

DAILY JOURNAL

IMPORTANT INFORMATION

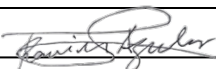
- INCLUDE TASK ASSIGNMENTS OR MOVEMENTS, REFLECTION ON THE DAY'S NEW LEARNING, ACCOMPLISHMENT, CHALLENGES FACED AND HOW YOU RESPONDED, OBSERVATIONS AND RECOMMENDATIONS ON THE IMPROVEMENT OF SYSTEMS / OPERATION / MANAGEMENT, ETC.
- SCANNED COPIES OF THIS FORM SHALL BE SUBMITTED ON A WEEKLY BASIS THROUGH APPROVED LMS.
- HARD COPIES OF THIS FORM SHOULD BE COMPILED AS PART OF THE STUDENT'S PORTFOLIO.

DATE	May 16 - May 20 2022	AREA ASSIGNMENT	ATA
TASK	Becoming a Raspi Developer & Becoming an IT Security Specialist	SHIFT/TIME	8:00 AM - 5:00 PM

May 16 I continued doing the becoming a raspi developer module where I learned the different functionality and use of each GPIO pin of raspi. I also learned how to control this pins to power various electronic components like LEDs and tact switch. I did not have a hard time in this part since the idea is basically the same in Arduino where you send 1s and 0s to turn on and off accordingly, the only different is that in raspi we need to use python in order to control the GPIO. For the last part, I was able to learn how to interface Pi cam to the raspi and take picture using command line and automate taking picture using a script but I wasn't able to replicate this since the camera that I have does not interface with the raspi. Lastly, I learned how to create a basic alarm system using a relay switch and a motion sensor, again I was not able to replicate this one since I do not have access to a motion sensor.

May 17 - May 20 I started the IT security specialist module, the first few part basically served as a review of my prior knowledge on IT security which is more about common practices in keeping information safe and basic risk management like identifying vulnerabilities and considering potential threat attacks. The next part is where things became interesting, I learned about threat modeling wherein we create a visualization of our entire system and network architecture and then we identify the potential entry points and list of attacks that can be done, then we can now manage those risk by putting a safeguard in the places that we identified as potential entry points. I also learned about SSL/TLS and how they work in the background like how they are validated using a serial number that are issued by the certificate authority. The next is about different activities and practices that we can do to manage vulnerabilities like updating windows, enabling core isolation that prevents an attack to insert malicious code in high-security processes, enabling isolated browsing by installing microsoft defender application guard to protect us while browsing the internet, and enabling egress filtering in our firewall to prevent the sending of data gathered through keylogger if we are infected.

I also learned how to apply AI techniques in cybersecurity like classifying problems to determine whether a code contains scripting vulnerabilities by mapping data into categories, how to use clustering techniques to find patterns in incoming internet traffic to our web server so that we can distinguish bot from real users. All in all this module is more about on concepts rather than using a specific tools to enhance security and better mitigate risks.


TRAINEE'S SIGNATURE