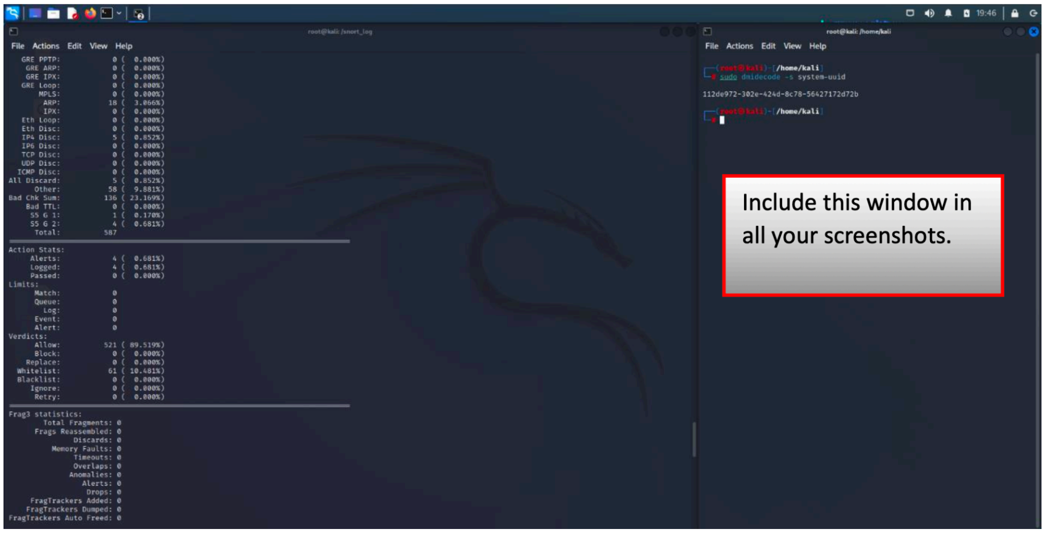
CS432/532 – Computer and Network Security
Spring 2024-2025 – Snort In-lab assignment

- No collaboration is allowed. You are not allowed to ask for and get help from your classmates. Any such activity will directly result in failure in this lab.
- All cell phones must be totally switched off if you are not using them as a modem.
- Any type of online communication via email, DM, WhatsApp, etc., with another human being will be treated as plagiarism.
- To complete the following exercises, you need to have Snort installed on your system. The easiest way to run Snort is on Kali Linux (but any Linux distribution is fine), so please make sure you are using Kali Linux and that Snort is installed. For detailed instructions on the installation process, refer to the `snort_presentation.pptx` file.

Your Tasks

In this in-lab assignment, you are asked to write some Snort rules, but before starting, please read the instructions carefully.

You will submit a PDF document that will include some screenshots. The screenshot format should be like that in the figure below. You will show some log or alert file for each question. While doing that, you need to show the UUID in another window. You can show the UUID with the following commands:
`sudo dmidecode -s system-uuid`, or you can use **`cat /sys/class/dmi/id/product_uuid`**.



```
     GRE PPTP:            0 (  0.000%)
      GRE ARP:            0 (  0.000%)
      GRE IPX:            0 (  0.000%)
     GRE Loop:            0 (  0.000%)
         MPLS:            0 (  0.000%)
          ARP:           18 (  3.066%)
          IPX:            0 (  0.000%)
     Eth Loop:            0 (  0.000%)
     Eth Disc:            0 (  0.000%)
     IP4 Disc:            5 (  0.852%)
     IP6 Disc:            0 (  0.000%)
     TCP Disc:            0 (  0.000%)
     UDP Disc:            0 (  0.000%)
    ICMP Disc:            0 (  0.000%)
  All Discard:            5 (  0.852%)
        Other:           58 (  9.881%)
  Bad Chk Sum:          136 ( 23.169%)
      Bad TTL:            0 (  0.000%)
       S5 G 1:            1 (  0.170%)
       S5 G 2:            4 (  0.681%)
        Total:          587
===============================================================================
Action Stats:
       Alerts:            4 (  0.681%)
       Logged:            4 (  0.681%)
       Passed:            0 (  0.000%)
Limits:
        Match:            0
        Queue:            0
          Log:            0
        Event:            0
        Alert:            0
Verdicts:
        Allow:          521 ( 89.519%)
        Block:            0 (  0.000%)
      Replace:            0 (  0.000%)
    Whitelist:           61 ( 10.481%)
    Blacklist:            0 (  0.000%)
       Ignore:            0 (  0.000%)
        Retry:            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
          Memory Faults: 0
               Timeouts: 0
               Overlaps: 0
              Anomalies: 0
                 Alerts: 0
                  Drops: 0
     FragTrackers Added: 0
    FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo dmidecode -s system-uuid

112de972-302e-424d-8c78-56427172d72b

┌──(root㉿kali)-[/home/kali]
└─# 
```

