Reflection Essay

Kirk Turner

Department of Interdisciplinary Studies, Old Dominion University

IDS493: Electronic Portfolio Project

Professor David Prihoda

May 3, 2026

Opening Statement:

Reflecting on my personal academic career can be very useful to understand how I have developed as a student and as someone entering the cybersecurity workforce. This reflection paper will discuss various artifacts I have selected that I feel represent my skills as a cybersecurity student at Old Dominion University. Further, I will mention several courses that have helped strengthen my ability to critically think, navigate and configure operating systems, and analyze sets of data. The following artifacts will display my competence of the three ODU learning objectives for cybersecurity:

1. Students will be able to manipulate and protect computer systems, networks, and online data from attack and compromise.
2. Students will be able to apply troubleshooting practices and identify potential security lapses.
3. Students will be able to examine and collect forensic evidence in prosecution of cyber crime.

Artifact 1 - CYSE301 Lab 3:

Artifact 1 is an assignment that was given in one of my previous courses: CYSE 301 - Cybersecurity Techniques and Operations. This lab required me to act as both an attacker and a defender using Kali Linux virtual machines. This assignment correlates to learning outcome 2 of ODU's expected learning objectives for cybersecurity students as I was required to essentially perform as a penetration tester and identify certain vulnerabilities within the virtual network. I found this important because it allowed me to understand some actions that an attacker might take to capture data and identify vulnerabilities within a network, while also teaching me certain

defensive actions that can be taken to block or limit any external traffic from entering a private network.

Artifact 2 - CYSE301 Lab 5:

Artifact 2 is another assignment from my Cybersecurity Techniques and Operations course wherein I used software to crack, or obtain/determine the real value of, both Linux and Windows password hashes. This lab assignment pertains to learning outcome 3 of the expected learning objectives as password hashes are considered digital forensics evidence. The process of password cracking is often carried out by malicious actors when they have collected enough password hashes to conduct brute-force attacks (trying every possible combination to find the correct one) or dictionary attacks (using an extensive list of known passwords to find a match). However, password cracking can be used by administrators to strengthen network security by identifying repeated or suboptimal user passwords. Since administrators have access to the /etc/shadow file for Linux systems and the SAM database or Active Directory database for Windows systems (Vatsa, 2022), they can utilize this access to perform password audits. Therefore, this assignment showcases my ability to collect digital forensic evidence for strengthening network security.

Artifact 3 - CYSE301 Lab 6:

Similar to the previous two artifacts, artifact 3 is a lab assignment that I completed in CYSE 301. This lab relates to learning outcome 3, and it required me to use digital steganography tactics to conceal a text file within an image file. I learned how to utilize a software known as steghide to embed data within files and extract the data back to its original form. By conducting this process, I learned that there are methods to transmit sensitive data other

than encrypting data and sending it through a secure channel. This method of data extraction is used by digital forensics experts to gather digital evidence that's often hidden in plain sight.

Artifact 4 - CYSE270 Lab 11:

Artifact 4 was collected from a course I took: CYSE 270 - Linux Systems for Cybersecurity. This course gave me an introduction to using Linux systems for tasks relating to system administration, security procedures, and shell scripting. Lab 11 is an overview of basic network configuration within a Linux environment. This assignment represents learning outcome 1 as it required me to obtain and modify the network configurations of my Linux virtual machine. Using the two different network configurations (NAT and Bridge Mode) taught me how either can be used to apply different routing procedures. Prior to this assignment, I was unaware of Bridge Mode as a network configuration, but completing the lab showed me that Bridge Mode can be used as an alternative to NAT to apply a unique IP address directly to a virtual machine.

Artifact 5 - IDS300W Course Research Paper:

Artifact 5 displays a research paper that I wrote for a course on Interdisciplinary Research Process and Theory - IDS 300W. This was a writing intensive course that helped build my critical thinking skills and taught me about the value of the interdisciplinary approach to solving problems. According to Repko (2007), interdisciplinary integration is required to provide solutions that account for problems affecting a vast range of disciplines. This artifact was written to provide an interdisciplinary approach to the problem of AI integration into work environments, and I believe it correlates to learning outcome 2 because it includes certain vulnerabilities that AI can introduce to the workplace. When introducing new technology into an area of business, it's always important to consider the potential downsides that might arise from

the product. In the case of AI integration for automation, there's always the possibility of periods of downtime and inaccurate data produced by these systems wherein monitoring, troubleshooting, and manual human override will be necessary.

