Group Project Analysis Document

Something that worked well was the script that analyzed the log files. The script would read the log files and then parse them to find relevant data such as login attempts during off hours, authentication failures, and unauthorized port access. This allowed us to find any suspicious log activity, which could possibly highlight if the system was being breached or how the attacker is attempting to log into the system. Having a log system that functions effectively also allows for the proper response to any incident, should any occur. Log files are able to give a timeline of events that can be used to identify the source of the attack and allow for the company to take the proper mitigation steps. The UML, activity and use-case diagrams, helped with providing visual representation on how the system operated and the roles of various actors; successfully allowing the team to clean up and improve the system.

A challenge that we had encountered was getting the automatic alert system to properly notify the company when an anomaly was detected. False positives were the biggest problem, with the alert system sending out alerts for legitimate activities. This was somewhat caused by bugs in the code, but was mostly due to the lack of threat analysis done by the company beforehand. This was all a result of the team lacking experience with python programming, making things harder to understand and work around. However, as we worked through the issues, we were able to learn more about python and overcome any problems we had. The team was also unfamiliar with using Git, which resulted in a few issues with merges, sharing code, and ensuring that all members were able to access the code.

We were able to detect several vulnerabilities and trends due to the system's data analysis and system monitoring. As we mentioned briefly before, our log monitoring system was a big part of identifying any potential security threats or risks, specifically looking out for the failed login attempts and system overuse. The results indicated that there were possible brute-force attacks or unauthorized access attempts. Our system monitoring, involving the CPU and memory, also showed patterns of system stress during times of suspicious activity. These results show there may be some malicious activity present in the system, and allow the team or company to highlight certain areas that need improvement. Thus, resulting in a system that has a lower number of risks and vulnerabilities.