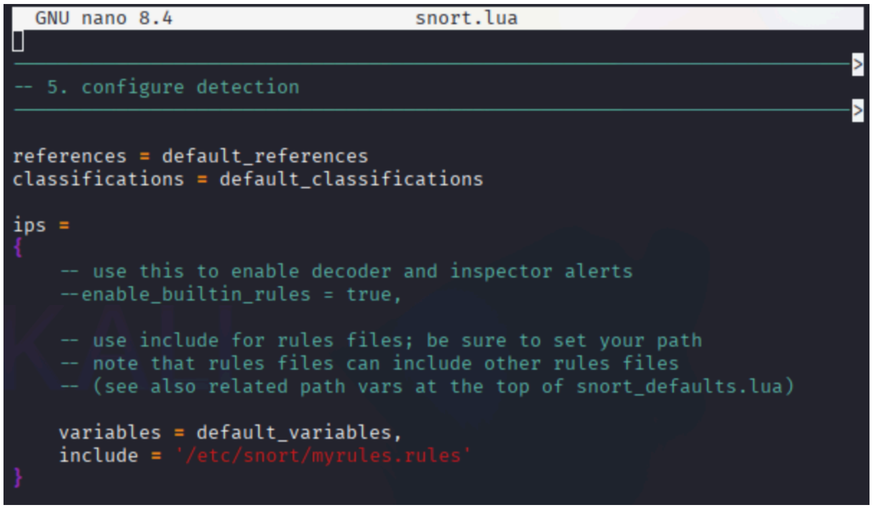
Include this window in all your screenshots.

1. Write a rule to alert if a packet with the destination port 80 contains a RAR file. How many packets did you find accordingly in the given pcap file, in other words, how many alerts did you get for this rule? (Take a screenshot of the alert file, write down the rule, and write the number of packets.) (Corresponding pcap file: Q_1.pcap)
2. Write a rule to alert if a packet with the source port 80 contains a Gzip file. What is the destination port of that packet? (Take a screenshot of the alert file, write down the rule, and write the destination port of packets.) (Corresponding pcap file: Q_2.pcap)
3. Write a rule to alert if a packet contains a JPEG file. (Corresponding pcap file: Q_3.pcap)

The pcap files are included in the `snort_in_lab_assignment.zip` file.

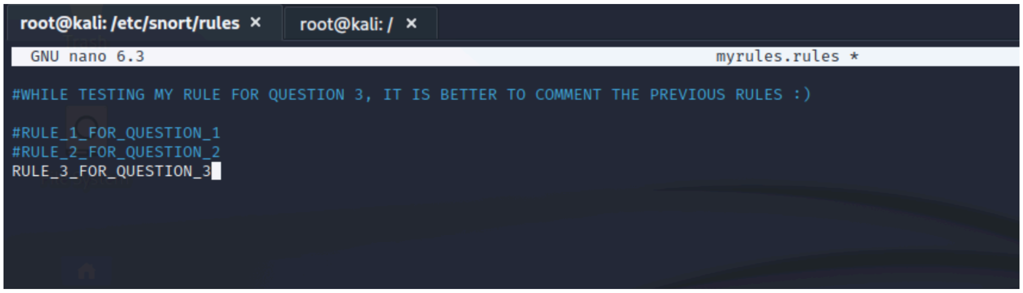
Some Notes:

1. Before answering the questions, please add your name, surname, and UUID to the top of your document.
2. Please comment or delete the other rule files (if you have any) and leave only myrules.rules in snort.lua file, which is located in the snort folder. It is important since there may be lots of alerts generated by default/community rules. Make sure the only rules file is myrules.rules. It is also easier for you to test your rules.



```
  GNU nano 8.4                         snort.lua

--------------------------------------------------------------------------->
-- 5. configure detection
--------------------------------------------------------------------------->

references = default_references
classifications = default_classifications

ips =
{
    -- use this to enable decoder and inspector alerts
    --enable_builtin_rules = true,

    -- use include for rules files; be sure to set your path
    -- note that rules files can include other rules files
    -- (see also related path vars at the top of snort_defaults.lua)

    variables = default_variables,
    include = '/etc/snort/myrules.rules'
}
```

