Self Reflection

Alexander Kotzian

October 11, 2025

Introduction

Throughout my time as a student at Old Dominion University, I have explored a multitude of different concepts from the courses I've taken. With that knowledge, I have decided to put forth what I thought was most valuable across my studies into my electronic portfolio. The three primary skills I decided to highlight first were Cybersecurity, reporting, and programming. Each of these skills has come from a multitude of interdisciplinary courses that greatly improve my value in the field of Cybersecurity. For Cybersecurity my artifacts come from the courses: Cybersecurity Techniques and Operations (CYSE301), Introduction to Cyber Risk Management (CYSE495), and Ethical Hacking and Penetration Testing (CYSE450). My reporting artifacts come from the courses: Cyber War (CYSE426) and Introduction to Cybersecurity (CYSE300). My programming artifacts come from the classes: Introduction to Game Programming (GAME111), Introduction to Programming With Java (CS151), and Basic Cybersecurity Networking and Programming (CYSE250). Each of these showcases an interdisciplinary contribution to my knowledge and expertise in Cybersecurity.

Cybersecurity

The first artifact is a penetration testing lab report in which I perform an exploit from a Linux system on a Windows 7 system. I use Metasploit to conduct a reverse shell connection to upload a payload that ensures persistent access upon login to a separate

Linux system. This course taught me how to conduct a multitude of different techniques to exploit vulnerabilities in Windows based systems. A previous course focused on Linux operations assisted me in writing a payload and using Metasploit to conduct the reverse shell connection. Penetration testing is a fundamental aspect to ensure an organization's cyber security is compliant with laws and regulations, and is a preventative measure. According to the National Cyber Security Centre of the UK, one of the most important parts in the success of a penetration test is the quality and expertise of the penetration tester (NCSC UK). This artifact gives an example of my hands-on qualifications regarding penetration testing. Penetration testing requires an in-depth understanding of vulnerabilities and the tools that are used in attacks.

The second artifact showcased on my skills page is an analysis paper on the importance of 'business impact analysis', business continuity plans, disaster recovery plans, and computer incident response team plans in the creation of a risk management policy. Each of these plays a particularly crucial role in a business's functions and continued operation in the event of a disaster or attack. This analysis of some of the core components of a risk management policy highlights my in-depth understanding of how to create one. According to CISA, a large portion of the United States' critical infrastructure is owned by the private sector (CISA). This fact makes this skill easier to apply across both public and private sectors. Understanding the impacts

of attacks and how to respond also gives insight into what potential motives these threats have.

The third artifact showcased within the Cybersecurity skill group is a lab in which I analyze the operations and effects of two different malware. This lab was conducted within an Ethical Hacking and Penetration Testing course. This course has expanded my knowledge even further when it comes to penetration testing. This particular artifact highlights my ability to analyze malware and determine its entry, methods, and goal. Particularly proving my ability to investigate recent and everchanging malware. Additionally, learning this has allowed me to identify other malware for others, providing me with further insight into malware. Malware is one of the primary tools used by hackers to infiltrate or disrupt organizations, so understanding how to analyze it is vital to conducting cybersecurity operations.

Reporting

The first artifact in this group is an analytical report of the social and technical aspects of cyberterrorism. In this report, I detail a multitude of cyberterrorist attacks, why they happened, who they effected, and what their goals seemingly were. With the rise of government-backed and domestic cyber terrorist groups, it is imperative that we understand why they conduct these attacks and who they're targeting. Anonymous is a persistent cyberterror actor who has a much larger presence than many government-backed cyberterror groups. Anonymous is more noticeably active in regard

to social issues, such as the Occupy Wall Street movement. This particular type of cyberterror is called hacktivism, which is “a form of contentious politics carried out by non-state actors in support of a variety of political, social, or religious causes… ” (Kenney 2014). Understanding the motivations behind hacktivists gives a much greater insight into where they may strike next and how. This type of deeper understanding of hacktivism is vital in the field of Cybersecurity, and helps me strategize accordingly.

The second artifact is the construction of a corporate database security policy. In this policy, I conduct a reasoned security policy that informs operational procedure and compliance. This security policy specifically uses the CIA triad as a framework, which is one of the foundational concepts in regards to a cybersecurity policy. This artifact showcases my ability to create a functioning security policy. According to Lipovac and Babac, the study they had conducted recorded a rise in technical skills being requested in job advertisements (Lipovac & Babac, 2021, p.512). The technical skill of being able to construct a practical security policy is vital in providing assistance in their creation, or creating them myself.

