CYSE 130 Group 5

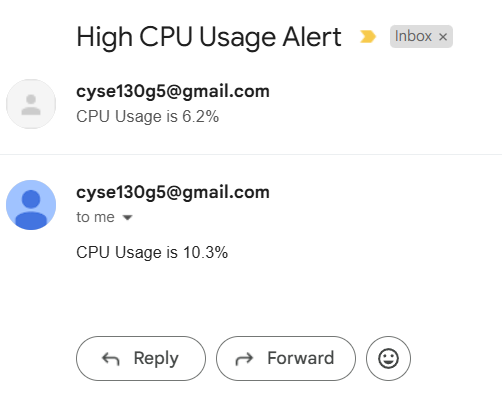
Automation Assignment Report

For clarity’s sake, we transferred our script over in code and markdown blocks that matched the detailed instructions given by Professor Paes. Seeing as we do not have any actual company’s data, we mostly used dummy logs and ip addresses for our scans and logs.

Starting from the top of the python notebook we submitted, we used the Windows\_2k.log\_structured.csv document as our fake company logs, scanning the document for any sort of repeated failed attempts or other warnings present in the logs. We then wrote all suspicious logs to a new text document.

In the next section, we collected actual system data, opting to just use high CPU usage as our suspicious activity. We logged the high CPU usage to a new text file, and then set up an alert email using a dummy gmail account that we created for our group with an app password we generated. Pictured below is the result of running the code with CPU usage higher than 5% designated as suspicious for the purposes of testing our code.

A screen shot of a computer program

Description automatically generated

After running the above script, we changed the CPU usage number back up to 90 for the sake of submitting the assignment.

Finally we used the provided scripts in the word document after setting up nmap and scapy to scan for vulnerable ports using namp, as well as monitoring network traffic using scapy.