Tobby Lie
CSCI 4742
October 1, 2019
Homework 3

CODE:

Lie_Port_Scanner.py

For my port scanner code it is exactly like the code we had implemented for lab 1 except it only utilizes tcp connection. Aside from that it also asks the user for input for the time interval to use in seconds to respect between connections.

Lie_PS_Detector.py

For my port scanner detector code I had a total of 5 threads. One thread for detecting connections and storing a tuple of (src_ip, dest_ip, dest_port) in a dictionary in order to ensure they are first-contact connections. The second thread is for throwing out all elements in the dictionary that are have been stored for more than 5 minutes, this function returns a list of keys for elements in the dictionary that need to be removed. The third thread is used for checking at each second interval the fanout calculations for connections per second. The fourth thread is used for checking at each minute interval the fanout calculations for connections per minute. The fifth thread is used for checking at each five minute interval the fanout calculations for connections per five minutes.

LAN SETUP:

The machine utilized for this assignment was a MacBook Pro 2019. VMware Fusion 11.1.1 was utilized. In VMware Fusion preferences, one can under Network settings, add a custom network. I did this and created vmnet2 which was Host-only. The subnet ID was 192.168.10.0 and subnet mask was 255.255.255.0. This is how I created a private VLAN. Running ifconfig in command line in "Kali_VM_1" let me know that my inet was 192.168.10.165. I then cloned this VM and created "Kali_VM_2" which was also on vmnet2. When running ifconfig in "Kali_VM_2" I got an inet of 192.168.10.178.

SCREENSHOTS IN ZIP FILE:

There are a total of **seven** screenshots included for this assignment assuming we respect the waiting time after each two consecutive connections:

5Min_Detection_0.01 - Port scanner detected after 5 minutes at wait time of .01 seconds.
Min_Detection_0.01 - Port scanner detected after minute at wait time of.01 seconds.
Sec_Detection_0.01 - Port scanner detected after second at wait time of .01 seconds.
5Min_Detection_0.5 - Port scanner detected after 5 minutes at wait time of .05 seconds.
Min_Detection_0.5 - Port scanner detected after minute at wait time of .05 seconds.
5Min_Detection_1.0 Port scanner detected after 5 minutes at a wait time of 1.0 seconds.
Min_Detection_1.0 - Port scanner detected after minute at wait time of 1.0 seconds.

* No other screenshots included as no other port scanners detected for any other times with respect to time mentioned in assignment description.

DISCUSSION:

1ms:

One connection between waiting times:
Port scanner is **detected** for **each time interval**. It is detected at every second because there are 1000 connections per second which is well over 5. It is detected at every minute because there are 1000*60 = 60000 connections per minute which is also well over 100. It is detected at every five minutes because there are 60000*5 = 300,000 connections per five minutes which is well over 300.

Two connections between waiting times:
Port scanner is **detected** for **each time interval**. It is detected at every second because there are 2000 connections per second which is well over 5. It is detected at every minute because there are 2000*60 = 120000 connections per minute which is also well over 100. It is detected at every five minutes because there are 120000*5 = 600,000 connections per five minutes which is well over 300.

0.5s:

One connection between waiting times:
Port scanner is **detected** for **minute** and **five minute** intervals. It is not detected for each second as there are only 2 connections per minute which is in fact not greater than 5. For every minute that passes there are 120 connections which is over 100. For every five minutes there are 600 connections which is over 300.

Two connections between waiting times:
Port scanner is **detected** for **minute** and **five minute** intervals. It is not detected for each second as there are only 4 connections per minute which is in fact not greater than 5. For every minute that passes there are 240 connections which is over 100. For every five minutes there are 1200 connections which is over 300.

1s:

One connection between waiting times:
Port scanner is **undetected** for **all intervals**. For every second that passes, there is only one connection which is not greater than 5. For every minute that passes, there are only 60 connections which is less than 100. For every five minutes that pass, there are only 300 connections and this is close but does not exceed 300 which means the scanner is still undetected.

Two connections between waiting times:
Port scanner is **detected** for **minute and five minute** intervals. For every second that passes, there are only 2 connections which is not greater than 5. For every minute that passes, there are 120 connections which is greater than 100. For every five minutes that pass, there are 600 connections which is greater than 300.

5s:
One connection between waiting times:
Port scanner is **undetected** for **all intervals**. For every second that passes, there are no connections. For each minute that passes, there are only 12 connections. For each five minutes that pass, there are only 60 connections.
Two connections between waiting times:
Port scanner is **undetected** for **all intervals**. For every second that passes, there are no connections. For each minute that passes, there are only 24 connections. For each five minutes that pass, there are only 120 connections.

10s:
One connection between waiting times:
Port scanner is **undetected** for **all intervals**. For every second that passes, there are no connections. For each minute that passes, there are only 6 connections. For each five minutes that pass, there are only 30 connections.
Two connections between waiting times:
Port scanner is **undetected** for **all intervals**. For every second that passes, there are no connections. For each minute that passes, there are only 12 connections. For each five minutes that pass, there are only 60 connections.

*** It was a little difficult to see results for the 0.001 seconds waiting time interval so I included screenshots for 0.01 second waiting interval as it was easier to retrieve results from this. This means that for every second that passes, there are 200 connections, for every minute that passes, there are 12000 connections, for every five minutes that pass, there are 60000 connections which means that a port scanner is detected at each waiting time. Knowing this, we can be certain that at an even more minuscule waiting time such as 0.001 seconds that a port scanner would certainly be detected for all time intervals as well.**

ASSUMPTIONS:

- It is assumed that for port scanners detected in a second interval that it is not possible to get the average connections per minute or five minutes aside from extrapolating this information from the average per second calculations, this is why for fanout per second I decided to omit statistics that pertain to minute and five minutes. The same logic goes for minute fanout and how five minute is not known unless with extrapolation.

- No screenshots are included for the waiting times of 1s, 5s, 10s. The way that this problem was defined, meaning 5 connections per second, 100 connections per minute and 300 connections per five minutes means that for the waiting times mentioned, there are no fanout calculations that apply as there are no port scanners that are detected.

- The results in the screenshots are not perfect due to delay even after incorporating multithreaded programming. The results mentioned above are in theoretically perfect conditions.