This is the first project assigned to my Cybersecurity boot camp by Vanderbilt University and Trilogy (Jan 2021 – July 2021). This project, in many regards, was a culmination of the concepts learned and executed during the first three months of the bootcamp. The logistical goal of the project was to create a virtual network (VN) in Azure to include the following components: resources groups, Jump Box (firewall), web server, ELK machine (stack), load balancer, network security rules (NSG), docker containers, and a subnet. The functional goal of the project was to run a damn vulnerable web application (DVWA) through an ELK stack analysis server so we could learn, and witness firsthand, how to view various data sets, and graphical representations, of web traffic and vulnerabilities.

This was a challenging project for two primary reasons: (1) docker, .yml, and FileBeat scripts don’t always run as planned, (2) and setting network security rules can be complicated if the full scope of the VN’s functionality is not realized. The three primary scripts needed to make this project function as intended required several tweaks (edits) to produce the desired results = copious amounts of research and trial and error; both of which are phenomenal lessons in learning and failing forward. Also, creating network security rules, while fascinating and fun, was another challenge of head-throbbing proportions. While the majority of the rules required were straightforward, the absolute last rule needed to secure the connection between the Web-Server and the ELK Stack proved to be frustrating, although the final solution was extremely simple – a recurring theme in IT and networking.

The end result of the project taught me an age-old lesson about perseverance, learning through improved failing, and trusting the process. Excited to start working on the next project!