Reflective Essay

Jasprit Kaur

School of Cybersecurity

IDS 493: Electronic Portfolio Project

Professor Phan

May 1, 2026

Throughout my academic career at ODU, I have developed numerous talents and skills related to cybersecurity and technology. With the fostering environment provided by the university, I was allowed to explore these new arenas and concepts without fear of failure or hesitation. Using this e-portfolio, I want to reflect upon the many projects and assignments that have helped me develop these skills. By curating a select few artifacts, I plan to discuss the importance of each one and the process that was involved in order to create it. Finally, I want to discuss the outcomes of each artifact, as they steadily built on each other as my degree progressed. In totality, I want to discuss these three skillsets: Linux operation, ethical hacking procedures, and interpersonal skills.

Linux Operation

The first artifact that I'd like to discuss is an assignment from my CYSE 270 course, or Linux for Cybersecurity. This course was my first introduction to the Linux operating system; it was quite jarring. I'd only ever interacted with MacOS/Windows prior to taking this course, and believed that it would be quite difficult for me to catch on. Unexpectedly, I found myself enjoying interacting with different Linux distributions, and I also gained valuable insight into Virtual Machine management. Although this artifact isn't the first assignment that we completed for the course, it was a culmination of weeks of learning. We'd taken weeks of basic Linux commands and compiled them in order to complete the listed tasks. We were tasked with creating new user accounts, changing their passwords, and adjusting the directory owner. From there, we were tasked with changing the permissions associated with a directory and file permissions for each user. By doing this, we could see account management in action and how administrators can utilize Linux commands to change the reading/editing permissions for different users as they pertain to certain resources in a system. Also, we were able to deploy root

privileges whilst working on this assignment, highlighting how important they are. This was a good assignment to work on, as it was the culmination of weeks of learning and experimenting with a new OS.

The second artifact that I want to highlight was one where we were tasked with disk partitioning and hard disk management of our virtual machines. This assignment was certainly more challenging than the previous one, and it took place in the latter half of the semester. Here we were tasked with examining the current partition table and creating a new primary partition on the virtual machine's hard disk. Once the new partition was created, we had to mount the new partition under a new directory, which was particularly difficult in my memory. To complete the assignment, we had to unmount our newly created directory. This artifact was one of the more difficult ones to complete, but it was worth it nonetheless. Storage management of virtual machines is critical in an environment where multiple VMs run at once. This was a good introductory rundown of the process.

Finally, to conclude my discussion of CYSE 270, I want to highlight the final artifact in this collection. This assignment was completed towards the tail end of the semester and incorporated a large portion of the class. At this point, we were comfortable with a range of Linux commands and were tasked with performing ping scans, DNS queries, and adjusting the VM's hardware components. This was a proper culmination of the semester and the course, as it depended on critical thinking and knowledge acquired over the course. Overall, CYSE 270 was one of the most valuable classes that I took while at ODU, and I am pleased to report that I am much more confident in my Linux abilities. Of course, I was apprehensive prior to taking the course, as I was still unsure about my abilities in cybersecurity; this course reaffirmed my abilities/confidence.

Interpersonal Skills

For my next artifacts, I want to segue into soft skills such as communication, teamwork, and responsibility. I learned all of these skills and more during my time at the Fall 2025 ODU/COVA Cybersecurity Clinic. Though I also gained experience in risk management and became familiar with different cyber frameworks, I want to highlight the interpersonal skills that I gained from this internship. My first artifact from the clinic is the first reflection assignment that we were tasked with a third of the way into the course of the internship. During this time, I was still apprehensive about the clinic and my ability to contribute to the cohort meaningfully. Despite this, I was able to valuably add to the many conversations occurring in the clinic and began approaching cybersecurity issues from an interdisciplinary mindset. At this point in the clinic, we became familiar with different cybersecurity frameworks, such as the NIST CSF 2.0, as well as the work of different government agencies offering cybersecurity guidance to small businesses. My next two artifacts, created during my tenure at the cyber clinic, further corroborate the soft skills I was able to develop.

