User Guide

LogAnalyzer

Pre-Installation

1. geolite2

   For getting a country information from IP address, we need geolite2

   pip install maxminddb-geolite2

2. tqdm

   tqdm instantly make loops show a smart progress meter

   pip install tqdm

How to use

python ApacheLogAnalyzer.py (log file path)

For example, 'python ApacheLogAnalyzer.py ./CTF1.log'

Then, you will get following files and directory.

1. SimpleIPList.csv
   - Unique IP address are in lines
2. DetailIPList.csv
   - Unique IP address with country and number of hits are in lines
3. Activity
   - Activity is directory and there are many (unique IP).csv files in Activity. Each csv files have activity which is consist of W3C extended log format fileds per unique IP address.
4. sqli_list.csv
   - It consists of suspicious lines as SQL injection.
5. rfi_list.csv
   - It consists of suspicious lines as Remote File Inclusion.
6. webshell_list.csv
   - It consists of suspicious lines as web shell
7. exception.txt
   - If some line is not matched with W3C extended log format, the line is saved in exception.txt