Writing Assignment Three: Reflection Essay

Brandon M. Burke

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Gordon-Phan

April 25, 2025

Abstract

This reflection explores the most important skills I've developed during my interdisciplinary cybersecurity degree—technical abilities, communication, and critical thinking—and how they've prepared me for real-world work in the cybersecurity field. Using nine different projects from a range of classes, I explain how each one challenged me to apply what I was learning in practical, hands-on ways. These projects included ethical hacking, building a command and control server, cracking passwords, giving speeches on digital security, analyzing cybersecurity laws, and writing research papers on privacy and data protection. Each experience helped me grow by improving my problem-solving, sharpening my ability to explain technical concepts clearly, and encouraging me to think deeply about ethical and legal issues. What made these projects especially valuable was how they brought together skills and knowledge from both technical and non-technical areas—like law, ethics, writing, and communication—which gave me a more complete understanding of cybersecurity as a field that impacts people, systems, and society. Overall, this essay shows how the combination of these diverse learning experiences has made me more confident, adaptable, and better prepared for the challenges of a career in cybersecurity.

Keywords: Cybersecurity, technical skills, communication, critical thinking

Writing Assignment Three: Reflection Essay

Introduction

Throughout my interdisciplinary cybersecurity degree program, I've acquired a variety of skills that have prepared me for a career in cybersecurity. These skills are a blend of technical expertise, communication proficiency, and critical thinking abilities. Over the years, my coursework and hands-on projects have allowed me to demonstrate my proficiency in these areas and have helped me build a foundation for tackling real-world challenges in the cybersecurity field. According to Brodnitz, research (i.e., technical skills), communication, and problem-solving (i.e., critical thinking) are among one of the most common and in-demand skills on the job market (Brodnitz, 2024). Furthermore, a job listing by the Federal Bureau of Investigation states that having technical, people, and critical thinking skills are all important to the role and to fulfill the role to the best of your ability (*Federal Bureau of Investigation Special Agent*, 2024). This reflection will explore three key skills—Technical Skills, Communication, and Critical Thinking—and analyze how my artifacts showcase these abilities. Additionally, I will discuss how my academic experiences have shaped my career readiness and positioned me for success as a cybersecurity professional in the future.

Technical Skills

In the field of cybersecurity, technical skills are undeniably essential, as they directly impact one's ability to protect systems, networks, and sensitive data. Over the course of my studies, I've gained hands-on experience through various projects that allowed me to apply my technical knowledge to real-world security scenarios. These artifacts reflect my technical abilities and showcase how I have successfully applied them in practical settings. Each project required me to tackle specific challenges and apply a range of tools and techniques to solve

problems effectively. These experiences have enhanced my technical competence and made me more confident in applying my skills to mitigate real-world cybersecurity threats.

Artifact 1: CYSE 301 - Ethical Hacking

In my Ethical Hacking class, I had the opportunity to work on an assignment where I learned how to identify and exploit vulnerabilities within computer systems. One of the key tasks was exploiting a vulnerability in an unsecured Windows computer using Metasploit to gain root access. This assignment required me to use tools like Kali Linux, Wireshark, and Metasploit to exploit a weakness in the system. The goal of this project was not only to understand how attackers could compromise a system, but also to learn how ethical hackers work to prevent such attacks from happening.

What stood out to me in this project was how critical it is to have a thorough understanding of the potential weaknesses in a system, whether it is a computer, network, or device. The most challenging aspect of this assignment was navigating the complexity of the tools involved and learning how to troubleshoot issues as they arose. I often had to rely on YouTube tutorials, Google searches, and online forums to resolve bugs. These resources helped me find solutions to problems that I would not have been able to solve on my own. Through this project, I developed problem-solving skills and became more adept at troubleshooting, which are key abilities that I will apply to any future cybersecurity challenge.

This project gave me a deeper appreciation for the importance of ethical hacking. It reinforced the idea that security is an ongoing process that requires vigilance and continuous testing. The skills I gained in this course are directly applicable to the work of cybersecurity professionals, particularly those who are tasked with identifying weaknesses in systems before malicious hackers can exploit them. The experience taught me to always be cautious when

interacting with unfamiliar systems and to continually test for vulnerabilities. This hands-on experience with ethical hacking tools has given me a strong foundation for entering the cybersecurity workforce.

Artifact 2: CYSE 250 - Command and Control Server

Another significant technical project was in CYSE 250, where I created a command and control (C&C) server to exfiltrate information from a client executing a malicious file. This was my first experience creating a program that interacted with other computers on a network level, which was both challenging and educational. It introduced me to the complexities of server infrastructure, networking, and the way malware can be used to compromise systems remotely. The assignment involved building a malicious server that could communicate with a compromised system, giving me the chance to explore network-based vulnerabilities.

