Project: Network Forensics

Synopsis

1) Objective:

- Analyze a PCAP file to determine (by plotting on graph) source IP address which has sent maximum amount of traffic to the destination IP address.
- All IP addresses which have sent traffic to the destination IP address will be checked against the blacklist file to determine if any of them are malicious.
- Plot malicious IP addresses and the corresponding number of packets sent by that address.
- Plot all Source and destination IP address pairs.
- If traffic sent to a destination port is above a certain threshold as set by the user, interpret as a suspected DDOS attack.
- Plot malicious IP addresses on Google Earth.

2) Visualization:

- There are 6 visualization files.
- Input for each file is generated by the python program
- Visualization files:

1. allip.html – plots each IP address with its sum total of packets- combination all packets sent/received
2. malip.html – plots only IP addresses present in blacklist file along with sum total combination all packets sent/received
3. SrcDst.html – plots all source to destination traffic and number of packet exchanges between them
4. DOS.html – plots suspected DDOS attack to particular source – destination pair along with number of packet exchanges between them
5. dport.html – plots traffic received by each destination port
6. sport.html – plots traffic sent by each source port

3) Google Maps:

- User can generate a KML file which can be used to plot malicious IP addresses on Google Earth or Google maps.

4) User Inputs:

1. .pcap file
2. Blacklist file
3. Geolite database (http://dev.maxmind.com/geoip/legacy/geolite/)--[optional]
4. Threshold value over which DDOS suspected [optional]
5. Port number on which DDOS attack suspected [optional]

4B) Required Files

1. Path of .PCAP file
2. Path of blacklist file
3. If KML file output is desired path of Geolite database is expected
4. If you want to check for suspected DDOS attacks port number and threshold limit is expected

5) Output

1. KML file which can be used to plot location of malicious IP addresses on Google Earth.
2. Data.tsv files for html files described above for visualization
3. Suspected DDOS attack with source and corresponding destination IP address on the screen

6) Extra work done:

1. Visualization of traffic received by source and destination ports
2. Identifying DDOS attack
3. Visualization of packets sent to destination port during the DDOS attack

7) Assumptions

1. Traffic received by destination port above a certain threshold is assumed as a possible DDOS attack
   This may not be necessarily true, but if a certain port is experiencing traffic over 10,000 packets we might want to investigate further
2. All source IP addresses which are investigated for DDOS attack have been added to the list of malicious IP address.
   This again may not be necessarily true.

8) References

1. www.irongeek.com
2. r/netsec (https://www.reddit.com/r/netsec)

3. r/ computerforensics (https://www.reddit.com/r/computerforensics)
4. Udacity (https://www.udacity.com/course/ud507)
5. http://d3js.org/