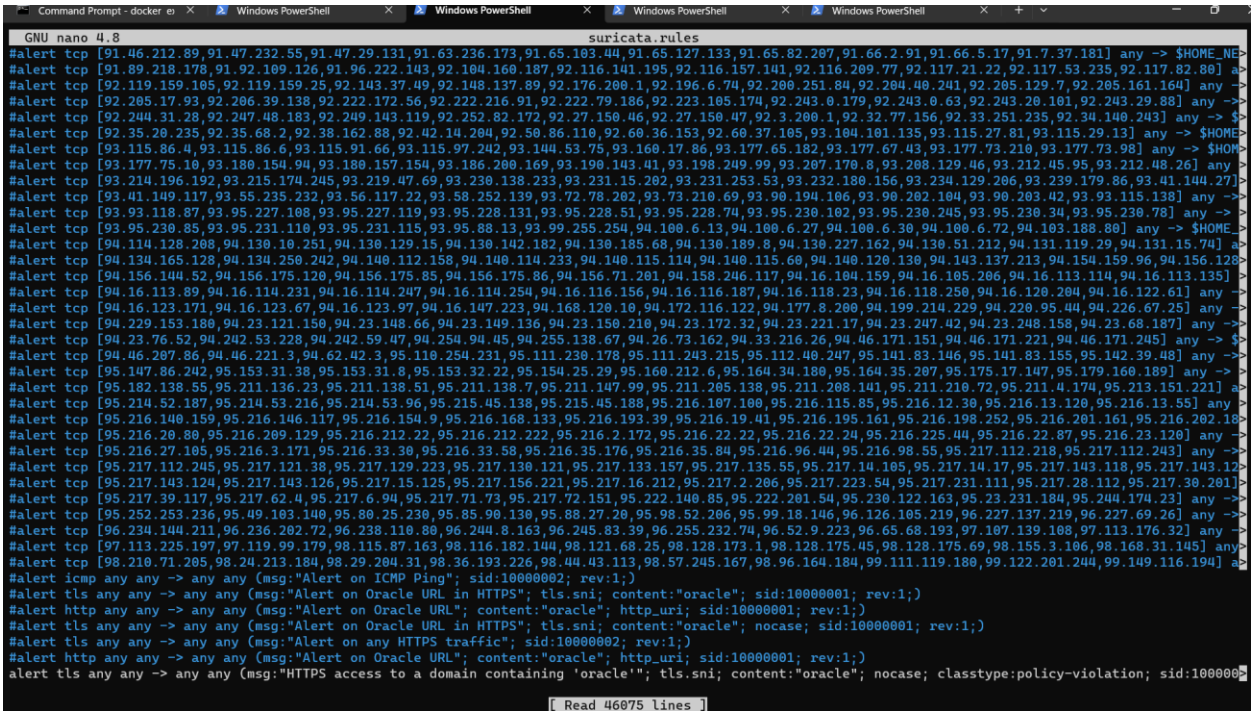
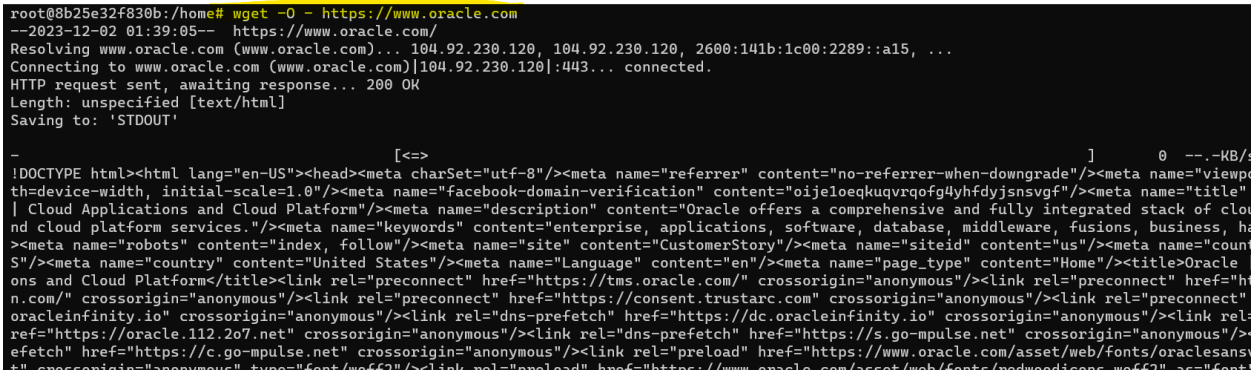
Name : Priyadharshini Stalin

IDS detection system:

- set up the following four Suricata scenarios and submit the results to Canvas.
- (part 1) 25%
    - create a Suricata rule that alerts when a browser attempts to access a URL with the string "oracle" in the URL.
    - submit the rule you create.

