Lab 8 - Visualizing the Data

The objective of this lab is to work to understand the data that is generated by our system (syslog) and OSSEC logs. We do this by by bringing that information into a data aggregator, in our case splunk, and use this as our first entry into this amazing world of data visualization.

Getting Started and Using Splunk

What is splunk? You can consider it a database that allows you to search for any part of the information that was uploaded (somewhat like google), classify data, and build dashboards. Having the data is only the first part of any problem, raw data needs to be converted to actionable intelligence. Take a minute and review some of the blogs and manuals listed below, as well as any others you find in your search (Note that we are using splunk 6.5.6):

- https://docs.splunk.com/Documentation/Splunk/6.5.6/Viz/CreateDashboards
- https://www.splunk.com/view/SP-CAAAGXD
- https://helgeklein.com/blog/2014/09/splunk-work/

To log onto the splunk server, connect to **cyber.moboard.com/splunk**, your username (mAlpha) and password is **changeme1**.

Problems

1. Create at least **four** Splunk dashboards to view your data, while there are no specific requirement for this problem, you need to put in some thought as to the information you want to search for, and it should provide information that you believe would be useful to a Cyber, IT, or Security specialist. Note that at least one of the dashboards should be focused on security events coming from the outside internet, and at least one should be focused on events that occur on your system.
2. **What data do you want to visualize**, **Why did you decide to build the ones you did**, and **Why do you believe that the dashboard would be useful?** Provide commentary for each of your dashboards.
3. You have 3 weeks to complete this lab, so expectations are high.

What to submit

When you have completed the lab **post all requested materials to your webpage**. Then, submit the link via email to your Professor.

The email subject line should be SY402 [Section Number] Lab [X]: Title of Lab (e.g., SY402 1111 Lab 8: Visualizing the Data). Email sent with a different subject line will reduce the overall grade by 5 points.

The web page link(s) should include:

1. (Attach) screenshots of **each** Dashboard that you built along side the explaination for each