Status Report
3/23/2023
TEAM RAD
Real-time Anomaly Detection

This Week’s Achievements

- Test SageMaker model with testing and validation data and recorded results automatically to S3 bucket csv file

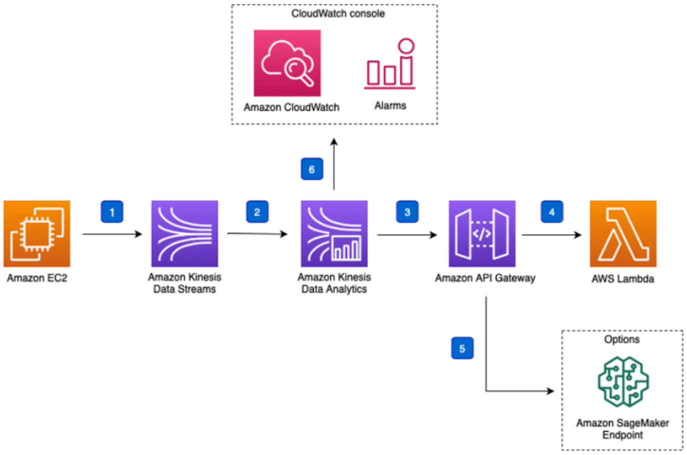
This Week's Goals

- Convert data preprocessing and endpoint invoking to a lambda function.
- Set up Scapy packet data to stream to kinesis firehose, to both store and send to the lambda function.
- Test neutral network traffic against the endpoint
- Completed one “Evil” simulation machines

Overall Goals

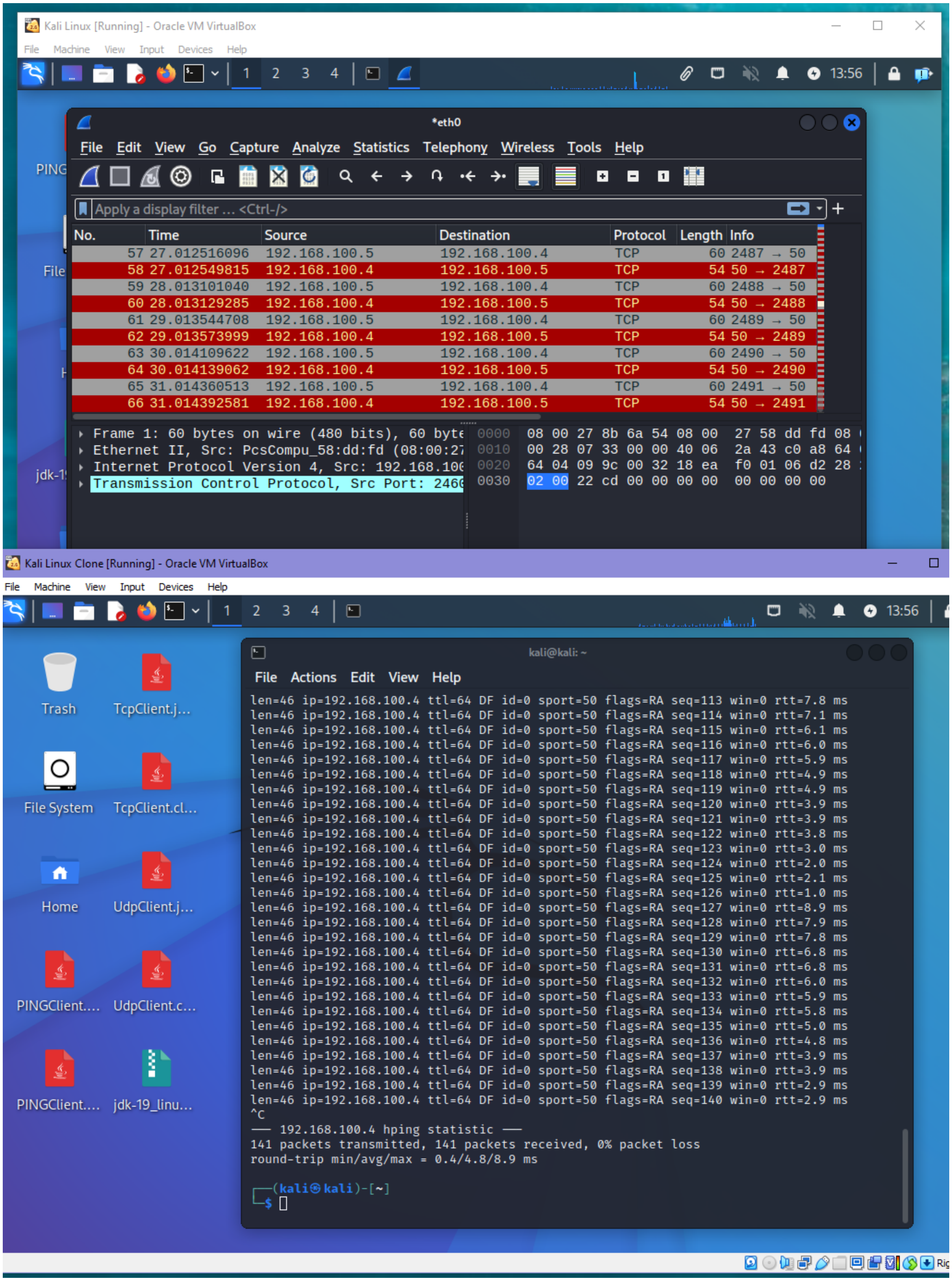
- Implement packet capture with python Scapy and output data as CSV string buffer
- Finish code for more VM “Evil” simulation machines

