

ASSIGNMENT 10

Name: Yogita Mundankar

Rollno. B22CS068

Task 1: Snort Installation

- **Install Snort on Kali Linux:** Snort was installed using the following commands:
sudo apt update
sudo apt install snort
- **Verify the installation and check the version:** After installation, the version was verified using:

```
(kali@kali)-[/home/kali]
PS> snort -V
64 bytes from 8.8.8.8: icmp_seq=81 ttl=128 time=75.1 ms
8.8.8.8: icmp_seq=82 ttl=128 time=60.2 ms
64 bytes from 8.8.8.8: icmp_seq=83 ttl=128 time=59.4 ms
8.8.8.8: icmp_seq=84 ttl=128 time=60.6 ms
64 bytes from 8.8.8.8: icmp_seq=85 ttl=128 time=59.0 ms
8.8.8.8: icmp_seq=86 ttl=128 time=85.3 ms
64 bytes from 8.8.8.8: icmp_seq=87 ttl=128 time=60.2 ms
8.8.8.8: icmp_seq=88 ttl=128 time=68.4 ms
By Martin Roesch & The Snort Team
http://snort.org/contact#team
Copyright (C) 2014-2024 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using DAQ version 3.0.19
Using LuaJIT version 2.1.1700206165
Using OpenSSL 3.4.1 11 Feb 2025
Using libpcap version 1.10.5 (with TPACKET_V3)
Using PCRE version 8.39 2016-06-14
Using ZLIB version 1.3.1
Using LZMA version 5.6.4
```

Task 2: Configuring Snort and write Snort Rules

- Configuring snort from the /etc/snort/snort.lua:

```
(kali@kali)-[/home/kali]
PS> sudo nano /etc/snort/snort.lua
[sudo] password for kali:
(kali@kali)-[/home/kali]
```

- Inside the configuration file made the following changes:

The **HOME_NET** variable was set to reflect the IP range of the local network:

IP of VM: 192.168.235.128

Subnet: 192.168.235.0/24

```
(kali@kali)-[/home/kali]
PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:23:d8:98 brd ff:ff:ff:ff:ff:ff
    inet 192.168.235.128/24 brd 192.168.235.255 scope global dynamic noprefixroute eth0
        valid_lft 1068sec preferred_lft 1068sec
    inet6 fe80::f27e:d33a:db51:f34a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
-- setup the network addresses you are protecting
HOME_NET = '192.168.235.0/24'
EXTERNAL_NET = 'any'

--HOME_NET = '192.168.235.0/24'

-- set up the external network addresses.
-- (leave as "any" in most situations)
--EXTERNAL_NET = 'any'
include 'snort_defaults.lua'
```

- Ensure local rules are included:

```
references = default_references
classifications = default_classifications
--RULE_PATH = '/etc/snort/rules'-
--include 'snort_defaults.lua'

ips =
{
    -- use this to enable decoder and inspector alerts
    -- enable_built_in_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)
    include = '/etc/snort/rules/local.rules',
    variables = default_variables
}
```

```
alert_fast = {file = true, }
--alert_full = { }
--alert_sfsocket = { }
```

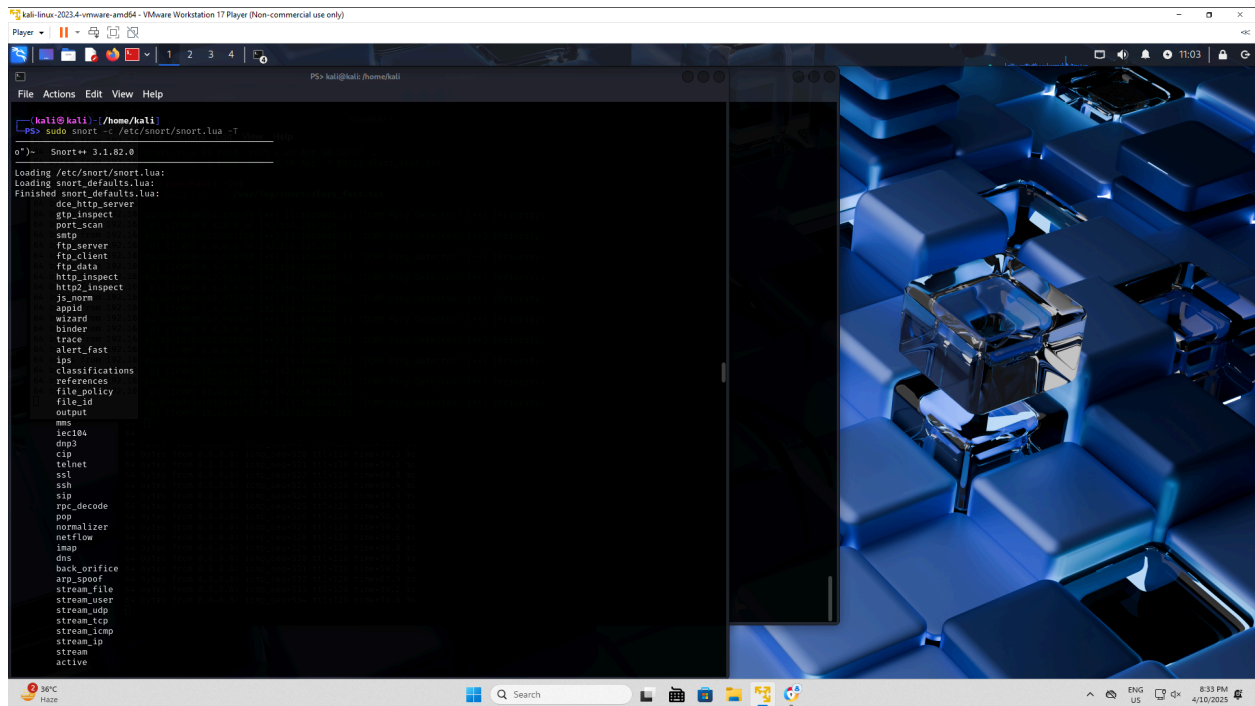
- Writing Snort Rules:

```
(kali@kali)-[/home/kali]
PS> sudo nano /etc/snort/rules/local.rules
```

