Joey Whitmore
IDS 493
Reflective Paper

Introduction

During my time at Old Dominion University (ODU) I have learned many hard and soft skills. Some of the most important skills that I have learned have come from ym hardest courses including Cyber Strategy and Policy, Network System Security, and Cyber Techniques and Operations. The hard skills I have learned include: Wireshark Packet Analysis,Python Coding,Red Teaming in Cybersecurity,Blue Team Rules in Cybersecurity,Cyber Security Capture the Flag (CTF). There has been many ups and dows with this program that was heavily attributed to my learning process during the course. There has been key lessons learned that made me appreciate the IDS program at ODU. The IDS program showed me how I need to use skills from multiple disciplines to solve complex problems and keeping this in mind I had to gain a certain amount of skills to do so.

Technical Skills

Wireshark is a powerful network protocol analyzer used to capture and inspect data packets traversing the network. When I learned this tool it equipped me with the ability to monitor and troubleshoot network traffic, identify vulnerabilities, and detect potential intrusions. By examining the packets in detail, the ability to uncover patterns of malicious activity, debugging network configurations, and ensuring data is transmitted securely. These skills are extremely critical for cybersecurity professionals and help maintain robust network defenses. I also learned python coding for cybersecurity and it is widely used for automating tasks, developing scripts, and analyzing data. When I was learning python it helped me know the creation of custom security tools, parsing log files, and helped conduct penetration testing.The libraries and frameworks that python has Scapy and Pycrypto, are particularly these are valuable for tasks like packet crafting and cryptographic analysis. Python’s simplicity and power make it the best scripting language in the cybersecurity field. I learned more red teaming techniques at ODU as well. This skill helps develop an understanding of offensive security strategies, including exploiting vulnerabilities, bypassing defenses, and testing an organization's incident response. Through red teaming exercises, I gained more insight on how attackers think and operate, which is crucial for designing better defense mechanisms. On the contrary I learned more blue team rules as well. Blue teaming focuses on the defensive side of cybersecurity, emphasizing the implementation of security measures, monitoring for threats, and responding to incidents. Learning these blue team techniques includes setting up intrusion detection systems(IDS), creating firewall rules, and managing security information and event management systems(SIEM) tools. Blue team skills are essential for maintaining continuous protection against evolving threats and ensuring system resilience. The final hard skill that was extremely valuable

to me is cybersecurity capture the flag techniques. These competitions are called CTFs and they are gamified challenges that test my problem solving and technical abilities in various aspects of cybersecurity. These exercises involve tasks like reverse engineering, cryptography, web exploitation, and forensics. Engaging in CTFs sharpens practical skills, promotes creative thinking, and provides me with hands-on experience in tackling real-world cybersecurity scenarios. This showed me how to apply theoretical knowledge in a competitive and collaborative environment. Each of these fruitful skills integrates technical expertise with problem solving and critical thinking, reflecting the interdisciplinary nature of cybersecurity. They blend concepts from computer science, network engineering, and information security to build a comprehensive skill set. These hard skills are also complementary to the various soft skills that I have gained over the years at ODU.

Interpersonal skills

The soft skills I have developed include: communication skills, critical thinking and problem solving, team collaboration, and continuous learning and curiosity. Communication skills are crucial in cybersecurity, whether I am explaining technical concepts to a non technical stakeholder or documenting incidents, being able to clearly communicate is important for cybersecurity professionals.This includes both verbal and written communication as well as the ability to make messages to diverse audiences, such as executives, team members, or clients. In cybersecurity, oftentimes I will be working in a team and this means that not only effective communication will be imperative to being a successful cybersecurity professional but having a successful collaboration strategy. When working with IT departments,management, and external vendors collaboration is important to foster effective teamwork, ensure smooth incident response, and facilitate alignment between different organizational goals and security practices. The cybersecurity field evolves constantly and being in the classes that make mention of the advances of cybersecurity make sure they harp on the advancements being made day by day. A mindset of continuous learning and curiosity ensures professionals stay updated on new threats, tools, and technologies. This includes seeking out training, certifications, and opportunities for professional development.

