Pcap Analysis with ELK stack
Documentation

Folder Structure:

1.pcapfiles

- This folder contains the pcap files

2.decodedfiles

- This folder contains the json files

3.tempdecodedfiles

- This folder is for intermediate processing (will be act as temporary buffer while pcapfolder_watcher.py script in process)
- (note : dont delete this folder)

4.logs

- This logs folder will save the logs (if any failures it will save the exception in txt file)

Repository consists of following files

1.simulator.py

This file that is a .pcap file generation script that simulates the mitigation process py generating random pcap files per second and put that generated pcap file to the **"pcapfiles"** directory

2.globaldata.py

The globaldata.py python file that stores the common data that will be used in all watchers
(if you want to change the name of directory ,You can change here and its completely optional)

3.pcapfolder_watcher.py

- The pcapfolder_watcher.py script that is one of the watchers that will keep track the activities in the **"pcapfiles"** directory
- If any new file is created in the **pcapfiles** directory this watcher will be triggered and the generated .pcap file will be decoded using tshak and the generated json file will be transformed to the **"dcodedfiles"** directory

4.Logstash.conf

-the logstash.conf file is a logstash configuration file that just parse the the necessary details from the file name and that read data will be pushed to elasticsearch

---

OPTIONAL script for json watcher in pythonic way (not needed)

4.jsonfolderwatcher.py

- This jsonfolderwatcher.py script that is one of the watchers that will keep track tha activities in the **"decodedfiles" directory**
- If any new file is created in the **decodedfiles directory** this watcher will be triggered and the newly came json file will be uploaded to elasticsearch

---

Steps to RUN

Step 1:
Run pcapfolder watcher

- **python pcapfolder_watcher.py**

Step 2:
Run jsonfolder watcher
(open another terminal tab and set your current directory as logstash folder and run the following)

- **bin/logstash -f logstash.conf**

NOTE: (change the directory path of json folder which should be watched by the logstash.conf in the logstash.conf file before running it)

Step 3 (optional)
Open another terminal tab and run simulator if need
(the simulator that generates pcap file per second)

- **python simulator.py**

Python version 3.6

Packages to be installed
1.pip install elasticsearch(if you use the optional jsonfolder watcher , you should have the elasticsearch package ,otherwise ignore)

2.pip install watchdog (for logging the events of the particular folder)(needed)

3.pip install scapy(if you want to use simulator.py)