2/06/2025

Initial Thoughts

I would like to begin by noting that during the writing of this documentation I have not fully documented the completion of my automated SOC lab using wazuh, shuffler.io and theHive. The road block that has prevented me from completing this has been my personal laziness, finishing my last semester and the previous paranoia of doing port forwarding.

When I was creating the lab, I was stuck on the step of connecting a shuffler.io request to access my VM containing TheHive. I was uneasy about the notion of allowing open ports directly to my VM without protection. I went through the knowledge I did learn from university and personally thought of running a DMZ(demilitarized zone) since this would remove the need of worrying about outside devices trying to access my private network.

I was also introduced to the notion of hosting the Thehive instance on the cloud as it was intentionally done with the MyDFIR tutorial but instead of digital ocean it would be AWS as this was a topic I am currently learning for my last semester at uni. This optionally wasn't bad except for the fact I would have to pay for services I use when the free trial would run out and after doing the university labs on deploying an application on aws with load balancing and auto scaling, the $50 credit was being used at an incredibly fast rate, around $2-3 dollars a day, I know I didn't need these services but the idea of worrying about credits doesn't give me any ideas of freedom in this space if you get what I mean.

After consulting ChatGPT on what I should do, it gave me the option of reverse proxy where I would install it on the VM containing theHive and I would have to configure and validate that the information that is being received from port 80 and 443 from the outside would only be from shuffler.io, effectively allowing me to have access to the outside whilst protecting my theHive instance. There was also the idea of OpenVPN to tunnel to shuffler.io, but idea wouldn't work since I don't own shuffler.io to do the tunneling.

I then did some research and remembered that Shuffer.io is an open-source application. Thank goodness for open-source applications cause that meant I would be able to host this service on a VM machine and make sure that nothing will be exposed to the internet and that everything will be simulated on the VM's. I think I will take this path as it seems that Shuffler.io runs on docker and would mean it is lightweight.

Final thoughts

I like the idea of reverse proxying, funny enough I was speed running through the google cybersecurity professional certificate, and they did have a run through proxy servers and the fact that I'm getting some knowledge on this sphere is interesting enough, I do feel a sense of satisfaction that I am getting more knowledgeable should I continue this route.