Three Lessons

My understanding of the Interdisciplinary Studies (IDS) program at ODU is showing the relationship between what most would say are unrelated disciplines and using them to solve complex problems. Using multiple disciplines to solve problems allows a holistic approach to problem solving and shows different niches in your field. For example, cybersecurity has a close relationship to the criminal justice field in many forms such as, having to have a documented report and liaising with law enforcement to proceed with a penetration test. Seeing the IDS

Joey Whitmore
IDS 493
Reflective Paper

program in ODU allowed me to learn how to discipline myself to learn things from other sources than cybersecurity professionals because everyone holds a unique perspective. The interdisciplinary studies program at ODU encouraged me to step outside the confines of traditional cybersecurity training and explore knowledge from various fields like psychology,sociology,business,and even philosophy. By delving in these disciplines, I learned that every individual regardless of their area of expertise can contribute to valuable insights into complex problems. Psychology offers various insights into human behavior which can be useful in understanding social engineering tactics or designing user friendly security protocols. Sociology can help me grasp the societal impact of cyber security policies or analyze trends in cybercrime. Business studies could even enhance my ability to communicate cyber security risks in terms of executive understanding and aligning security strategies with organizational goals. Another lesson that interdisciplinary studies has taught me is how to seek knowledge independently and go beyond just formal instruction or mentorship from cybersecurity professionals. I actively explored different viewpoints and resources to help me develop the habit of self-discipline. So that means that I'm not just waiting for guidance, but taking initiative to learn for myself.I did this by researching emerging threats and technologies from tech blogs and academic journals, even online forums. I incorporated lessons from unrelated fields into cyber security challenges to build connections across industries to understand the broader context of what cybersecurity is to me.I held this lesson along with the previous one to recognize that everyone holds a unique perspective that could foster collaboration and creative thinking.A legal expert might provide insight into compliance requirements, while marketing professional could highlight the risks associated with customer data breaches. By embracing this diversity, I gained a holistic approach to cybersecurity, understanding not just how systems fail, but why organizations and people interact the way they do.this mindset strengthened my ability to adapt innovate and communicate effectively and gave me a blueprint to focus on key skills for tackling multifaceted challenges of cyber security and real world scenarios.Interdisciplinary studies also helped me learn leadership and initiative skills to help me learn more effectively and made me realize how valuable these skills are for managing security teams ; driving strategic initiatives and influencing organizations and cultures around cybersecurity.This initiative shows a proactive approach to identifying potential risks and proposing solutions and continuously improving defenses. With these leadership and initiative skills I've gained from the interdisciplinary study program and overarching theme that I learned is knowing when to step back as a leader ,and let somebody else take the bull by the horn so to speak. Knowing when to step back is so valuable because you gain so much knowledge when you sit back and listen and take information from different sources to have a holistic approach when trying to evaluate cybersecurity problems. The artifacts that I have chosen for my eportfolio go in tandem with cyber security because not only is that my major but a passion of mine. Some artifacts I have chosen include: penetration test write up I made, python script, and a linux grouping and users assignment. I will choose the Linux grouping and Users assignment as an artifact because it shows my understanding of the different operating systems and Linux is a prominent operating system when working in the

discipline of cyber security. I will be using a python script as another one of my artifacts because not only is python a relatively easy and simple programming language to learn but it is prominent in the cybersecurity realm. I will be using the penetration test write up to show how my major (cybersecurity) and my minor (criminal justice) relate in the real world. Some of my challenges that I have gotten with my artifacts include the lack of knowledge with a given subject to be general. Looking at my python script artifact the lack of knowledge is there but the challenge was understanding the syntax because I came from a Java background and everything is done manually by the user except loading the memory in sequences. The simplistic format of python made me overcomplicate my scripts and made them less efficient than they could have been in the beginning. The main challenge with the python script write up was the understanding of laws that are put in place during a penetration test on an organization's network.

Conclusion

The IDS program in so many words humbled and grounded me in a sense of reality. Showing me that you do not have to be the smartest person in the room or the most technically sound person in the room to make an active contribution to the task at hand. They programmed me to be disciplined and take in advice from others so I can include different perspectives when problem solving. I took these perspectives and ran with them to start learning more on my own which is another lesson the IDS program taught me. The way that the IDS program restructured my mind to use other disciplines to solve complex problems is an invaluable experience I will carry with myself for the rest of my life. The skills that I learned were not just learned from my classes but took insights from other disciplines to solve problems and have a holistic view of a problem rather than being stuck thinking about a problem from a technical perspective. An excellent example of this would be end user training and awareness in the cybersecurity field. Knowing the knowledge and putting it on a sheet of paper would be useful for some learners depending on their learning style. Taking from an adult educational discipline we would deduce the learning styles to show the training in multiple ways rather than regurgitating the information on a piece of paper. Taking in these lessons and perspectives allows me to attack the real world with the upmost confidence knowing that ODU has prepared me for not just my field of work but how to effectively communicate with people with different perspectives to come to an astute resolution when problems arise in the workplace.