Reflective Essay

Samuel Baidoo

Old Dominion University

Abstract

This reflective essay explores the development of key skills and competencies achieved through creating an electronic portfolio during the IDS 493 course, emphasizing three pivotal areas: analytical thinking, technical skills, and writing/research experience. By engaging in targeted assignments, readings, and projects, I have honed my technical capabilities, advanced my critical thinking, and refined my ability to synthesize and present complex information.

In the realm of technical skills, my work in the Cyber Techniques and Operations (CYSE 301) course involved configuring and utilizing Snort on a virtual machine running Ubuntu to monitor network activity and detect potential threats. This hands-on experience enabled me to deepen my understanding of intrusion detection systems, develop custom detection rules, and analyze traffic to effectively mitigate cybersecurity risks.

Critical thinking was cultivated further through the IDS program and my philosophical exploration in PHIL 355E, where I examined SCADA systems and their vulnerabilities. This analysis underscored the ethical and technical challenges associated with protecting critical infrastructure, offering insights into the importance of modernizing these systems to prevent catastrophic societal consequences.

Finally, my research and writing skills were enhanced through a detailed study of cyberwarfare, SCADA systems, and the Colonial Pipeline attack of 2019. This work required an in-depth investigation of the interplay between cybersecurity vulnerabilities and real-world impacts, showcasing my ability to evaluate data critically and present well-structured, evidence-based arguments. Together, these experiences reflect my ongoing development and readiness to excel as a cybersecurity specialist.

Technical Skills

When it comes to a class that I had, Cyber Techniques and Operations (CYSE 301), there was an assignment where I had to apply my knowledge of cybersecurity in a practical setting using a virtual machine running the Ubuntu operating system. The focus of the assignment was on utilizing Snort, a powerful open-source intrusion detection and prevention system, to monitor and analyze network activity. I began by setting up Snort, which required configuring the environment, including network interface settings and establishing directories for log storage.

Once Snort was operational, I delved into writing custom detection rules tailored to specific types of network traffic and potential threats, such as scanning for unauthorized access attempts or detecting specific types of malware signatures. The process involved understanding the rule syntax, using appropriate actions (such as alert, log, or drop), and specifying parameters like IP addresses, ports, and protocols.

After deploying these rules, I tested them by generating simulated network traffic to see how Snort responded. The next step involved analyzing the alerts generated by Snort in response to this traffic. This analysis required interpreting log files and using tools like Wireshark to cross-reference and validate the detected activities. Through this assignment, I gained a deeper understanding of how intrusion detection systems operate, the importance of precise rule-writing, and how to respond to potential security incidents effectively.

Reflective Essay

Critical thinking

When it came to developing my critical thinking skills, the IDS program played a significant role in deepening my understanding of cybersecurity threats and enhancing my analytical approach to addressing them. By engaging with real-world scenarios and dissecting complex network activities, I was able to strengthen my ability to identify vulnerabilities and assess potential risks effectively. Additionally, in the class PHIL 355E, I further honed these skills by writing a comprehensive paper on SCADA systems, focusing on their inherent dangers to society. This paper examined the critical role SCADA systems play in managing essential infrastructure, such as power grids and water supply, and highlighted the severe consequences of vulnerabilities in these systems. The combination of technical training from the IDS program and philosophical analysis in PHIL 355E helped me critically evaluate both the technical and ethical implications of protecting critical infrastructure in an increasingly digital world.

In my analysis, I emphasized the urgent need for modernizing SCADA systems by incorporating advanced cybersecurity measures, such as intrusion detection systems, segmentation of networks, and regular security audits. Additionally, fostering collaboration between policymakers, engineers, and cybersecurity professionals is critical to developing comprehensive strategies to protect these systems. Without proactive measures, the vulnerabilities of SCADA systems could lead to devastating societal and economic consequences, highlighting their importance as a focal point in cybersecurity defense.

Reflective Essay

Writing skills/ Research

To demonstrate my growth in writing skills and research capabilities, I conducted an in-depth research article focusing on cyberwarfare, SCADA systems, and the 2019 Colonial Pipeline attack. This project required a critical examination of how SCADA systems, integral to managing critical infrastructure, have become a focal point for cyber adversaries due to their vulnerabilities. My research delved into the technical aspects of SCADA systems, the growing prevalence of ransomware attacks, and the Colonial Pipeline incident as a case study. Through comprehensive analysis, I explored the methods employed by attackers, the cascading effects of such attacks on society and the economy, and the lessons learned from this breach. The process honed my ability to synthesize complex technical information and present it in a clear, structured manner. Additionally, it reinforced the importance of robust research methodologies, including sourcing reliable references and critically evaluating data to support my arguments. This experience not only enhanced my writing proficiency but also deepened my understanding of cybersecurity's critical role in safeguarding national infrastructure.

Reflective Essay