Daniel Akpovi

CYSE 368

Spring 2026

Professor Teresa Duvall

TA Joshua Russell

McDonald Army Health Center / Information Management Division

Reflection # 3

Third 50 Hours

In the third set of 50 internship hours, the main challenge remains the limited access that I have to the network system, especially the Palo Alto firewall. The fact that I had read-only access to the firewall, most of my work was to review requests to validate ports, source, and destination IP addresses, among others, before sending them to the appropriate team for the implementation via Siphon. Instead of getting discouraged by this limitation, I decided to create a home lab with pfSense and Tenable Nessus, thus getting the much-needed experience on the firewall configuration and network vulnerability scanning. This gave me the possibility to put into practice the concepts that I had been observing during my internship.

Creating a home lab gave me an eye-opening experience even before I started configuring my first set of firewall rules. I have to configure interfaces, networks, and ensure that traffic flows as it was supposed to. This reminded me of what I learned from the first set of 100 hours about the importance of network segmentation, and more specifically it gave me the chance to put into practice concepts that I had learned from theory in class. I had to think about

communication between systems: which ones would communicate with each other, the type of traffic that I would allow to pass via the firewall, and the consequences if I got the rules' order wrong.

The most impactful part of the experience was the freedom that I had to create the firewall rules and test the results of the firewall configuration with Nmap, Nessus, and various network testing tools. This involved the ability to deny access to the network resource based on the source and destination IP addresses, among others. It reminded me of the methodological approach that I had to adopt in evaluating access requests using Siphon at the workplace. After making changes, I use Nmap and Nessus to scan the devices to ensure that the changes did not expose a resource more than it was intended to. That made the experience feel a lot more real because it involved the creation of firewall rules and testing the impact it had on the security of the system. In addition, I was also able to test the network address translation (NAT) and port forwarding to get a better understanding of how the access from the external network gets to the internal resource and how a firewall that is not well configured may allow unauthorized access to internal resources. When the firewall did not allow access to the requested resource, I troubleshot to figure out the reason for the failure.

I was also able to further explore the network segmentation that I touched on earlier when I mentioned that I saw VLANs and ACLs as security measures rather than network design. I segmented networks within the pfSense firewall and allowed for movement between networks to further understand how a poorly configured firewall could allow unauthorized movement between networks.

Another component of this lab that I found to be helpful was the log and monitoring feature. In my previous reflection, I mentioned that SolarWinds made events more significant

once they were being measured against a baseline. This was also true with pfSense, where I was able to review the logs of the firewall and see the traffic that was blocked and the packet captured of the failed connections. I was also able to document any changes made to the firewall, the reason behind making these changes, and the result of these changes.

These last 50 hours were more comprehensive because I combined my internship responsibility with hands-on learning from my home lab. Although I still acknowledge the shortcomings of my position at MCAHC, I was also able to use my home lab as a way of furthering my knowledge of firewalls and vulnerability assessment, something I lacked prior to this lab. At the end of this time, I have improved my abilities in rule creation, segmentation, monitoring, troubleshooting, documentation, and basic vulnerability scanning. More seriously, however, I am more careful in making decisions surrounding the firewall as I realize the impact changes can have on the overall network.