- A custom rule was created to detect ICMP (ping) traffic:

```
File Actions Edit View Help
GNU nano 8.3 /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
#drop icmp any any -> any any (msg:"ICMP packet dropped"; sid:1000002; rev:1;)
```

- Checked if the file is configured successfully:



```
service rule counts      to_srv to_cli
file_id:      208      208
total:      208      208

fast pattern groups
to_server: 1
to_client: 1

search engine (ac_bnfa)
appid: MaxRss diff: 2748
appid: patterns loaded: 300

pcap DAQ configured to passive.
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting
```

Snort is successfully configured as can be seen from the above message.

Task 3: Running Snort in IDS Mode

- Running Snort in IDS:

Start Snort in IDS mode and monitor network traffic:

```
(kali@kali)-[/home/kali]
PS> sudo snort -c /etc/snort/snort.lua -i eth0

o")~  Snort++ 3.1.82.0

Loading /etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
bytes fr active 16
bytes fr alerts 16
bytes fr daq 16
bytes fr decode 16
bytes fr host_cache 16
bytes fr host_tracker 16
bytes fr hosts 16
bytes fr network 16
bytes fr process 16
bytes fr search_engine 16
bytes fr so_proxy 16
bytes fr dce_http_proxy 16
bytes fr gtp_inspect 16
bytes fr stream 16
bytes fr trace 16
bytes fr stream_icmp 16
bytes fr stream_udp 16
bytes fr wizard 16
bytes fr dce_udp 16
classifications
references
binder
alert_fast
appid
js_norm
file_policy
file_id
http2_inspect
http_inspect
ftp_data
ftp_client
ftp_server
smtp
output
port_scan
dce_http_server
ips
dce_tcp
dce_smb
s7commplus
modbus
mms
iec104
dnp3
cip
```

```

Action stream_ip
packets
Finished /etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /etc/snort/rules/local.rules:
Finished /etc/snort/rules/local.rules:

ips policies rule stats
bytes from 192.168.1.0/24 loaded shared enabled file
bytes from 192.168.1.0/24 209 0 209 /etc/snort/snort.lua

rule counts
bytes from 192.168.1.0/24 total rules loaded: 209
bytes from 192.168.1.0/24 text rules: 209
bytes from 192.168.1.0/24 option chains: 209
bytes from 192.168.1.0/24 chain headers: 2

port rule counts
bytes from 192.168.1.0/24 tcp udp icmp ip
bytes any m 192.168.1.0/24 0 1 0
bytes total m 192.168.1.0/24 0 1 0

service rule counts
bytes from 192.168.1.0/24 file_id: to-srv to-cli
bytes from 192.168.1.0/24 total: 208 208

fast pattern groups
to_server: 1
to_client: 1

search engine (ac_bnfa)
instances: 2
patterns: 416
pattern chars: 2508
num states: 1778
num match states: 370
memory scale: KB
total memory: 68.5879
pattern memory: 18.6973
match list memory: 27.3281
transition memory: 22.3125
appid: MaxRss diff: 3072
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
^C** caught int signal
= stopping
-- [0] eth0