My second artifact, which is the second reflection I produced during my internship, examines how I developed better teamwork skills, productive communication, and task allocation. Before this period, I was always averse to groupwork and greatly preferred to complete tasks on my own. Despite this, I went into the clinic knowing that teamwork wouldn't just be inevitable, but required to produce any work at all. Unexpectedly, I quickly adapted to the new environment and meshed completely with my teammates. We were able to adequately divide responsibilities and supported one another when required. Overall, the clinic taught me what it means not just to show up for yourself, but rather for the collective.

My last artifact taken from my time at the cyber clinic is my final course reflection, which I completed as the program came to an end. It allowed me to reflect on my growth as a student, cybersecurity professional, and most importantly, as an empathetic communicator. By working in tandem with my team and my team's client, we were able to produce results that everyone was satisfied with. In totality, the cyber clinic not just developed my technical/policy skills, but also a myriad of interpersonal skills that will assist me in any future scenario. Being able to navigate conflict and diffuse situations as they arise requires a concious level headedness that can be applied anywhere within the cyber/technology realm.

Ethical Hacking

To conclude the discussion of my skillset and associated artifacts, I want to highlight artifacts from the CYSE 301 course that helped me understand different fundamental hacking operations. Although I have decided to explore the policy side of cybersecurity, being able to understand the exploitation process can help me better understand the reasoning behind regulatory writing and policy. My first artifact for ethical hacking showcases my knowledge of password-cracking exploits. For this lab, we were tasked with using exploits available in Metasploit, a tool in Linux, to crack passwords associated with user accounts that we created. The point of the exercise was to showcase how weak hashing methods and poor password hygiene can lead to easily cracked passwords that can be decoded within minutes. Furthermore, we also explored how outdated WiFi security schemes hardly protect network passwords. This exercise was integral to my understanding of cybersecurity, as it showed me just how insecure an outdated network can be, and that freely available open source tools have the potential to wreak havoc in the right hands.

The next artifact that I'd like to discuss in reference to my knowledge of ethical hacking is the reverse shell lab. Now, this lab was particularly frustrating, as the exploit that we were tasked with using was finicky and quite touch-and-go. To complete the exploit, I had to establish a remote shell connection and remotely escalate my privileges through the target system, but even with the correct execution, I was unable to get it to work after several attempts. I became quite frustrated with myself and the application, as I wasn't making any glaring mistakes that would prevent me from establishing a connection. After several more attempts, the exploit finally worked, and I was able to complete my intrusion into the target system. More than just the technical side, this lab taught me that cyber operations aren't always finite, and that they can behave unpredictably even in a controlled environment. There is no telling as to how an exploit will behave, which makes cyber diligence all the more important.

Finally, the last artifact that I'd like to discuss rounds out my ethical hacking skillset. In this lab, we were tasked with tweaking firewall rules for a local network and examining how those changes affected the ping traffic we generated. This assignment was interesting, as it demonstrated how protective measures can prevent attack precursors and deter active security scanning by attackers. Furthermore, it allowed us to explore a wide range of cybersecurity tools, including firewalls, Nessus, and Wireshark. Being able to navigate these tools and applications is topical for anyone exploring a career in cybersecurity, even if they want to explore the policy side of the field.

Conclusion

Overall, from my time at Old Dominion University, I will be taking away both technical and interpersonal skills that I can carry into any potential career with me. Furthermore, multidisciplinary classes have also prepared me for the road ahead, as they incorporated

teachings and concepts from different fields that are universally applicable. Since cybersecurity is an interdisciplinary field, I will be incorporating lessons from psychology, sociology, and law to better understand cybersecurity policy and implementation. This wide array of knowledge and skills will allow me to succeed regardless of any unpredictable challenges that lie ahead.