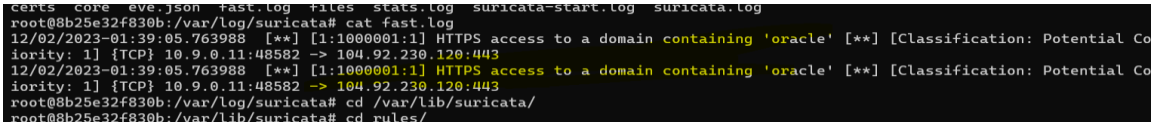
IDS-Router:





- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

IDS-router:



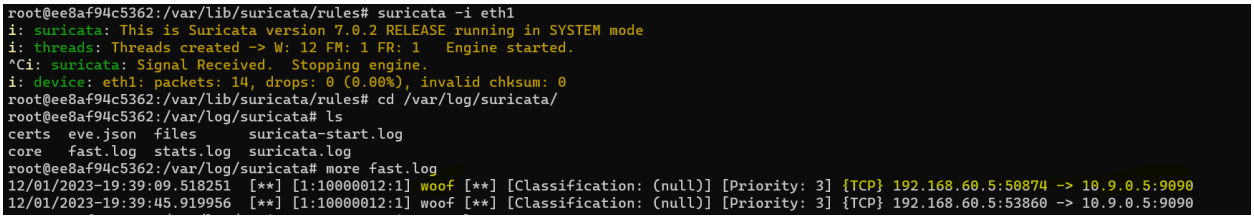
part 4) 25%

- create a Suricata rule that detects a content text string from the lassie.txt file on Host 1
- submit the rule you create.

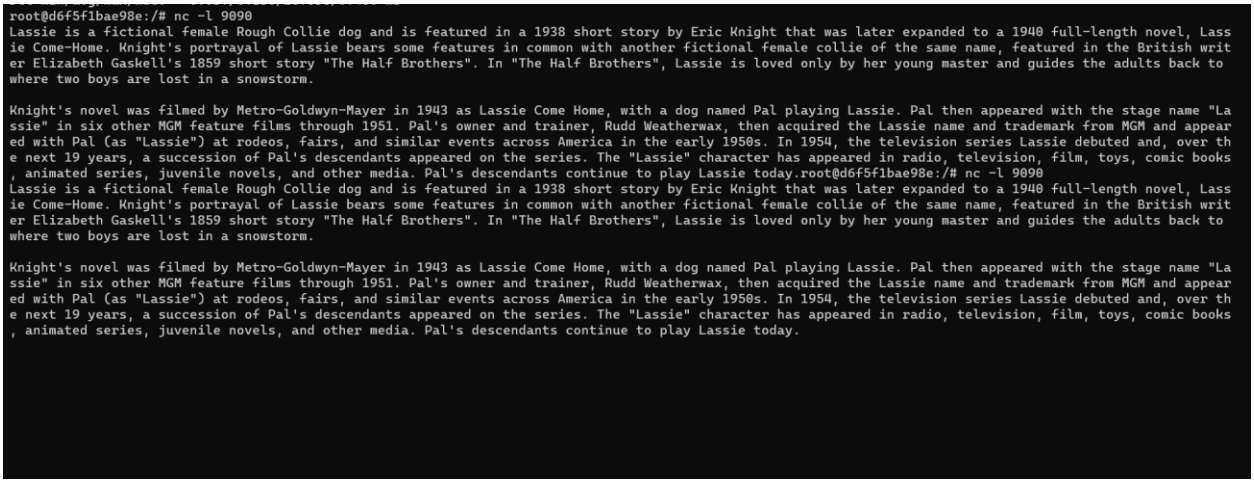
IDS-Router:

- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

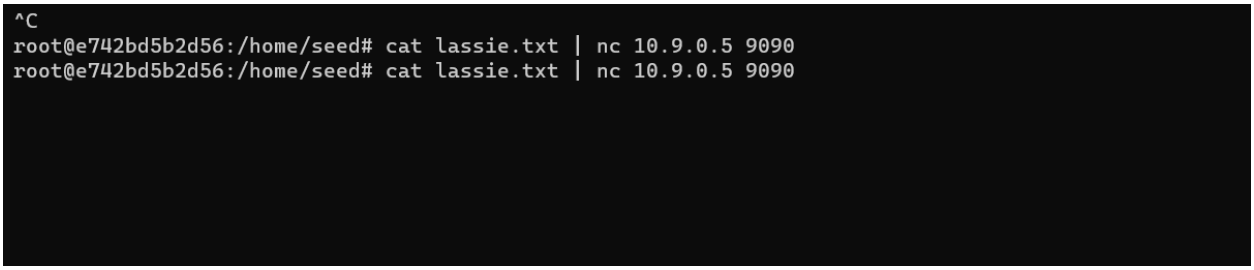
IDS-Router



Host A



Host1



part 2 25%

- create a Suricata rule that alerts when any host is pinged.
- submit the rule you create.

- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

Host A:

```
^C
root@d6f5f1bae98e:/# nc -l -p 9090
```

Host 1:

```
root@e742bd5b2d56:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.992 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.235 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.167 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.284 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.138 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=63 time=0.097 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=63 time=0.128 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=63 time=0.139 ms
64 bytes from 10.9.0.5: icmp_seq=9 ttl=63 time=0.166 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=63 time=0.329 ms
64 bytes from 10.9.0.5: icmp_seq=11 ttl=63 time=0.229 ms
64 bytes from 10.9.0.5: icmp_seq=12 ttl=63 time=0.188 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=63 time=0.149 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=63 time=0.186 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=63 time=0.159 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=63 time=0.144 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=63 time=0.123 ms
64 bytes from 10.9.0.5: icmp_seq=18 ttl=63 time=0.135 ms
64 bytes from 10.9.0.5: icmp_seq=19 ttl=63 time=0.189 ms
64 bytes from 10.9.0.5: icmp_seq=20 ttl=63 time=0.115 ms
64 bytes from 10.9.0.5: icmp_seq=21 ttl=63 time=0.091 ms
64 bytes from 10.9.0.5: icmp_seq=22 ttl=63 time=0.201 ms
64 bytes from 10.9.0.5: icmp_seq=23 ttl=63 time=0.144 ms
64 bytes from 10.9.0.5: icmp_seq=24 ttl=63 time=0.176 ms
64 bytes from 10.9.0.5: icmp_seq=25 ttl=63 time=0.111 ms
64 bytes from 10.9.0.5: icmp_seq=26 ttl=63 time=0.130 ms
64 bytes from 10.9.0.5: icmp_seq=27 ttl=63 time=0.180 ms
64 bytes from 10.9.0.5: icmp_seq=28 ttl=63 time=0.279 ms
64 bytes from 10.9.0.5: icmp_seq=29 ttl=63 time=0.167 ms
64 bytes from 10.9.0.5: icmp_seq=30 ttl=63 time=0.116 ms
64 bytes from 10.9.0.5: icmp_seq=31 ttl=63 time=0.188 ms
```

IDS-router:

suricata.rules

Alert log:

```
root@ee8af94c5362:/var/log/suricata# suricata -i eth1
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 12 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: eth1: packets: 445, drops: 0 (0.00%), invalid chksum: 0
root@ee8af94c5362:/var/log/suricata# more fast.log
12/01/2023-22:21:30.647367  [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-22:21:30.647676  [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 10.9.0.5:0 -> 192.168.60.5:0
12/01/2023-22:21:51.439393  [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-22:21:51.439449  [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 10.9.0.5:0 -> 192.168.60.5:0
root@ee8af94c5362:/var/log/suricata#
```

(part 3) 25%

- create a Suricata rule that alerts when telnet traffic is seen on the network.
- submit the rule you create.
- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

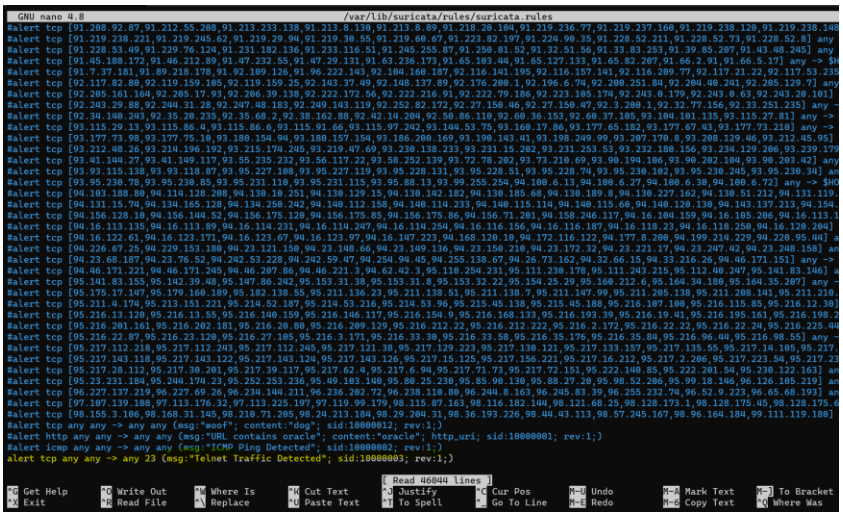
Host1:

```
root@e742bd5b2d56:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d6f5f1bae98e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Dec  1 22:31:49 UTC 2023 from 192.168.60.5 on pts/2
seed@d6f5f1bae98e:~$
```

Host A:

```
root@d6f5f1bae98e:/# nc -l -p 9090
```

IDS-Router



Alert: