Writing Assignment Two: Personal Narrative Essay

Brandon M. Burke

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Gordon-Phan

April 2, 2025

Abstract

This essay reflects on my journey toward a career in cybersecurity, focusing on important experiences, challenges, and achievements along the way. My interest in technology began at a young age through gaming, where I became curious about how systems work and how to protect them. Key moments, like building a Python-based command and control server and earning the CompTIA Security+ certification, strengthened my commitment to the field. Despite challenges such as balancing school with personal responsibilities and keeping up with fast-changing technologies, my determination to succeed in cybersecurity has only grown. Mentors and hands-on learning have helped me understand the field better, while overcoming academic challenges like struggling in one of my classes called Networked System Security. This has taught me the value of persistence and using available resources. My goal is to contribute to national security and cybersecurity policies with the Federal Bureau of Investigation (FBI). Furthermore, my journey shows the importance of ongoing learning, flexibility, and passion in this ever-changing field.

Keywords: Cybersecurity, career path, academic challenges, passion and curiosity

Writing Assignment Two: Personal Narrative Essay

Introduction

The journey toward a career in cybersecurity is rarely linear. For me, it has been a path shaped by various experiences, from gaming to academic pursuits. The combination of curiosity, personal interests, and key academic and professional moments helped me realize that cybersecurity was the right fit for me. As I reflect on my experiences, I'm reminded of how each event has contributed to my growth and determination to succeed in this dynamic field. According to McAdams (2001), the process of constructing one's life story is fundamental to identity development, as individuals make sense of their past experiences and use them to inform their future. This concept resonates with my own journey, where each challenge and success has been woven into the broader narrative of my personal and professional growth.

While cybersecurity is often seen as a field for tech enthusiasts or those with a deep technical background, I believe that anyone with the right mindset and passion can thrive. In this essay, I will share my journey, which started with my fascination for technology and expanded into a commitment to keeping systems secure in an increasingly digital world. The path wasn't without its challenges, but each one served as an opportunity to grow, learn, and adapt, driving my determination to make a lasting impact on the cybersecurity landscape.

Early Interest in Technology

My fascination with technology began at a young age. Growing up, I was always curious about how systems worked, which led me to explore computer science and cybersecurity online using various platforms such as YouTube. I was especially interested in troubleshooting, problem-solving, and understanding how devices communicate. This natural curiosity was a

significant foundation for my eventual pursuit of cybersecurity. However, my first exposure to

technology wasn't through formal computer courses, but rather through my passion for gaming.

In my teenage years, I became interested in cheating in video games, specifically in *Clash*

of Clans. The only device I had at the time was an iPhone 4s, which led me to search for ways to

manipulate the game. Through YouTube tutorials, I learned how to jailbreak my iPhone, which

allowed me to gain root access to the device and install third-party applications to modify the

game client. This experience introduced me to the broader world of computer security, including

hacking and penetration testing, which sparked a deeper interest in the field. What started as an

attempt to bypass in-game mechanics soon turned into an exploration of the vulnerabilities

within systems and software. I became fascinated with the idea that there were flaws within

seemingly secure platforms, and my curiosity to understand and manipulate these flaws led me to

learn about cybersecurity, ethical hacking, and how individuals can protect systems from such

vulnerabilities.

A Key Academic Moment

My academic journey took a pivotal turn during my CYSE 250 Networking and

Programming course. For the final project, I created a Python command and control server that

could control a client or victim computer. This hands-on experience was crucial in solidifying

my interest in cybersecurity. The idea that I could control another system, albeit in a controlled

and ethical manner for the purposes of learning, gave me an immense sense of accomplishment.

To add to the excitement, the class held a vote to determine who had the best project, and I was

voted at the top, winning $20. I used this prize to buy dinner that evening, but more importantly,

it gave me a confidence boost and further fueled my desire to pursue a career in cybersecurity. It

was at this moment that I fully realized the potential I had in this field and the passion I held for

it. The project not only challenged me technically but also solidified my belief in the importance of securing systems and understanding the implications of exploiting vulnerabilities.

Another significant milestone was earning my CompTIA Security+ certification in 2022. At the time, I had limited knowledge of cybersecurity, but I decided to take on the challenge of studying for the exam. After three weeks of intensive preparation, I passed the exam on my first try. This accomplishment was a testament to my commitment and determination, reinforcing my belief that cybersecurity was the right path for me. I felt proud not only because of the accomplishment but also because the certification opened doors to new learning opportunities and resources, enhancing my understanding of the concepts needed to protect systems. The realization that cybersecurity was a highly structured yet dynamic field encouraged me to continue growing my expertise in the area.

Challenges Along the Way

Despite these successes, my academic journey wasn't without challenges. One of the biggest obstacles I faced was balancing coursework with personal responsibilities. There were times when the workload became overwhelming, and managing stress while staying focused on my studies was difficult. This struggle was compounded by the constant demands of adapting to new technologies and evolving concepts in the field of cybersecurity. Learning how to manage stress while maintaining focus required me to develop better time management skills, which have since been invaluable in my professional and academic life. The challenges in keeping up with the rapid changes in technology were also a frequent concern. As cybersecurity is an ever-evolving field, I found myself constantly needing to learn new concepts, tools, and best practices. Each new development in the field required a fresh approach and deeper understanding. In the face of these challenges, I adopted a mindset of continuous learning,

knowing that staying up-to-date with trends was not just a necessity but also an opportunity to keep expanding my skill set.

