Large pcap file link: <https://archive.wrccdc.org/pcaps/2024/33/wrccdc.2024-02-17.104826.pcap.gz>

**Measurement process**:

* Time and errors/warnings:

Snort provides them.

* %cpu and %mem usage:

They are measured using the ps command and logging it every 0.001 seconds for more accurate results

while true; do

    ps -o pid,%cpu,%mem,cmd -C snort >> ps\_log.txt

    sleep 0.001

done

Output (every 0.001 seconds):

    PID %CPU %MEM CMD

  11566  0.0  0.2 snort -c /home/snorty/snort3/etc/snort/snort.lua --talos -r wrccdc.2024-02-17.104826.pcap

...

**Results**:

* Time: 2.116 seconds (~76k packets/s)
* %CPU and %mem are plotted below:

A graph with a red line

Description automatically generated

* Errors/warnings:

There aren’t any major error messages. The only notable warnings are:

* + Bad checksum packets (bad\_tcp4\_checksum: 34580)
  + Discarded packets (discards: 34580 (21.279%))

Optimization actions:

To improve the efficiency of the snort we can optimize the rules that are checked for each packet. For instance, rule 11000002 (Port scan packet rule) is checked 30839 but isn’t matched for any of them in this traffic. This could be because of the large array of ports it has to check [HTTP, HTTPS, SSH, TELNET, FTP, DNS, RTSP, SQL, RDP, MQTT], so reducing it or matching any dst\_port could have better results.

The next step is to try and match the flow types and the content of the packets (assuming it is the same as instructions provided). For example adding the “flow: to\_server” skips over packages that aren’t to the server which will not be malicious.