Reflection Essay

Destiny Hale

Professor Prihoda

IDS 493

May 3, 2026

Introduction

My experience within the cybersecurity program at Old Dominion has been a great opportunity for me to learn everything about networking protocols to hacking. At the beginning of this program, I didn't know anything regarding cybersecurity principles besides keeping passwords safe from cybercriminals and maintaining a clean digital footprint. As I progressed through the program, my knowledge of the principles grew stronger through hands-on simulations and analytical problem-solving situations that challenged my understanding of how computers and networks work and how to protect them. In addition, I gained experience working with various tools, researching security-related topics, and applying concepts in practical assignments. Throughout my time studying cybersecurity at Old Dominion University, I developed skills such as research, analytical thinking, and technical application. The courses in my e-portfolio, such as Biocybersecurity, Cybercriminology, and Ethical Hacking, showcase these skills through labs, papers, and project artifacts.

Biocybersecurity

Artifact #1: AbbVie Cybersecurity Assessment

Biocybersecurity is an interdisciplinary field that combines "principles of cybersecurity, biology, and data science to protect biological systems and information" (Mubeen, 2024). This field addresses the risks associated with DNA information, biomedical devices, and synthetic biology to provide frameworks for protecting digital systems and biological data. In CYSE 495: Biocybersecurity, I worked with other students to develop a cybersecurity assessment for the pharmaceutical company AbbVie that focused on these high risks. This project/artifact was

divided into numerous deliverables that focused on the company's background, risk management, assets, and security recommendations, all by implementing the NIST framework.

While working on this artifact, our group came across a few challenges, such as identifying and ranking the risks of each asset of AbbVie and implementing the five NIST functions: Identify, Protect, Detect, Respond, and Recover to ensure that our security recommendations were prioritized based on actual risks. In addition, we also had to assign who was responsible for taking care of these in risk management. For instance, on my part, I addressed the risk of e-clinical systems, which are systems that help with clinical trials and healthcare. The risks associated with these systems were tampering, human error, and data leaks that cause patient data to be exploited. The most challenging part for me was assigning the categories (Information processes and procedures & Security continuous monitoring), sub-categories (PR.IP-4, PR.IP-7, DE.CM-7, DE.CM-8), such as those from the main NIST function (Protect and Detect). This process challenged my research skills because I had to learn what these NIST functions, categories, and sub-categories do to gain a better understanding of how to align specific vulnerabilities with the security protocols of the pharmaceutical industry.

Artifact #2: Medijacking

The second artifact was a small research paper that involved a mix of research and analysis regarding medijacking, using a class reading of four case studies conducted by TrapX Research Labs (2018). This research for me shifted the discussion from data privacy to physical security. For this paper, I chose the third case study, which involved the research team analyzing how malicious actors gain access to the networks and systems that most healthcare facilities use. The results from the analysis revealed that most of the systems were outdated, which led to the

hacker affecting the facility's PACS image viewer machine. From this research paper, I learned that most healthcare organizations rely on outdated software such as Windows XP, which is highly vulnerable to modern cyberattacks. It was interesting to see how hackers were able to gain access to these systems by using a backdoor for a command and control (C&C) attack. This artifact also taught me the difference between the nature of exposure and compromise; exposure provides indirect access while compromise allows a hacker to tamper with devices.

Artifact #3: Hacking Humans

Lastly, the third artifact involved researching DNA hacking risks through a class reading of Rizkallah's (2018) "Hacking Humans" article, which deepened my understanding of non-traditional cyberattacks. In cybersecurity terms, this is called social engineering, where a cybercriminal tricks a user into giving their personal credentials by impersonating either an organization or a known individual. However, human hacking in biocybersecurity terms involves gathering genetic information from users through DNA databases (such as 23AndMe) for personal gain by exploitation. For instance, Rizkallah (2018) stated that if we look at our DNA as Personally Identifying Information (PII), hackers can still use this as a benefit for personal gain from sales on the black market and great access to DNA service websites. The risks associated with genetic information involve genetic discrimination, biometric malware, identity theft, and more. While working on this research paper, I never knew that our own DNA could be at risk and be weaponized by cybercriminals; for example, in the case of identity theft, malicious actors can influence individuals to share personal information or pay for fake testing or treatment services (Vavekanand, 2024) Additionally, this revealed to me that we have to take high consideration of who we give our information to and to check how our personal or biological

