Cyber security is an extremely interdisciplinary profession as it takes so many skills and areas to become proficient. For example, the skills that I have highlighted are a compilation of other skills that have had to be cultivated. Cloud security involves the understanding of networking, infrastructure, scripting, and more to make a secure environment. Within this congregation of skills, networking itself takes a multitude of skills such as investigations, networking layers, and internet protocols (IP) addressing. Additionally, with programming and scripting, there are so many languages that can be learned that can be further used to do so many

different things. There are certain programming languages that are better for backend services, while there are other languages that are better for user interface services. Furthermore, scripting helps automate processes and these processes can be every changing when more criteria are moved to being included. This has moved me to be very open minded in new concepts and methodologies. Cyber security is ever evolving in terms of technology and threats which means you have to constantly evolve your skills to protect against threats.

Interdisciplinary courses such as IDS 300W have taught me to expand my thinking beyond the binary solutions in front of me. By thinking deeper on areas of study, you can open layers of skills or attributes that you may not have had on the surface. I was then able to see underlying similarities between different tasks or assignments with would lead me to solutions easer with a deeper understanding of said task. By working to continue evolving with technologies and becoming a jack-of-all trades, I will be able to quickly identify gaps in security and implement solutions to these gaps. I will also be able to quickly work to solve engineering tasks as I can find relations between different products and integrating them together to further create more secure environments or solutions. Reflecting on all of these artifacts that I have completed over the course of my college years has really opened my eyes to how far that I have come. I constantly am looking forward to focus on the next obstacle and the next task that I must tackle in life. However, looking back has shown me all the struggles and projects that I have overcome. This has made me very proud of myself and to take pride in my college journey.