One of the main challenges I faced during this project was debugging repeated errors that occurred throughout the process. Debugging can often be frustrating, but I learned that persistence is key. To resolve the issues, I turned to online resources like Reddit, Stack Overflow, and various cybersecurity forums, where I found solutions and learned from others' experiences. This process taught me the importance of patience and resourcefulness when troubleshooting network-based issues. Moreover, it reinforced the need to always stay updated on security best practices and to be cautious when dealing with network communications.

Through this project, I gained valuable insights into how attackers control systems remotely and exfiltrate data. I also learned the importance of ensuring that malicious files are never executed on a system unless the code is thoroughly vetted. This assignment enhanced my understanding of both offensive and defensive cybersecurity strategies. It taught me how essential it is to be vigilant about security measures when interacting with files and systems over

a network, and it instilled in me the discipline to carefully monitor and control access to critical data.

Artifact 3: CYSE 270 - Password Cracking

In CYSE 270, I worked on a password cracking project where I used tools like John the Ripper and Hashcat to crack hashed passwords. This task was designed to demonstrate how easily weak passwords can be compromised using modern password-cracking techniques. The project was a stark reminder of the importance of password strength and how easily attackers can gain unauthorized access to systems that rely on weak passwords.

The most surprising part of this assignment was how quickly I was able to brute-force an 8-character password. I had previously underestimated the ease with which attackers can crack simple passwords. This project was an eye-opening experience because it made me realize just how vulnerable systems can be when passwords are not complex enough. It also reinforced the need for strong password policies in organizations and for individuals to adopt secure password practices. The project taught me that password length and complexity are paramount in securing sensitive systems.

Additionally, this assignment showed me the importance of implementing multi factor authentication (MFA) as an extra layer of security. While strong passwords are important, they are not enough on their own to prevent unauthorized access. The combination of a strong password and MFA can greatly reduce the risk of a successful attack. This experience deepened my understanding of the need for multi-layered security strategies and highlighted the importance of educating users about the risks associated with weak passwords.

Communication

In addition to technical skills, effective communication is crucial in cybersecurity. Cybersecurity professionals must be able to explain complex issues in clear, understandable terms to both technical and non-technical audiences. Throughout my coursework, I've had the opportunity to refine my communication skills, particularly when it comes to presenting technical information to diverse audiences. Whether in written reports, presentations, or speeches, I've learned how to convey information in a way that is both informative and accessible.

Artifact 1: IT 315 - Financial ROI Analysis

In my IT 315 class, I conducted a financial return on investment (ROI) analysis to determine the cost-effectiveness of wiring Ethernet in a high school. This assignment required me to present technical information in a way that was accessible to school administrators and IT staff, who might not have extensive technical backgrounds. The goal was to break down the technical aspects of the project into clear, understandable terms so that decision-makers could make an informed choice.

To make the information more digestible, I broke down the costs into clear categories such as labor, equipment, and installation, and I used simple language to explain the financial implications. I also included tables for the cost breakdown, which helped the audience better visualize the data. This experience taught me how to present complex technical information in a way that was understandable to people without a technical background. It also helped me learn how to adjust my communication style to suit different audiences, whether they are highly technical or not.

Through this assignment, I realized the importance of clear communication, especially when discussing technical topics with people who may not have the same level of expertise. It reinforced the need to simplify complex concepts and provide clear explanations, which is essential in both professional and academic settings. It also helped me understand how technical decisions, like the installation of new networking infrastructure, can have far-reaching implications for organizations and individuals.

Artifact 2: COMM 101R - You Are Not Secure

In COMM 101R, I delivered a speech titled "You Are Not Secure," where I discussed how even seemingly secure digital environments are vulnerable to cyberattacks. My goal was to raise awareness about the risks associated with digital security and to emphasize the importance of understanding these risks. The speech was designed for a general audience, and I used relatable examples to help convey the message effectively.

One of the main strategies I used to engage my audience was providing real-world examples, such as how Wi-Fi networks can be hacked. I also used simple, non-technical language and analogies to make the message more relatable to people without a technical background. For instance, I compared the security of a home to the security of a Wi-Fi network, which made the concept easier for people to grasp. I also emphasized how everyone uses Wi-Fi and how the security of these networks affects everyone, regardless of their technical expertise.

This experience taught me the importance of clear and concise communication when discussing cybersecurity topics. It also helped me realize that cybersecurity awareness should be shared with everyone, not just technical experts. Presenting these concepts in an engaging and relatable way is key to spreading awareness and promoting better security practices. Effective

communication plays a vital role in educating the public about cybersecurity and encouraging them to adopt safer online habits.

