**Threat Hunting Report**

By Khosyi Yoga

**Unique IP Address**

The unique IP address is filtered through Python script. Firstly, the rows in the logs are loaded and lists all the IP using regex that will search patterns as such xxx.xxx.xxx.xxx, where number of digits can be from 1-3, whilst it will accept all numbers. The list will then be filtered using Counter to select only distinct values, and omit the IP address that starts with 172 (host). The list of IP is then written to CSV file.

**Unique IP Address and Frequency**

The same method is used as above, but added the hit frequency per IP address. The country origin is not available within the log file hence it is not included.

**Activity list per IP Address**

The first step is to list all unique IP address within the log file, then to search through the file for every activity per IP address listed. The activities are then written into single CSV file per IP address. The method works, but due to the size of the log file, only some CSV is generated (it takes too long to generate all the files), but should have proven the logic.

**SQLi Detection**

The activities within the log file is searched for SQL Injection by searching the keyword “SELECT” (ignoring case), through Python script. Though it seems generic, but it is quite effective as it is relatively obvious. As can be seen in the result, there are few SQL injections using this method. The script however, is not as effective as it should be, because the word “SELECT” should only match if its found as a whole word.

**RFI Detection**

The detection is done by searching for the keyword “file=”. In my short time of research, it is found that RFI usually includes file from a remote source, and I have concluded that the chosen keyword can point out RFI activities.

**Web Shell Detection**

The web shell detection is done by searching for the keyword “passwd”. It is commonly used to gain access to the web shell by modifying the HTTP header. As tested, there are a few trials from the same IP address by using this method.