CYSE 130 Group 5

Project Analysis

Throughout the project timeline, there were not many portions that caused issues. The project can be broken down into 4 distinct parts, only one of which brought about challenges. The first portion of the project consisted of the construction of requirements. To do so, our team had to draft concise questions to locate the critical areas within the company. After doing so, the team had determined that the best area to focus on was login security. UML diagrams were drawn up to understand the overarching goals of the project. There was only one modification made to the UML diagrams during the project lifespan: the addition of emailing the proper authority of an unauthorized or suspicious login.

The team then began working on a script to analyze the log files. The script would read through the log files searching for keywords such as, “blocked” or “error,” and record the time, IP address, and any other information about that event. The suspicious logs could then be viewed by an administrator at any time. The next step was by far the easiest and involved setting up an automation of the script. To save on efficiency, the log analyzer would not check every login as they were attempted, but instead do a check of every log within the past hour, every hour. This was achieved by simply adding a repeat function into the python script. The final portion of the project was to send an email to an authorized admin when the analyzer found any suspicious activity. This task posed difficult for the team as they were unable to successfully link the python script to an email. The problem was eventually resolved, and the emails were successfully sent and received. Ultimately, the project concluded smoothly due to a very streamlined approach with plenty of resources at the team’s disposal.