Artifact 3: ENGL 211C - Cybersecurity Imperative Measures

In ENGL 211C, I wrote a research paper on cybersecurity imperative measures, where I argued that people, companies, and governments should work together to develop effective strategies for protecting personal data. I used a combination of academic sources, news articles, and cybersecurity reports to support my arguments. The paper was designed to persuade readers of the importance of cybersecurity measures and to highlight specific actions that individuals and organizations can take to protect personal data.

Through this assignment, I learned how to organize my thoughts more clearly and effectively communicate complex ideas through writing. I also learned how to break down technical jargon into simple language so that my audience could easily understand my points. This ability to write clearly and persuasively is crucial in cybersecurity, where effective communication can often mean the difference between successfully protecting data and exposing it to risk. Writing this paper also helped me better understand the broader implications of cybersecurity beyond technical considerations, such as legal and ethical concerns.

Critical Thinking

Critical thinking is a core skill in cybersecurity, as professionals must constantly evaluate potential threats and solutions, weighing various factors such as ethics, legal issues, and technological implications. According to the Great Learning Editorial Team, “the ability to analyze issues critically and make informed decisions is essential, especially in fields requiring strategic planning and business acumen” (Team, 2025). Throughout my coursework, I’ve been tasked with analyzing complex issues, considering multiple perspectives, and developing

well-reasoned conclusions. Critical thinking has allowed me to evaluate security risks more effectively and to come up with solutions that are both practical and ethical.

Artifact 1: IDS 300W - Balancing National Security and Privacy

In IDS 300W, I wrote a paper examining the tension between national security and privacy rights. This issue has been a longstanding debate, particularly in the context of cybersecurity and government surveillance. In my paper, I argued that while national security is essential for the safety and stability of the country, it should not come at the expense of individual privacy rights. This is exemplified by Alan Westin, a sociologist. He states "a survey of Internet users in early 2002 found that 87% were still concerned about privacy," particularly under the U.S. Patriot Act (2003). In this paper, I explored how mass surveillance and data collection could infringe on civil liberties and lead to unwarranted invasions of privacy.

The critical thinking skills required for this paper were essential. I had to carefully weigh the ethical, legal, and political implications of surveillance programs. I analyzed various policies, such as the USA PATRIOT Act (USPA), and considered their impact on both national security and personal freedoms. My research also required me to evaluate the consequences of sacrificing privacy in the name of security and whether it would ultimately undermine the democratic values that the government seeks to protect. According to Kerr, the USPA gives the government more power to intercept internet traffic and fight cybercrime, expanding its authority over communications networks used daily by millions of Americans for postal services, phone calls, and internet access, which allow users to send, receive, and store information but also provide opportunities for criminal activity like organized crime, terrorism, and other threats to national security (Kerr, 2003). However, this comes at the cost of privacy, which can be argued is a fundamental right under the Fourth Amendment of the United States Constitution. This

assignment sharpened my ability to assess the trade-offs inherent in cybersecurity policy and reinforced the importance of considering multiple viewpoints when tackling complex issues.

One of the most significant lessons from this paper was understanding the importance of finding a balance between security and privacy. It taught me that while cybersecurity is essential, it must be implemented in a way that respects individuals' rights. This issue continues to be relevant as new technologies emerge, and it has shaped my thinking on the ethical challenges cybersecurity professionals face when making decisions that could affect both national security and personal privacy.

Artifact 2: CYSE 280 - Latest Security Threats and Mitigation Strategies

In CYSE 280, I wrote a paper on the latest security threats and the strategies available to mitigate these threats. This artifact required me to think critically about the rapidly changing landscape of cybersecurity and how emerging threats could compromise systems. I researched various types of attacks, including ransomware, phishing, and denial-of-service (DoS) attacks, and evaluated the effectiveness of existing mitigation strategies. The goal was to assess which defense mechanisms worked best in specific scenarios and propose additional measures that could help organizations stay ahead of evolving threats.

What stood out in this project was the sheer speed at which cyber threats are evolving. I had to critically assess the risks posed by each type of attack and consider the resources required to defend against them. This meant not only looking at the technical aspects of cybersecurity, but also considering the practical implications of implementing specific mitigation strategies. For example, while encryption may be an effective solution for data protection, it can also slow down system performance, requiring a balance between security and usability. This project helped me

understand that cybersecurity is not just about deploying the latest technologies; it's about making strategic decisions that align with the specific needs and limitations of an organization.