data is stored with these organizations. It also sparked my interest in researching more about how our DNA can be used as a digital exploit. Collectively, these artifacts reinforced my research skills and understanding in biocybersecurity; these attacks aren't just about the loss of medical data but physical risks that weaponize our genetic data to the devices we use daily.

Cybercriminology

Artifact #1: Thematic Analysis of Cyberattacks

Cybercriminology is another interdisciplinary field that combines the fields of "criminal justice, cybersecurity, and digital forensics" to understand and prevent cyber-related crimes (Kent State Editorial Staff, 2025). A few key elements this field covers are cybercrime investigation, cybersecurity threat mitigation, and criminological theory/crime. For the course of CRJS 310: Cybercriminology: Foundations, I had to conduct a thematic analysis for a midterm regarding cyberattacks, utilizing 10 different news sources. This required a high level of analytical thinking, as I had to synthesize each source to find recurring patterns, themes (Victim Targeting, Technology Vulnerabilities, Methodologies, and Evolving Techniques), and evolving trends (Weaponization of AI and Stolen Credentials) among the articles. It was a challenging assignment because it involved connecting the dots between the incidents, ranging from nursery ransomware attacks to AI deepfake impersonation attacks, to understand how cybercriminals use both psychological and technical exploits to gain access to databases and steal credentials. The process showed me how to look at the "why" instead of the "how" of these attacks, which became the primary trends of cybercrime. Additionally, this strengthened my understanding of shifts in cybercrimes, moving from strictly technical exploits to stealthier exploits.

Artifact #2: Cybercrime Concept Map

The second artifact involved applying every concept that we have learned in the course and putting it into one concept map of how these are associated with cybercrime. Although the professor encouraged us to use AI in helping with creating this map, I still had to think of concepts that fit within the broad topic. This project also challenged my analytical thinking skills because not only did I have to piece together 15 categories with 65 subcategories, but I also had to connect them to explain why they correlate with each other. For example, in the map, I've marked key relationships such as motives and the criminology theories. Criminology theories such as Social Learning, Rational Choice, and Routine Activity provide a background explanation for cybercriminal behavior and how they gain their motives. For example, the routine activity is the theory that involves a motivated offender, a target, and an absent guardian (Graham & Smith, 2024). How this theory correlates with motives is that cybercriminals look for opportunities to exploit a system or individual for personal gain. While creating this map, it made me feel like an investigator, as it required me to synthesize a broad, complex topic into numerous categories and a logical structure.

Artifact #3: Tampa Bay Romance Scam

Lastly, for this artifact, I had to analyze and evaluate a scenario involving a cyber fraud case. Cyber fraud can come in the form of phishing and identity theft, which Jennifer became a victim of in this assignment. According to our class textbook from Graham & Smith (2024), phishing involves "sending fraudulent communications to obtain personal information." On the other hand, identity theft involves using another person's credentials in some way to deceive another individual into giving their personal information. These two cyber fraud crimes made me

realize that attackers like David can weaponize trust by blending scam attacks, such as romance and investment fraud, for financial gain. This also made me realize that cyberattacks aren't always technical-based exploitations, but psychologically manipulative exploitations; however, they use technology to make them look trustworthy to their victims. For example, David lured Jennifer by impersonating a realtor and forged business credentials to make himself look legit. This assignment also taught me what emotional vulnerability looked like. From the results of the scam, Jenniffer lost everything, and she was heartbroken due to the love bombing that David did to keep her hooked. Overall, these artifacts represent the growth of my analytical thinking from surface to deep-level thinking, allowing me to connect cybercriminal motives behind modern cybercrimes.