Additionally, my journey was greatly influenced by the learning experiences shared by mentors and YouTubers like David Bombal, NetworkChuck, and the PC Security Channel. These individuals introduced me to a wide range of tools, techniques for malware detection, ethical hacking, and other cybersecurity concepts, which helped deepen my understanding of the field. Their content provided practical, real-world examples that made theoretical concepts easier to grasp. I was especially drawn to their ability to break down complex topics into simple, digestible lessons, making it easier to build confidence in my skills. Their engaging and approachable teaching styles not only kept me motivated but also inspired me to explore areas like penetration testing, vulnerability assessment, and digital forensics. As I followed their videos and interacted with their communities, I found myself experimenting with new tools and taking on personal projects to apply what I learned. This exposure to various aspects of cybersecurity not only broadened my knowledge but also opened my eyes to the diverse career paths within the field. These experiences reinforced the importance of staying curious, continuously learning, and never underestimating the power of accessible, self-paced education.

The Turning Point

A major turning point in my journey came when I realized that to truly succeed in cybersecurity, I needed to expand my education and skills. While I had some hands-on experience and basic knowledge, I knew that formal education would help me sharpen my abilities and open up new opportunities. Wanting to pursue a career in cybersecurity, I applied to Old Dominion University to major in the field. At first, I considered studying IT or computer science, but my interest in security and protecting digital systems led me to choose cybersecurity.

This decision was the start of my deeper dive into the field, where I could apply what I had learned and build more knowledge. As I moved into my academic studies, I found that the experience offered new challenges, but I embraced them. I worked hard in my classes and hands-on projects, learning everything from network security to ethical hacking. This helped me not only gain technical skills but also understand the bigger picture of cybersecurity, including the need for strategic thinking and staying ahead of threats. The combination of education and practical experience made me even more committed to my goal of working in cybersecurity and prepared me for the challenges and opportunities that lie ahead.

Overcoming Academic Hurdles

One of the most challenging academic experiences I encountered was my Networked System Security class. The course was demanding and required me to apply both theoretical knowledge and hands-on skills to understand complex security protocols and techniques. The assignments were difficult, especially when it came to understanding configuring, securing, and protocols associated with network systems. These concepts required a deep understanding of networking concepts. At times, I struggled to keep up with the pace and the technical details, and it felt overwhelming. However, I sought help by using additional resources like online tutorials, textbooks, and discussions with my professor and classmates. This support system, combined with my determination, allowed me to successfully complete the course and gain a deeper understanding of network security. The experience taught me the importance of persistence and how vital it is to ask for help when facing difficulties. It also reinforced that learning in cybersecurity is not only about individual effort but also about collaborating with others and utilizing every resource available to fully grasp the complexities of the field.

Following my experience in the Networked System Security class, another challenging yet rewarding course I took was my Python programming class. The course required me to shift from simply learning concepts to actively applying them in practical coding exercises. In the beginning, I struggled with understanding Python's syntax and the logic behind coding, especially when creating scripts for tasks like automating processes or analyzing data. However, much like in my network security class, I realized the importance of mastering these foundational concepts, and the more I practiced, the clearer the logic became. As I worked on various hands-on projects, I learned how programming in Python could be used to build security tools, analyze network traffic, and automate security-related tasks. This practical application of Python helped me understand how programming is a crucial skill in cybersecurity, especially when it comes to tasks like penetration testing and vulnerability analysis. The experience not only deepened my technical skills but also reinforced the value of persistence and problem-solving. It showed me how combining theory with hands-on practice was key to truly grasping complex cybersecurity concepts and developing the ability to think critically about solving security challenges.

Future Goals and Conclusion

As I look to the future, my goal is to work for the FBI in their Cyber Division, applying my skills to combat cybercrime and protect national security. I aim to deepen my expertise in digital forensics, threat analysis, and incident response, and I hope to specialize in tracking cybercriminals and identifying vulnerabilities in critical systems. I also see my career evolving toward both offensive and defensive cybersecurity strategies, potentially leading to roles in cyber intelligence and security architecture. In the long term, I aspire to contribute to shaping cybersecurity policy and best practices, helping organizations defend against emerging threats.

Additionally, I hope to mentor the next generation of cybersecurity professionals and foster a culture of security awareness. Ultimately, I want to be part of a team that not only reacts to cyber threats but also proactively works to prevent them.

Reflecting on my journey, I realize that passion, curiosity, and the willingness to continuously learn are essential for success in cybersecurity. My story is not defined by a single event but by a series of experiences, from gaming to academic challenges, that fueled my desire to pursue this career. The field is constantly changing, and staying adaptable, determined, and committed to growth has been key to my journey. I am excited to continue on this path, knowing that every challenge I face is an opportunity to grow and make a meaningful impact in the world of cybersecurity.

References

McAdams, D.P. (2001). The psychology of life stories. *Review of General Psychology*, *5*(2),

    100-122.