CSC841 Lab05- Graylog

Centrally locating network information is essential to any environment where threats may present themselves. Many platforms exist for this purpose, some vendor specific, some open source, some commercial, and others freely available. We'll explore that option for centrally locating our 802.11 management frame data.

Overall Goals

We will enhance our tool to generate JSON formatted data that can be shipped to an external log management tool. Once we have aggregated enough data, we will begin to formulate the baseline for what security implications may exist on the network and hunt for threats that would not be detected from traditional network sensors.

A Graylog VM is provisioned for each student; bring the VM online and configure it to capture data from your Python tool. The default console credentials are dsu/Password1!

You may need to launch Graylog via docker (*sudo docker compose up* from the home directory) Everything should be accessible via your web interface once Graylog is online (run the command *ip a* to determine the address assigned to your ens160 interface). You should be able to access Graylog via: http://IP_Address:9000

The default web interface's credentials are: admin/Password1Bang

Basic Requirements

Building upon your tool from Lab05, enhance it to meet the following requirements:

- Modify your python tool to send the JSON formatted data to Graylog
- Capture and parse both association and authentication requests/responses 2.4 gHz
- For all frame types, determine the signal strength and include it
- Aggregate your data captured from each frame into a single JSON object
- Configure a Graylog instance to capture and parse your JSON packets you generate

Submission

For full credit on this assignment, submit your tool for capturing, parsing, formatting, and shipping the 802.11 frame information as well as a screenshot showing you have successfully parsed the data inside of your Graylog instance.

Tips

Everyone has their own Graylog server deployed, you may check the IP address to ensure that you're logging into your own.
The username/password for the shell of the Graylog machine are: dsu/Password1!
The username/password for the web interface of graylog are: admin/Password1Bang