Upcoming Logic for data stream implementation



Instead of EC2 generating random data for our model, our data will come from our VM environments and Scapy streaming data directly to kinesis to both collect and run our AWS lambda function on it. The lambda function will both format and then subsequently run inference on our hosted ML endpoint, the ML model will automatically store the result which then can be sent to AWS kinesis analytics or another analytical or notification service.
https://docs.aws.amazon.com/pdfs/solutions/latest/streaming-data-solution-for-amazon-kinesis/streaming-data-solution-for-amazon-kinesis.pdf#solution-overview

Simulated SYN flood Attack


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
13:56
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Kali Linux Clone [Running] - Oracle VM VirtualBox
Trash
TcpClient.j...
File System
TcpClient.cl...
Home
UdpClient.j...
PINGClient....
UdpClient.c...
PINGClient....
jdk-19_linu...
kali@kali: ~
File Actions Edit View Help

No.	Time	Source	Destination	Protocol	Length	Info
57	27.012516096	192.168.100.5	192.168.100.4	TCP	60	2487 → 50
58	27.012549815	192.168.100.4	192.168.100.5	TCP	54	50 → 2487
59	28.013101040	192.168.100.5	192.168.100.4	TCP	60	2488 → 50
60	28.013129285	192.168.100.4	192.168.100.5	TCP	54	50 → 2488
61	29.013544708	192.168.100.5	192.168.100.4	TCP	60	2489 → 50
62	29.013573999	192.168.100.4	192.168.100.5	TCP	54	50 → 2489
63	30.014109622	192.168.100.5	192.168.100.4	TCP	60	2490 → 50
64	30.014139062	192.168.100.4	192.168.100.5	TCP	54	50 → 2490
65	31.014360513	192.168.100.5	192.168.100.4	TCP	60	2491 → 50
66	31.014392581	192.168.100.4	192.168.100.5	TCP	54	50 → 2491

```
› Frame 1: 60 bytes on wire (480 bits), 60 byte
› Ethernet II, Src: PcsCompu_58:dd:fd (08:00:27
› Internet Protocol Version 4, Src: 192.168.100
› Transmission Control Protocol, Src Port: 2460
```

```
0000  08 00 27 8b 6a 54 08 00  27 58 dd fd 08
0010  00 28 07 33 00 00 40 06  2a 43 c0 a8 64
0020  64 04 09 9c 00 32 18 ea  f0 01 06 d2 28
0030  02 00 22 cd 00 00 00 00  00 00 00 00
```

```
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=113 win=0 rtt=7.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=114 win=0 rtt=7.1 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=115 win=0 rtt=6.1 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=116 win=0 rtt=6.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=117 win=0 rtt=5.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=118 win=0 rtt=4.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=119 win=0 rtt=4.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=120 win=0 rtt=3.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=121 win=0 rtt=3.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=122 win=0 rtt=3.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=123 win=0 rtt=3.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=124 win=0 rtt=2.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=125 win=0 rtt=2.1 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=126 win=0 rtt=1.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=127 win=0 rtt=8.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=128 win=0 rtt=7.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=129 win=0 rtt=7.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=130 win=0 rtt=6.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=131 win=0 rtt=6.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=132 win=0 rtt=6.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=133 win=0 rtt=5.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=134 win=0 rtt=5.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=135 win=0 rtt=5.0 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=136 win=0 rtt=4.8 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=137 win=0 rtt=3.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=138 win=0 rtt=3.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=139 win=0 rtt=2.9 ms
len=46 ip=192.168.100.4 ttl=64 DF id=0 sport=50 flags=RA seq=140 win=0 rtt=2.9 ms
^C
--- 192.168.100.4 hping statistic ---
141 packets transmitted, 141 packets received, 0% packet loss
round-trip min/avg/max = 0.4/4.8/8.9 ms

┌──(kali㉿kali)-[~]
└─$ 
```