Artifact 6 - CYSE280 Course Research Paper:

Artifact 6 is a research paper written for the course CYSE 280 - Windows System Management and Security. As the course title suggests, this course educated me on configuring, managing, and navigating Windows systems to enhance their security. This specific artifact involves a literature review to identify online risks and struggles faced by senior populations and provide potential solutions for educating them on digital literacy. Teaching senior citizens how to properly identify online threats and malicious data would lead to an increase in collected digital forensic evidence because more potential attacks would be reported to proper authorities, therefore, artifact 6 pertains to learning outcome 3. From this research, I was able to understand the importance of user education when it comes to operating a system, as well as some of the barriers that limit certain demographics and put them at a higher risk in online environments.

Artifact 7 - CYSE425W Midterm Paper:

Artifact 7 required that I analyze the National Cybersecurity Strategy passed by the Biden-Harris administration in 2023 for my Cyber Strategy and Policy course. This assignment depicts learning outcome 1 because it tasked me with researching and understanding a real-world cybersecurity framework. This allowed me to gain insight on how cybersecurity professionals might create regulations and policies for companies that adhere to this national strategy. Through analyzing a high level framework passed by the federal government, I was able to understand the process of assigning responsibilities to individuals for dealing with risk and enhancing security.

Artifact 8 - CS462 Course Report:

Artifact 8 is a report I wrote for my cybersecurity fundamentals course describing a significant data breach that took place in 2024. This course provided an overview of information and network security, with an emphasis on the issues faced by cybersecurity personnel. This artifact represents learning outcome 2 because it allowed me to understand the methods used by cybercriminals to exploit system vulnerabilities that led to the success of this attack. To identify potential security lapses, it's important that I first understand what tools and methods are commonly used by threat actors to execute their attacks. In the case of this data breach, the attackers were able to steal user credentials and gain access to confidential data due to a lack of multi-factor authentication (MFA) when signing into the database (UNC5537, 2024). Therefore, I learned that a thorough credential policy, defining factors such as password complexity and MFA policy, is an important development taken to prevent security lapses within a corporate setting.

Artifact 9 - CRJS406 Article Review:

Artifact 9 was taken from one previous course I've taken, cyber law, and it contains a review of an article based on the topic of commercial cyber espionage. Cyber law was a course that taught me about the various laws and regulations that pertain to online user activity, such as digital privacy, accessing information, and basic Internet regulations. Additionally, I learned about the extent of power concerning various legal authorities and government agencies when conducting cyber investigations. This artifact relates to learning outcome 1 as it touches on the subject of commercial cyber espionage, and whether nations should have the power to conduct such measures to gain an advantage over competitors in terms of acquiring trade secrets. According to a PowerPoint lecture taken from this course, when responding to a cyber incident,

informed decisions must be made based on information gathered from a conducted investigation (Mann, n.d.). Therefore, companies, especially large ones, must be prepared to account for data breaches or attacks that result from commercial cyber espionage. Factoring in these types of incidents could impact the ways that computers and networks are configured within a facility. For example, businesses may opt to introduce constant monitoring of user and network activity to identify any malicious or unauthorized access of data.

Conclusion:

My experience as a cybersecurity undergraduate has been extremely valuable, and if I've learned anything it's that cybersecurity is a highly dynamic field. The vastness of technology and online systems requires cybersecurity to encompass a wide array of subfields. Looking back on the progress I've made over the years has enabled me to understand how far I've come and how much farther I still have to go. So long as I remain in this field of study, I will continue learning and developing new skills as technology will forever experience new innovation.

References:

Mann, P. (n.d.). *Practical and Legal Challenges in Addressing Cyber Conflict* [PowerPoint Slides]. Canvas@ODU. https://canvas.odu.edu/courses/173350/files/48476574?module_item_id=8277997

Repko, A. (2007). Integrating Interdisciplinarity: How the Theories of Common Ground and Cognitive Interdisciplinarity Are Informing the Debate on Interdisciplinary Integration. *ISSUES in INTEGRATIVE STUDIES*, *25*, 1–31. https://www.oakland.edu/Assets/upload/docs/AIS/Issues-in-Interdisciplinary-Studies/2007-Volume-25/03_Vol_25_Integrating_Interdisciplinarity_How_the_Theories_of_Common_Ground_and_Cognitive_Interdisciplinarity_Are_Informing_the_Debate_on_Interdisciplinary_Integration.pdf

UNC5537 targets snowflake customer instances for data theft and extortion. (2024, June 10). Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

Vatsa, S. (2022). *CYSE 301 Module 4 Password Cracking* [PowerPoint Slides]. Canvas@ODU. https://canvas.odu.edu/courses/188124/files/50306252?module_item_id=8537183