3. Please choose meaningful messages related to the question, you can use filenames for that.
4. While answering the questions, please comment out the other rules in myrules.rules file so that only the alerts corresponding to the rule that you write for the question will be in the alert file. For example:



```
  GNU nano 6.3                                         myrules.rules *

#WHILE TESTING MY RULE FOR QUESTION 3, IT IS BETTER TO COMMENT THE PREVIOUS RULES :)

#RULE_1_FOR_QUESTION_1
#RULE_2_FOR_QUESTION_2
RULE_3_FOR_QUESTION_3
```

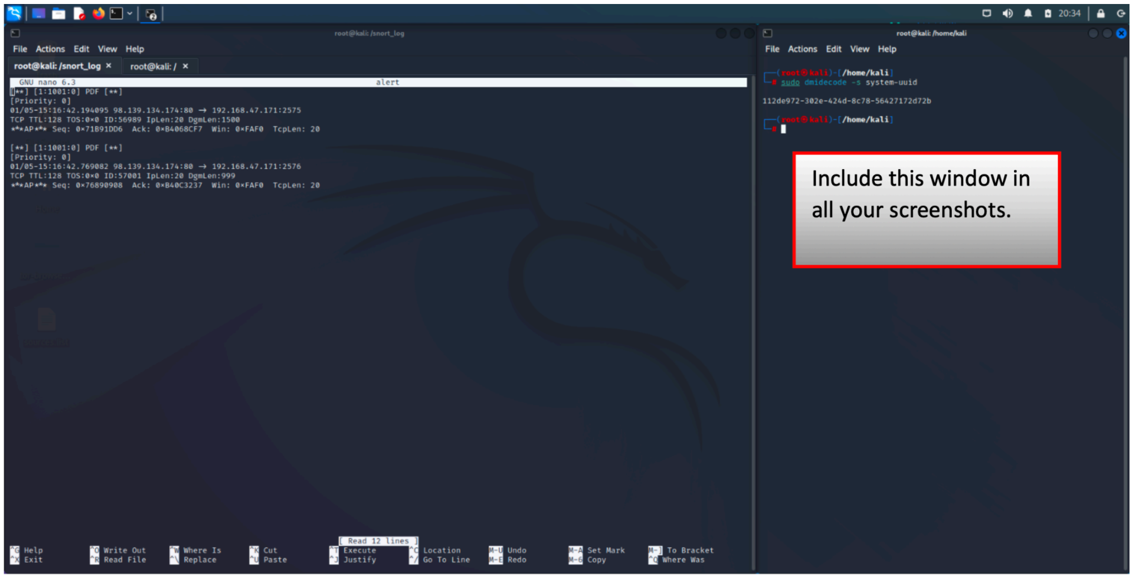
5. And you can delete the alert and log files after answering a question, they will be generated again automatically.

Please ensure that the alert file and UUID in the screenshots are visible.
Good luck!

A sample answer for questions:

Q: Please write an alert rule for packets that contain a PDF file. How many packets contain PDF in the given pcap file? What are the destination ports?

A:



```
  GNU nano 6.3                                alert
[**] [1:1001:0] PDF [**]
[Priority: 0]
01/05-15:16:42.194095 98.139.134.174:80 → 192.168.47.171:2575
TCP TTL:128 TOS:0×0 ID:56989 IpLen:20 DgmLen:1500
***AP*** Seq: 0×71B91DD6  Ack: 0×B4068CF7  Win: 0×FAF0  TcpLen: 20

[**] [1:1001:0] PDF [**]
[Priority: 0]
01/05-15:16:42.769082 98.139.134.174:80 → 192.168.47.171:2576
TCP TTL:128 TOS:0×0 ID:57001 IpLen:20 DgmLen:999
***AP*** Seq: 0×76890908  Ack: 0×B40C3237  Win: 0×FAF0  TcpLen: 20

                    [ Read 12 lines ]
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo dmidecode -s system-uuid

112de972-302e-424d-8c78-56427172d72b

┌──(root㉿kali)-[/home/kali]
└─# 
```

Rule: alert tcp any any -> any any (content:”%PDF”;msg:”PDF”;sid:1001)
There were 2 packets containing a PDF file.
The destination ports are 2575 and 2576.