# Snort3 Rule Modification for TCP Packet Alerts

**Modify Snort3 rules so as to generate alert for TCP packets  and demo this in the pcap file generted by Snort.**

## Introduction

In this activity, we are using Snort3, a powerful intrusion detection system (IDS) and intrusion prevention system (IPS) tool, to generate alerts specifically for TCP (Transmission Control Protocol) packets. TCP is a core protocol in computer networking, responsible for establishing and maintaining reliable connections between devices on a network.

By modifying Snort3 rules, we can create custom rules that trigger alerts whenever TCP packets are detected. These alerts help network administrators and security analysts identify potential threats or suspicious activities related to TCP traffic.

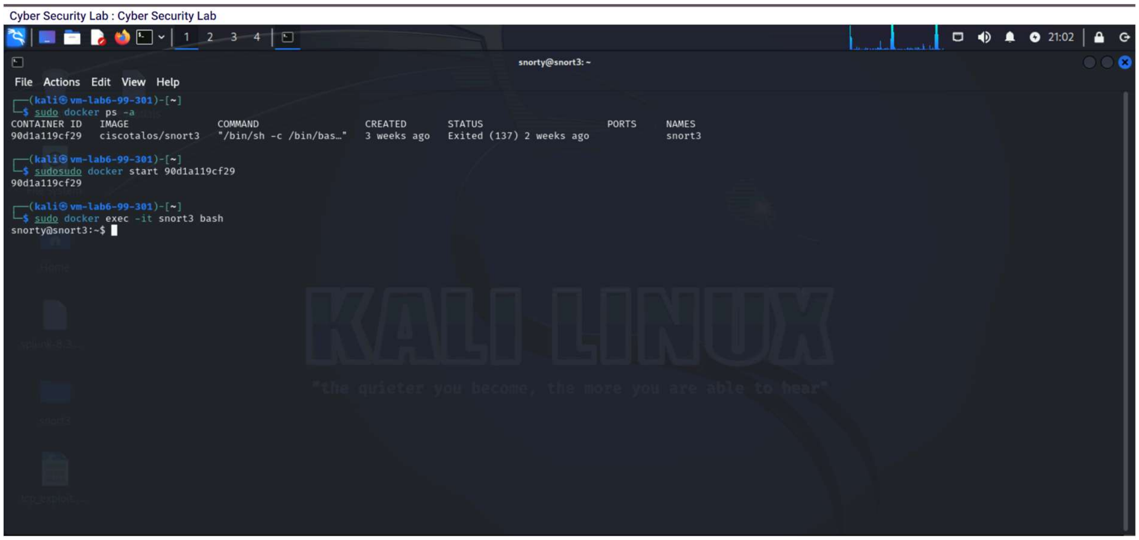
In this demonstration, we will modify Snort3 rules to generate alerts for TCP packets and then showcase this functionality using a pcap (Packet Capture) file generated by Snort. The pcap file contains network traffic data captured by Snort, which we will analyze to validate the effectiveness of our custom TCP alert rules.

Through this activity, we aim to highlight how Snort3 can be tailored to detect and respond to specific network protocols like TCP, enhancing network security and threat detection capabilities.

## Setting up Docker and configuring Snort3 involves the installation and setup processes for both Docker and Snort3.

1. Open Kali Linux machine
2. Open terminal
3. Run git clone https://github.com/madler/zlib
4. CD into the directory of the cloned Repo, then
   ./configure
   Make
   sudo make install
5. Download the Container docker pull ciscotalos/snort3
6. Start the Container docker run --name snort3 -h snort3 -u snorty -w /home/snorty -d -it ciscotalos/snort3 bash
7. Enter the Snort Container docker exec -it snort3 bash
8. The above command will able to install snort 3 and entering in the docker container
   In my machine I have alerdy done this so I hace to follow some different steps which are as follows:-
9. To see the last docker running sudo docker Ps -a
10. Then you will see the container id , copy container id then,Sudo docker start  <docker container id>

11. Entering in docker Sudo docker exec -it snort3 bash

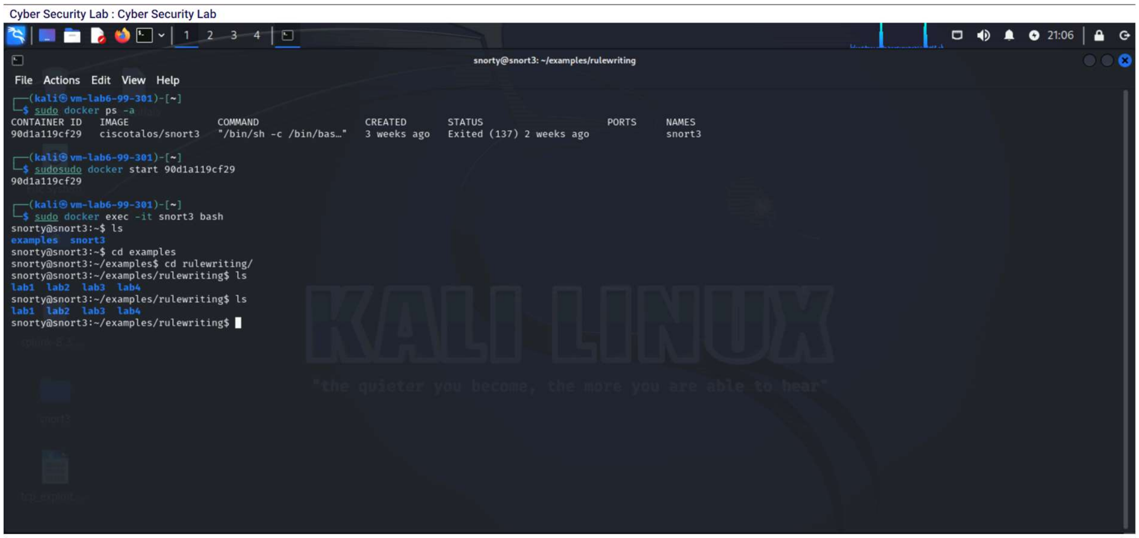

Cyber Security Lab : Cyber Security Lab
1 2 3 4
21:02
snorty@snort3: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE               COMMAND                  CREATED       STATUS                       PORTS     NAMES
90d1a119cf29   ciscotalos/snort3   "/bin/sh -c /bin/bas…"   3 weeks ago   Exited (137) 2 weeks ago             snort3

┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudosudo docker start 90d1a119cf29
90d1a119cf29

┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudo docker exec -it snort3 bash
snorty@snort3:~$ █
```

12. Go to the examples in snort be cd examples
13. Go for rule writing by cd ruleswriting/

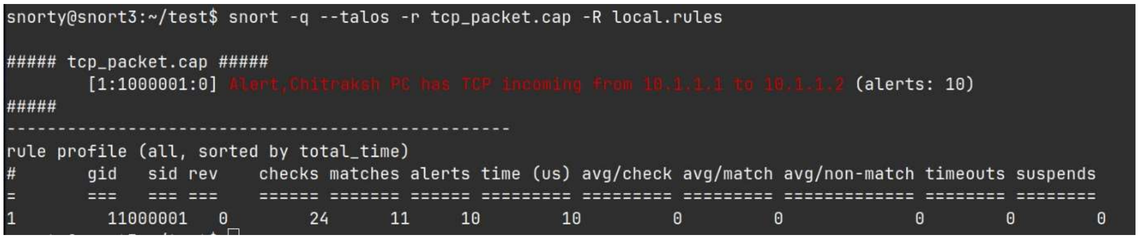

Cyber Security Lab : Cyber Security Lab
1 2 3 4
21:06
snorty@snort3: ~/examples/rulewriting
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE               COMMAND                  CREATED       STATUS                       PORTS     NAMES
90d1a119cf29   ciscotalos/snort3   "/bin/sh -c /bin/bas…"   3 weeks ago   Exited (137) 2 weeks ago             snort3

┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudosudo docker start 90d1a119cf29
90d1a119cf29

┌──(kali㉿vm-lab6-99-301)-[~]
└─$ sudo docker exec -it snort3 bash
snorty@snort3:~$ ls
examples  snort3
snorty@snort3:~$ cd examples
snorty@snort3:~/examples$ cd rulewriting/
snorty@snort3:~/examples/rulewriting$ ls
lab1  lab2  lab3  lab4
snorty@snort3:~/examples/rulewriting$ ls
lab1  lab2  lab3  lab4
snorty@snort3:~/examples/rulewriting$ █
```

14. Change pcap file in lab1 (download it by internet which consists of sending multiple tcp packet sending from 10.1.1.1 to 10.1.1.2 so that we can generate alert
15. Now open vim local.rules
16. Change rule to *alert tcp 10.1.1.1 any -> 10.1.1.2 any (msg:"Alert, Chitraksh PC has TCP incoming from 10.1.1.1 to 10.1.1.2"; sid:1000001;)*
17. Run *snort -q --talos -r tcp_packet.cap -R local.rules* after changing pcap file (Packet Captures - PacketLife.net)
18. Then the alert has been show

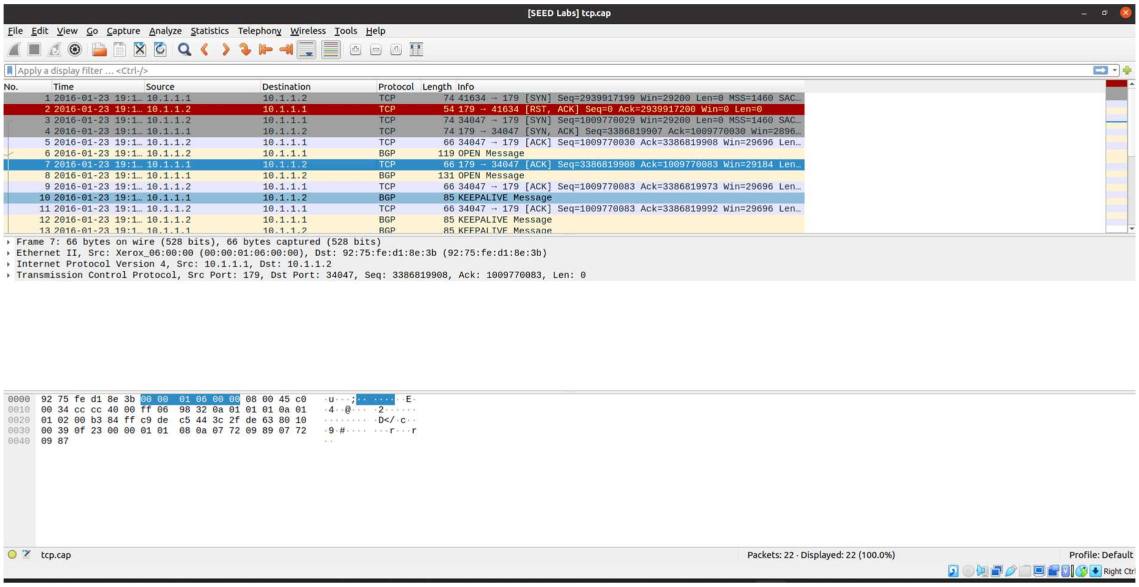


```
snorty@snort3:~/test$ snort -q --talos -r tcp_packet.cap -R local.rules

##### tcp_packet.cap #####
        [1:1000001:0] Alert,Chitraksh PC has TCP incoming from 10.1.1.1 to 10.1.1.2 (alerts: 10)
#####
--------------------------------------------------
rule profile (all, sorted by total_time)
#       gid   sid rev    checks matches alerts time (us) avg/check avg/match avg/non-match timeouts suspends
=       ===   === ===    ====== ======= ====== ========= ========= ========= ============= ======== ========
1         11000001   0       24      11     10        10         0         0             0        0        0
```

19. As you see that it **generated alert for TCP packets**

## Wireshark


[SEED Labs] tcp.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time             Source     Destination  Protocol Length Info
    1 2016-01-23 19:1… 10.1.1.1   10.1.1.2     TCP       74 41634 → 179 [SYN] Seq=2939917199 Win=29200 Len=0 MSS=1460 SAC…
    2 2016-01-23 19:1… 10.1.1.2   10.1.1.1     TCP       54 179 → 41634 [RST, ACK] Seq=0 Ack=2939917200 Win=0 Len=0
    3 2016-01-23 19:1… 10.1.1.2   10.1.1.1     TCP       74 34047 → 179 [SYN] Seq=1009770029 Win=29200 Len=0 MSS=1460 SAC…
    4 2016-01-23 19:1… 10.1.1.1   10.1.1.2     TCP       74 179 → 34047 [SYN, ACK] Seq=3386819907 Ack=1009770030 Win=2896…
    5 2016-01-23 19:1… 10.1.1.2   10.1.1.1     TCP       66 34047 → 179 [ACK] Seq=1009770030 Ack=3386819908 Win=29696 Len…
    6 2016-01-23 19:1… 10.1.1.2   10.1.1.1     BGP      119 OPEN Message
    7 2016-01-23 19:1… 10.1.1.1   10.1.1.2     TCP       66 179 → 34047 [ACK] Seq=3386819908 Ack=1009770083 Win=29184 Len…
    8 2016-01-23 19:1… 10.1.1.1   10.1.1.2     BGP      131 OPEN Message
    9 2016-01-23 19:1… 10.1.1.2   10.1.1.1     TCP       66 34047 → 179 [ACK] Seq=1009770083 Ack=3386819973 Win=29696 Len…
   10 2016-01-23 19:1… 10.1.1.1   10.1.1.2     BGP       85 KEEPALIVE Message
   11 2016-01-23 19:1… 10.1.1.2   10.1.1.1     TCP       66 34047 → 179 [ACK] Seq=1009770083 Ack=3386819992 Win=29696 Len…
   12 2016-01-23 19:1… 10.1.1.2   10.1.1.1     BGP       85 KEEPALIVE Message
   13 2016-01-23 19:1… 10.1.1.1   10.1.1.2     BGP       85 KEEPALIVE Message

› Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
› Ethernet II, Src: Xerox_06:00:00 (00:00:01:06:00:00), Dst: 92:75:fe:d1:8e:3b (92:75:fe:d1:8e:3b)
› Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.2
› Transmission Control Protocol, Src Port: 179, Dst Port: 34047, Seq: 3386819908, Ack: 1009770083, Len: 0

0000  92 75 fe d1 8e 3b 00 00  01 06 00 00 08 00 45 c0   ·u···;·· ······E·
0010  00 34 cc cc 40 00 ff 06  98 32 0a 01 01 01 0a 01   ·4··@··· ·2······
0020  01 02 00 b3 84 ff c9 de  c5 44 3c 2f de 63 80 10   ········ ·D</·c··
0030  00 39 0f 23 00 00 01 01  08 0a 07 72 09 89 07 72   ·9·#···· ···r···r
0040  09 87                                              ··
```

Upon analyzing the pcap file, it becomes evident that numerous TCP packets are being transmitted to establish connections. However, our IDS (Intrusion Detection System) Snort is successfully generating alerts in the Snort terminal, indicating its capability to detect and respond to suspicious or potentially malicious TCP packet activity. This demonstrates the effectiveness of our IDS in monitoring and safeguarding network traffic against potential threats.

## Learnings

1. Get to know about the snort rule and how we can create for tcp as well
2. To learn more about ids and how we can detect and prevent any type of activity with my pc , also how ids is very important for pc.