Status Report
3/16/2023
TEAM RAD
Real-time Anomaly Detection

This Week's Achievements

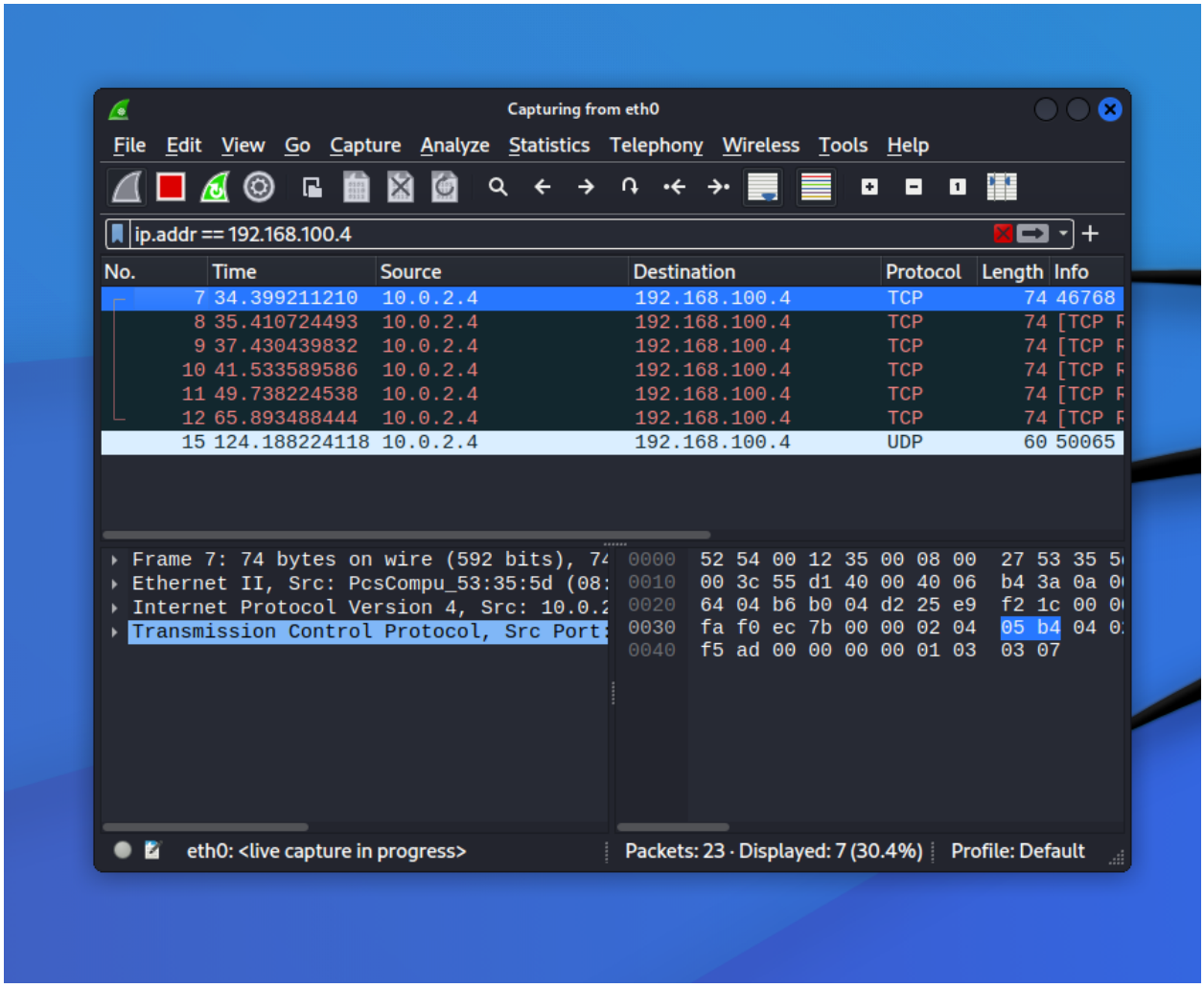
- Created SageMaker Notebook instance, model configuration and endpoint configuration
- Uploaded updated SageMaker tar.gz file and generate functional endpoint for SageMaker inference
- Created more neutral network traffic, this includes a continuous flow of TCP and UDP traffic going between Server and Client

This Week's Goals

- Finish data preprocessing in SageMaker to format incoming data
- Test data against the SageMaker inference endpoint (what are our real-time metrics?)
- Test neutral network traffic against the endpoint

Overall Goals

- Test SageMaker model with testing and validation data and record results to S3 bucket
- Implement packet capture with python Scapy and output data as CSV string buffer
- Finish code for VM "Evil" simulation machines
- Find how much friendly traffic is suitable for testing


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.100.4
No. Time Source Destination Protocol Length Info
7 34.399211210 10.0.2.4 192.168.100.4 TCP 74 46768
8 35.410724493 10.0.2.4 192.168.100.4 TCP 74 [TCP
9 37.430439832 10.0.2.4 192.168.100.4 TCP 74 [TCP
10 41.533589586 10.0.2.4 192.168.100.4 TCP 74 [TCP
11 49.738224538 10.0.2.4 192.168.100.4 TCP 74 [TCP
12 65.893488444 10.0.2.4 192.168.100.4 TCP 74 [TCP
15 124.188224118 10.0.2.4 192.168.100.4 UDP 60 50065
Frame 7: 74 bytes on wire (592 bits), 74
Ethernet II, Src: PcsCompu_53:35:5d (08:
Internet Protocol Version 4, Src: 10.0.2
Transmission Control Protocol, Src Port:
0000 52 54 00 12 35 00 08 00 27 53 35 5
0010 00 3c 55 d1 40 00 40 06 b4 3a 0a 0
0020 64 04 b6 b0 04 d2 25 e9 f2 1c 00 0
0030 fa f0 ec 7b 00 00 02 04 05 b4 04 0
0040 f5 ad 00 00 00 00 01 03 03 07
eth0: <live capture in progress>
Packets: 23 · Displayed: 7 (30.4%)
Profile: Default