Reflective Essay

Isaac Huston

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

December 5, 2025

Introduction

Throughout my degree program I learned that the technical skills I came in with were only part of what I needed. The courses I took pushed me to understand how different disciplines fit together and why cybersecurity work is never just technical. Networking, scripting, policy, critical thinking, and communication each played a specific role in shaping how I approach problems. That mix is what helped me identify the three skills that represent me the most. Those skills are network security analysis, scripting and automation, and penetration testing. Each one came from different classes, labs, and projects, but they ended up complimenting each other in a way that made me more prepared for the type of work that is actually done in the field.

My coursework was never isolated. Every class tied back to something bigger. Even general education and interdisciplinary courses like IDS 300W taught me how to frame my ideas clearly, explain technical concepts, and connect theory to real scenarios. Other classes pushed me deeper into practical work, where I had to take the concepts and convert them into something usable. That combination shaped how I built my portfolio and why these nine artifacts represent who I am as I move toward a cybersecurity career.

Network Security Analysis

Network security analysis became one of the areas where I was able to excel in. I spent enough time working with tools like Nmap, Wireshark, and multiple scanning utilities that the process started to feel natural. The artifacts I selected for this skill reflect that. My TryHackMe Blue Walkthrough, my HTB Crocodile Walkthrough, and my Nmap Scan Procedure Documentation show the different pieces that go into analyzing a system, identifying an attack path, and figuring out what the network is actually doing.

Working on Blue was the first time I really chained together enumeration, exploitation, and confirmation all the way through without guessing. I had to be intentional with every step. The process showed me how important small details are when you are looking at a system that is trying to hide its weaknesses. My analysis changed when I started treating every piece of data as something that could matter later. That is what helped me slow down and make decisions based on evidence rather than just trying things until something worked.

Crocodile added more depth because it required me to understand service behavior and how small misconfigurations become full entry points. It pushed me toward a penetration testing mindset, but it also strengthened my network analysis skills because the entire attack path depends on reading the system correctly. If I misread a port, service, or response, the entire workflow falls apart. That type of thinking came directly from my classes where we learned why scanning is important and why understanding network behavior matters more than memorizing commands.

The Nmap Scan Procedure Documentation is the artifact that ties everything together. It shows my process, my command choices, and the steps I take to interpret results. A lot of people run Nmap without having a reason for what they are doing. Writing out the procedure forced me to slow down and think about why I choose specific flags and how I translate raw results into something useful. That was shaped by my coursework and by the emphasis on structured thinking in my degree program. It helped me see how disciplines like writing and critical analysis support technical work, because documenting my approach made the work cleaner and easier to replicate.

Scripting and Automation

Scripting and automation became one of my most valuable skills because it removes repetitive work and gives me more control over how I approach tasks. The artifacts for this skill include my Bash Ping Sweep Script, my Port Sweep with Service Mapping Script, and my Python Ping Sweep Script. Each one came from hands-on learning where I had to figure things out by testing, rewriting, and comparing results.

The Bash Ping Sweep Script taught me how to think logically about what I wanted the script to do. I wanted a lightweight way to see what was alive on a network before running anything heavier. Even though the script itself is simple, the process of building it made me think differently about how to automate tasks. It also helped me understand how much time can be saved with a tool that only takes a few minutes to write.

The Python scripts pushed me further. I had to think about flow, error handling, output formatting, and making the tool usable in more than one environment. When I first learned Python, I only focused on getting things to run. Over time, I learned how to build something that could be reused and understood by someone else. The process of scripting made me better at breaking down problems and solving them in a structured way. My coursework supported that by giving me a foundation in logic, analysis, and evaluating whether the output makes sense. That is not just a technical skill. It comes from the interdisciplinary side as well.

Automation matters in cybersecurity because so much of the work involves triage, reconnaissance, and repetitive tasks. These scripts gave me a way to speed up that process while understanding exactly what the tool was doing. It also helped me see how programming connects with networking, penetration testing, and broader problem solving.

Penetration Testing and Exploitation

Penetration testing is where my analytical work, scripting, and system thinking come together. This skill set developed naturally as I went through challenges, labs, and walkthroughs that required me to identify weaknesses and use them in a controlled way. The artifacts I selected show the type of work that reflects my growth. They include additional exploitation work tied to system enumeration, privilege escalation, and identifying how attack paths form when multiple small issues combine.

Penetration testing has always been interesting to me because it forces you to understand systems at a deeper level. You cannot just run a tool and call it a day. You need to know what the system is doing internally, how the network communicates, and where the pressure points are. The work I did in this area helped me improve my decision making, my patience, and my ability to move from theory to practical execution.

My classes played a big part in shaping this skill. Learning about threats, policies, secure network design, and risk assessment gave me context for why certain vulnerabilities matter more than others. Even the non-technical classes helped by improving the way I communicate and structure my thinking. When you break into a system during a lab, you still have to explain what happened and why it matters. That academic background helped me become more organized in how I approach penetration testing and how I document the results.

Conclusion

Looking back at my degree, the mix of disciplines is what made the biggest difference. I did not just learn technical material. I learned how to think through problems, document my work, and connect ideas from different fields. Courses like IDS 300W built a foundation for writing clearly and explaining technical ideas in a way that makes sense to someone else. Other

courses taught me how to apply those ideas inside real cybersecurity projects. That balance between writing, analysis, and technical practice helped me grow in a way that aligns with what employers look for in this field.

The artifacts I chose represent the skills I think are really important. They show my process, my growth, and my ability to take on real work. They also show how different disciplines supported each other. Networking helped my penetration testing. Scripting supported my analysis. Writing helped me understand what I was doing and communicate it. That combination prepared me for my career goals and clarified how I want to move forward in cybersecurity.

Being an interdisciplinary thinker matters because the problems we face are never just technical. They involve people, communication, design, planning, and strategy. This program helped me see that clearly. It shaped the way I approach my work and gave me the skills to handle challenges from more than one angle. That is what makes me ready for the field and confident in the path I am taking.