Jaden Medina

Electronic Portfolio, Old Dominion University

IDS-493

Professor Andrews

April 28, 2025

Introduction

During my time at Old Dominion University, I have been able to expand my knowledge and understanding of various concepts and ideas. Through this I have learned a lot of technical skills and knowledge, critical thinking skills, as well as communication skills which are all necessary for a successful career in cybersecurity. These skills were cultivated through a variety of term papers, course labs, and tasks completed at my internship. These skills have given me a greater understanding of what is to come in the future when I start my career.

The cybersecurity program at Old Dominion University is fast paced and accelerated however it causes all of the students to problem-solve and think outside the box to push through different issues and problems. As Students we are given the ability to take pieces from different disciplines and merge them together to have a cohesive yet better understanding of an issue. This in turn creates well rounded individuals who are better equipped to face the various cyber security issues we may face. An example would be how I have seen my writing skills improve and my critical thinking skills improve as I was tasked with writing very different yet complex papers on niche topics. All of my Artifacts/ evidence is proof of how important these skills are and how they are able to transfer over towards my goal of being a cybersecurity Analyst, cyber security specialist, or penetration tester.

Skill 1 technical skills:

Technical skills are baseline skills for any role in cyber security. The skills that I developed over the years have taught me to use industry standard tools and overall technical information, and how to react in

certain situations. These are shown through the various artifacts I have selected to showcase my technical skills.

Artifact 1:

The first artifact that i have chosen to showcase is, "Assignment #2 - Traffic Tracing and Sniffing" from my CYSE 301 course. In this assignment, I was tasked with monitoring and analyzing the network's traffic using Wireshark and various ethical hacking activities while on the virtual network. I learned how to capture network traffic during a "Ping test" during a brief browsing session. Afterwards I learned the roles of filers such as DNS and ICMP and how to isolate the traffic. Then I examined the credentials and other sensitive information that is changed between both Ubuntu and External Kali.

Artifact 2:

The second artifact chosen to represent my technical skills is the assignment, " Assignment 3: Sword vs. Shield" which I completed for my CYSE 301 course. This was one of my favorite assignments because it deals with both attacking and defending a network. I had to identify vulnerabilities and then I had to set up and apply the appropriate defences while using tools such as pfSense, Nmap, and Wireshark. For the sword part of the assignment, we used Nmap to perform active reconnaissance on the subnet, which were pfSense, Ubuntu, and the Windows Server. The goal of Sword was to teach us how to gather critical network information. While Shield switched the roles, focusing on the defence. This taught me how to use pfSense to put up firewall policies to secure the network against various attacks.

Artifact 3:

In this artifact I took a "ticket" which was assigned to me at my internship. While working for

Old Dominion University's ITS help desk I gained a wide array of skills and experience. On the

day of this ticket I was tasked with assisting a professor in her classroom with some technical

issues. I was dispatched to the room and had to go into the rack, a tower which holds the

technology in a room, and identify the issue. Once I identified the issue I had to reseed the piece

of equipment. I then completed the ticket. Understanding how a system works and more

importantly how to fix it is necessary for one's technical skills.

Critical thinking:

Critical thinking in the realm of sap security is very important. semi-professionals are required to

solve complicated problems, sometimes even time sensitive threats, issues, and errors. During

my time as an undergrad I have been given different opportunities to use critical thinking in the

realm of cybersecurity.

Artifact 1:

During my Cybersecurity, Technology, and Society course at ODU I learned about how

cybersecurity and technology fit into today's society. I chose to write this paper and use it for my

skills because it represents my critical thinking skills. I researched different examples of which

there was a need for cybersecurity. Weather for personal information, banking information, or

sensitive data used for work. This artifact showed I am able to find common weaknesses,

common vulnerabilities, and tricks users and organizations may face.

Artifact 2:

For artifact 2 I Chose my Journal entries for my 200t course. This gave me a view into how technology is used and integrated in society. These journal entries encouraged me to think outside the box and made me look at issues and questions from all different angles to gain a greater understanding. By forcing me to think critically I was able to expand on the technical, legal, ethical, and social ramifications of cybersecurity and technology in society.

Artifact 3:

For my third artifact under critical thinking I chose my paper, " Navigating the Ethical Landscape of Jailbreaking and Rooting Mile Devices in Today's Era of Digital Copyright." I chose this essay because a lot of the time users do not see the risks of jailbreaking a device or installing unauthorized third party programs on a device. Throughout this paper I navigated the fine line between the trade-off of a user's freedom and the difficulties of a damaged device.

Communication:

 Throughout my entire life I have always been an extroverted person. However limited I know how important being an extrovert or a person who loves to communicate will be when it comes to cyber security. Throughout this course we have learned different types of skills employers will be looking for.   The first skills that employers are looking for are called "hard skills". Hard Skills are any skills that can be learned and are needed for a Position. As seen throughout this reflection these are technical proficiency, knowledge of a programming language etc. However not everyone can possess "soft skills". Soft skills such as communication are necessary in cyber

security because without it cyber professionals will not be able to hold meetings, educate employees and protect and inform an organization of an attack or error. communication also has other less extreme uses such as building better employee to employer relationships, better teamwork and collaboration, and better relationships with the clientele.

Artifact 1:

The first artifact I have chosen for my communication skill is a speech I gave in my public speaking course. As a cyber security professional I know the benefits of having cellular and other devices in the home. However, when it comes to children the need and the benefits of these devices shift. This speech taught me how to gather information that was researched, compose it in a sense that is easy to relay and then deliver the speech to educate my peers and instructor on the risks of giving children of the age five and below devices.

Artifact 2:

The second artifact I have chosen for my communication skills is my research interdisciplinary essay on cybersecurity and accessible use policies. Throughout this paper I dove into the ethical battles between protecting a user's privacy and the saving security of an organization.

This artifact shows my ability to make informed decisions and choices and portray them in a light which is moral yet just.

Artifact 3:

My last artifact that I have chosen for communication is my term research paper on zero trust architecture and how they can be implemented with Windows operation systems. As most Enterprise and other organizations use Windows based systems to store, communicate and transfer information it is important that this information is not only protected.

Conclusion:

My experience and journey at Old Dominion University has been enriching and overall transformative. Throughout my coursework, Hands-On Labs internet experience and variety of my papers/research base assignments I have gained numerous technical, critical thinking and strong communication skills. All of which are necessary and essential for a successful cyber security. The artifacts that I have chosen reflect not only growth and development but a deeper understanding Of the coursework as well as real world experiences. whether it's configuring firewalls, solving complex problems, communicating cyber risks, or even analyzing Network traffic every experience that I've gone through has brought me alarm set closer to my goal of being a well-rounded staff security professional as of now I feel confident and prepared to pursue various roles such as a cyber analyst cyber Specialist or even a penetration tester.