Ethical Hacking

Artifact #1: Malware Analysis

Ethical hacking is a field in cybersecurity that involves the use of hacking techniques by friendly parties in an attempt to uncover, understand, and fix security vulnerabilities" in computer systems (IBM, n.d). In order to understand and fix these vulnerabilities, the professionals have to conduct malware analysis and penetrate the network to strengthen the security protocols of the devices and the company. In CYSE 450: Ethical Hacking, I had to conduct a malware analysis to understand the strength and characteristics of Mirai and keylogging malware using the tool Malware Baazar. This type of malware can bypass systems, modify software, monitor keystrokes, and check proxy server settings of a computer. This lab strengthened my technical understanding of how malware can give a hacker an advantage to disrupt a system or network without being detected. From an ethical hacker professional

perspective, this gives them insight into how they can provide mitigation solutions to prevent malware from compromising the systems.

Artifact #2: Passive Reconnaissance

In this artifact, I conducted a passive reconnaissance of a web camera using the tools Shodan, MITRE ATT&CK, and WHOIS Domain Lookup. Passive reconnaissance is the first stage of penetration testing; this involves gathering all possible information about a company and its overall digital landscape without actively exploiting it. This helps ethical hackers gain a better understanding of how to execute attacks to identify vulnerabilities and fix them to keep the systems secured. However, hackers also utilize this method to plan their attacks to compromise systems. By conducting this stage, I learned how to identify potential entry points and vulnerabilities such as privilege escalation, authentication bypass, and remote command injection. Later, I provided mitigation methods to address these vulnerabilities in the web camera, such as application logs and watchdog timers.

Artifact #3: SQL Injection

Lastly, for this artifact, I executed an SQL injection attack by using the tools DVWA, Kali Linux, and Mutillidae. This lab required technical application skills, using the command “sqlmap” on Kali to identify vulnerabilities in web applications and to execute SQL injection queries. For example, I used the query injection “cyse-450” in Mutillidae to bypass authentication to potentially obtain a user's login credentials from the database. Additionally, I analyzed how the security levels (0,1,5) of the site changed. These two vulnerable web applications represent what modern organizations face when they fail to secure user inputs and

databases. These also provide vulnerabilities and attacks to help you understand how they work through documentation. Through investigating both applications, I gained an understanding of how to execute and protect against SQL injection attacks. In all, these three artifacts showcase the growth of my technical skills, using the practical application of offense and defense security strategies.

Conclusion

Reflecting on my cybersecurity journey at Old Dominion University, I have grown from a student who started with the basic knowledge of password and digital footprint safety to a student who is capable of exploring complex biological, criminal, and network-based attacks. Through the heavy research conducted in Biocybersecurity, the analytical thinking from Cybercriminology, and hands-on experience from Ethical Hacking, I have gained the skills that helped me understand and connect technical applications with the motives behind cybercrime. In all, these courses have prepared me to approach cybersecurity challenges with both technical and strategic awareness.

References

Graham, R. S., & Smith, S. K. (2024). *Cybercrime and Digital Deviance* (2nd ed.). Routledge. https://doi.org/10.4324/9781003283256

IBM. (n.d.). *What is ethical hacking?* IBM. https://www.ibm.com/think/topics/ethical-hacking

Mubeen, S. (2024, December 27). *LinkedIn*. Linkedin. https://www.linkedin.com/pulse/bio-cybersecurity-safeguarding-intersection-biology-syed-mubeen-lz1me

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

Rizkallah, J. (2018, November 29). *Hacking Humans: Protecting Our DNA From Cybercriminals*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/

TrapX Research Labs. (2018). MEDJACK.4 Medical Device Hijacking By TrapX Research Labs . In *Trust Dimension* (pp. 2–25). https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf

Vavekanand, R. (2024). Data Security and Privacy in Genomics Research: A Comparative Analysis to Protect Confidentiality. *Studies in Medical and Health Sciences*, *1*(1), 23–31. https://doi.org/10.48185/smhs.v1i1.1158