The critical thinking involved in evaluating security threats and mitigation strategies helped me understand that cybersecurity solutions must be tailored to the unique needs of each situation. There is no one-size-fits-all approach, and the most effective strategies often involve a combination of technologies and processes. This project reinforced my belief that critical thinking is crucial in cybersecurity because it allows professionals to adapt to changing threats and devise solutions that are both effective and efficient.

Artifact 3: CYSE 406 - Overview of Privacy and Data Protection Issues

In CYSE 406, I wrote a research paper that provided an overview of privacy and data protection issues, focusing on how legal and ethical frameworks shape the way personal data is handled. This paper required me to critically examine various privacy laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and evaluate how they are applied in the context of cybersecurity. For context the GDPR, instituted in the European Union (EU), is a comprehensive data protection law with key provisions including broad coverage including organizations processing personal data of individuals in the EU, irrespective of location, and encompasses EU citizens' data being processed outside the EU. Key data protection principles established by the GDPR include data minimization, purpose limitation, and accountability, all aimed at ensuring that individuals have greater control over their personal information (European Union, 2024). This law is not in effect in the United States leaving the country vulnerable to breach of privacy among its citizens. In addition, I also analyzed the challenges organizations face when trying to comply with these laws and the consequences of failing to protect personal data.

This paper required a deep dive into the intersection of cybersecurity, law, and ethics. I had to think critically about how privacy laws affect the decisions cybersecurity professionals make when it comes to data protection. For instance, the GDPR places strict requirements on organizations regarding the collection and storage of personal data, and failure to comply can result in significant fines. I analyzed how businesses navigate these regulations and how they balance the need for data security with the desire to protect users' privacy.

The most challenging part of this paper was understanding the legal implications of cybersecurity measures and how they impact business practices. I had to consider how laws like the GDPR influence the way organizations collect, store, and process data, and how failing to adhere to these regulations could lead to legal consequences. This assignment reinforced the importance of critical thinking in cybersecurity, especially when dealing with sensitive data. It also emphasized the need for cybersecurity professionals to stay informed about privacy laws and best practices in order to ensure compliance and protect individuals' rights.

Conclusion

In conclusion, my interdisciplinary degree program in Cybersecurity has significantly developed my skills in technical proficiency, communication, and critical thinking. The various artifacts collected and discussed in this portfolio reflect not only the knowledge I have gained but also the practical application of that knowledge in real-world situations. Through my coursework and hands-on projects, I have built a strong foundation in cybersecurity, enhanced my ability to communicate complex technical concepts effectively, and honed my critical thinking skills to analyze and address the ever-evolving challenges in the field.

Each of the skills I have acquired has prepared me for a successful career in cybersecurity, where I can apply both technical expertise and effective communication strategies

to solve complex problems. For example, my work with Metasploit and command and control servers allowed me to apply my technical skills to real-world security issues, while my communication projects, such as creating presentations and research papers, helped me convey intricate cybersecurity concepts to diverse audiences. The critical thinking projects, particularly those that required analyzing privacy laws and emerging security threats, have shaped my understanding of the ethical and legal aspects of cybersecurity and prepared me to navigate the complexities of this field in a responsible and effective manner.

Reflecting on my degree, it is clear that interdisciplinary thinking has been central to my growth as a cybersecurity professional. My studies have shown me how combining knowledge from different disciplines—such as law, ethics, and technology—provides a more comprehensive approach to problem-solving. The ability to think critically, communicate clearly, and apply technical skills across different contexts will be invaluable in my future career. As I move forward, I am confident that the lessons learned during my program will continue to guide me as I pursue opportunities in cybersecurity, where I can contribute to securing our digital world while considering the broader social and ethical implications of my work.

References

Brodnitz, D. (2024, February 8). *The Most In-Demand Skills of 2024*. LinkedIn. https://www.linkedin.com/business/talent/blog/talent-strategy/linkedin-most-in-demand-hard-and-soft-skills

European Union. (2024, April 22). *General Data Protection Regulation*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Federal Bureau of Investigation Special Agent: Cybersecurity/Technology Background. Glassdoor. (2024, December 3). https://www.glassdoor.com/job-listing/special-agent-cybersecurity-technology-background-federal-bureau-of-investigation-JV_IC1130306_KO0,49_KE50,81.htm?jl=1009551306223

Kerr, O. S. (2003). Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't. *Northwestern University Law Review*, 97(2), 607. https://doi.org/10.2139/ssrn.317501

Team, G. L. E. (2025, January 6). *The importance of soft skills in today's evolving professional landscape*. Great Learning Blog: Free Resources that Matters to shape your Career! https://www.mygreatlearning.com/blog/what-are-soft-skills/

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072