The third artifact is a research report on the Equifax data breach that occurred in 2017. In this report, I consolidate my findings on the breach itself, how it happened, and how it affected victims of the breach. Additionally, I provide insight on what could have prevented the breach and some of the missteps that caused it. This report highlights a lot of the information I’ve gathered over many of my previous courses. It

showcases how I understand ethics in the cybersecurity industry and my knowledge of repercussions in the event of a breach. Being able to look at past mistakes and prevent those same mistakes from occurring is beyond valuable in any position. This particular paper shows my ability to apply those observations in Cybersecurity. Additionally, adding insight to a future risk management or security policy.

Programming

The first artifact that showcases my programming skills is a programming project written in C#. This project utilizes a random number generator and a stopwatch tool to create a math quiz that takes a certain amount of time to complete. This highlights my knowledge of tools and program creation within C#. C# is the fifth most popular programming language in the world according to the TIOBE index (Jansen 2025). This artifact showcases my variety of programming language knowledge and skills in the C family of programming languages. Additionally, C# is commonly used in game development, broadening my scope of skills on an interdisciplinary level.

The second artifact is a lab program created to calculate, average, and define grades through the use of multiple methods. This lab was conducted in Java, the fourth most popular programming language according to the TIOBE index (Jansen 2025). The functionality of this program showcases my ability to conduct multiple operations in a single program without error. Additionally, it furthers my variety of programming languages that I hold expertise in.

The final two artifacts are two programs that create a voting server. This creates a secure client-server connection that requires authentication and login information stored on the server. The server is able to withhold multiple client connections and inputs at one time. This highlights my practical knowledge of Python in creating programs that can interact with other programs and devices. Furthermore, it proves my knowledge of encryption and decryption methods and my ability to apply them in my programming. Python is the most popular programming language by far according to the TIOBE index (Jansen 2025). The value of Python programming experience is incredibly vast, as it covers a multitude of different disciplines. Relative to me, Python is used in many of the penetration testing tools I use, such as Nmap. Additionally, Python can be used to create custom scripts to exploit vulnerabilities in systems. Python is also largely used in machine learning, which is one of the more rapidly expanding concepts in cyber space. This gives me insight in how to react and prevent attacks and infiltration techniques that are entirely artificial intelligence. This directly applies to previous artifacts through the use of it in malware and payload creation.

Conclusion

Throughout this reflection paper, I examined my artifacts and what they meant to me. I saw what interdisciplinary aspects they had and what they didn't. A majority of these artifacts play a smaller role in another skill represented. Primarily providing a very good overall foundation to Cybersecurity. Direct interaction between penetration

testing and Python programming. Additionally, Cybersecurity interacts with all programming languages. Reporting provided a social and analytical value to Cybersecurity. I absolutely utilized my expertise in penetration testing script writing and translated that to practical programming knowledge for each of the three programming languages I presented. Python knowledge, in particular, is assisting in the use of penetration testing tools and techniques. The Interdisciplinary Theory and Concepts course gave me insight on how to apply the different disciplines within others, such as with Python and penetration testing, or with risk management analysis and security policy creation. In conclusion, it is vital to appreciate and utilize an interdisciplinary perspective in order to bring the most value from all of my experiences to each and every step I take in pursuit of my career.

References

Penetration testing. NCSC. https://www.ncsc.gov.uk/guidance/penetration-testing

Risk management. Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov/topics/risk-management

Kenney, Michael (2014, November 17) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Volume 59, Issue 1, Pages 111-128, ISSN 0030-4387, https://doi.org/10.1016/j.orbis.2014.11.009 or https://www.sciencedirect.com/science/article/pii/S0030438714000787

I. Lipovac., M. B. Babac. (2021, November 26). *CONTENT ANALYSIS OF JOB ADVERTISEMENTS FOR IDENTIFYING EMPLOYABILITY SKILLS*. Indecs. https://www.indecs.eu/2021/indecs2021-pp511-525.pdf

Jansen, P. (2025, October). *Tiobe index*. TIOBE. https://www.tiobe.com/tiobe-index/