Daniel Akpovi

CYSE 368

Spring 2026

Professor Teresa Duvall

TA Joshua Russell

McDonald Army Health Center / Information Management Division

Reflection # 1

First 50 Hours

My first 50 hours felt familiar and new at the same time. I work full-time as a network specialist, and I am counting my current role as my internship. So, the environment did not change. My mindset did. I now began to view my daily network tasks in terms of cybersecurity, and I paid attention to why each task is important.

During the few days of this internship, I discussed with Richard Trabbold, my supervisor and an experienced network engineer, what I should focus on during this first stretch. Richard stated the goals in a simple way. First, apply security basics during normal network work. Second, learn the tools and processes that people use in an actual organization. Third, develop an incident response and vulnerability work skill. Fourth, communicate well and make ethical choices, even when doing routine work. Hearing out the goals helped me make the connection between what I learned during my classes and real tasks.

Richard started with identity and access control. He explained how authentication, authorization, and accounting are important in our day-to-day work. He said a variety of factors,

including access rules, device logins and levels of privilege all influence risk. During these hours, I paid closer attention to who receives access, how access gets approved, and how access gets reviewed later. I also started to become interested in the question of who needs this access, and what happens if credentials get stolen. In the meantime, I was given some access that I did not have before, such as administrator's access to SolarWinds, submitter's access to Siphon, and Read-Only access to Palo Alto firewall.

Next Richard discussed segmentation. He has described segmentation as a safety barrier, not a networking style choice. VLANs, ACLs and routing decisions are used to limit movement around the network. And, when segmentation is kept clean, any problem will stay smaller. During these first 50 hours, I saw segmentation rules in a new light. I focused on scope, sequence of rules, whether rules were appropriate to real needs. I also observed the ease with which accidental over-permission can occur when credentials are not verified properly. This reminded me of an accidental SERVIN permission to a technician of the Automation Team, who has no business getting such permission. By the way, SERVIN is the platform used to control the authentication server here at McDonald Army Health Center (MCAHC).

We also touched on the topics of hardening and vulnerability management. Rich told me security work, so often, looks like boring discipline. Patch planning, firmware tracking, secure configuration baselines and back-up planning are all ways of reducing risk. This has pushed me to spend time going through configurations on some switches for consistency and checking documentation to see if there was anything I needed to change on switch configurations. No moment of drama occurred and that is what I prefer.

Richard also highlighted monitoring and incident responding. He opened my eyes on how logs are used as a timeline for accountability and troubleshooting. It is very important for time

sync to be consistent, as time inconsistencies slow down response time. During these hours, I was focused on building habits around log checks, alert follow up and writing down what I changed and why I changed it. I did not manage any major incident during this time, so I am not pretending otherwise. Still, I learned what good evidence looks like, and I learned how small clues add up.

Communication and ethics came up in every part of our talk, as Richard insisted on how important it is to be able to explain technical issues to non-technical personnel. He also reminded me to take privileged access as a responsibility, rather than a perk. I took that seriously.

After 50 hours I find that I am more focused. I want my next hours to include more practice on everything that we have discussed.