```

Packet Statistics

```
daq from 192.168.1.100:10000 to 192.168.1.100:10000
bytes from 192.168.1.100:10000 received: 748
bytes from 192.168.1.100:10000 analyzed: 748
bytes from 192.168.1.100:10000 allow: 748
bytes from 192.168.1.100:10000 rx_bytes: 70866
```

```
code from 192.168.1.100:10000 to 192.168.1.100:10000
bytes from 192.168.1.100:10000 total: 748 (100.000%)
bytes from 192.168.1.100:10000 arp: 68 ( 9.091%)
bytes from 192.168.1.100:10000 eth: 748 (100.000%)
bytes from 192.168.1.100:10000 icmp4: 655 ( 87.567%)
bytes from 192.168.1.100:10000 icmp6: 5 ( 0.668%)
bytes from 192.168.1.100:10000 igmp: 5 ( 0.668%)
bytes from 192.168.1.100:10000 ipv4: 669 ( 89.439%)
bytes from 192.168.1.100:10000 ipv6: 11 ( 1.471%)
bytes from 192.168.1.100:10000 ipv6_hop_opts: 5 ( 0.668%)
bytes from 192.168.1.100:10000 udp: 15 ( 2.005%)
```

Module Statistics

```
appid from 192.168.1.100:10000 to 192.168.1.100:10000
bytes from 192.168.1.100:10000 packets: 680
bytes from 192.168.1.100:10000 processed_packets: 680
bytes from 192.168.1.100:10000 total_sessions: 8
bytes from 192.168.1.100:10000 service_cache_adds: 3
bytes from 192.168.1.100:10000 bytes_in_use: 456
bytes from 192.168.1.100:10000 items_in_use: 3
```

```
arp_spoof
packets: 68
```

```
back_orifice
packets: 15
```

```
binder
raw_packets: 68
new_flows: 8
inspects: 76
```

```
detection
analyzed: 748
hard_evals: 660
alerts: 327
total_alerts: 327
logged: 327
```

```
port_scan
packets: 680
trackers: 11
```

```
search_engine
non_qualified_events: 333
```


- Generate ICMP traffic:

```
(root@kali)-[~]  
# ping 192.168.235.128  
  
PING 192.168.235.128 (192.168.235.128) 56(84) bytes of data.  
64 bytes from 192.168.235.128: icmp_seq=1 ttl=64 time=0.025 ms  
64 bytes from 192.168.235.128: icmp_seq=2 ttl=64 time=0.056 ms  
64 bytes from 192.168.235.128: icmp_seq=3 ttl=64 time=0.025 ms  
64 bytes from 192.168.235.128: icmp_seq=4 ttl=64 time=0.058 ms  
64 bytes from 192.168.235.128: icmp_seq=5 ttl=64 time=0.037 ms  
64 bytes from 192.168.235.128: icmp_seq=6 ttl=64 time=0.042 ms  
64 bytes from 192.168.235.128: icmp_seq=7 ttl=64 time=0.046 ms  
64 bytes from 192.168.235.128: icmp_seq=8 ttl=64 time=0.041 ms  
64 bytes from 192.168.235.128: icmp_seq=9 ttl=64 time=0.032 ms  
64 bytes from 192.168.235.128: icmp_seq=10 ttl=64 time=0.040 ms  
64 bytes from 192.168.235.128: icmp_seq=11 ttl=64 time=0.047 ms  
64 bytes from 192.168.235.128: icmp_seq=12 ttl=64 time=0.025 ms  
64 bytes from 192.168.235.128: icmp_seq=13 ttl=64 time=0.054 ms  
64 bytes from 192.168.235.128: icmp_seq=14 ttl=64 time=0.024 ms  
64 bytes from 192.168.235.128: icmp_seq=15 ttl=64 time=0.024 ms  
64 bytes from 192.168.235.128: icmp_seq=16 ttl=64 time=0.023 ms  
64 bytes from 192.168.235.128: icmp_seq=17 ttl=64 time=0.025 ms  
64 bytes from 192.168.235.128: icmp_seq=18 ttl=64 time=0.022 ms  
64 bytes from 192.168.235.128: icmp_seq=19 ttl=64 time=0.063 ms  
64 bytes from 192.168.235.128: icmp_seq=20 ttl=64 time=0.023 ms  
64 bytes from 192.168.235.128: icmp_seq=2976 ttl=64 time=0.025 ms  
64 bytes from 192.168.235.128: icmp_seq=2977 ttl=64 time=0.061 ms  
64 bytes from 192.168.235.128: icmp_seq=2978 ttl=64 time=0.061 ms  
64 bytes from 192.168.235.128: icmp_seq=2979 ttl=64 time=0.050 ms  
64 bytes from 192.168.235.128: icmp_seq=2980 ttl=64 time=0.053 ms  
64 bytes from 192.168.235.128: icmp_seq=2981 ttl=64 time=0.023 ms  
64 bytes from 192.168.235.128: icmp_seq=2982 ttl=64 time=0.033 ms  
64 bytes from 192.168.235.128: icmp_seq=2983 ttl=64 time=0.037 ms  
^C  
— 192.168.235.128 ping statistics —  
2983 packets transmitted, 2983 received, 0% packet loss, time 3053612ms  
rtt min/avg/max/mdev = 0.017/0.047/0.289/0.020 ms
```


- Capture alerts in the Snort logs.

```
(root@kali)-[~] 969 ttl=64 time=0.054 ms
# sudo tail -f /var/log/snort/alert_fast.txt
192.168.235.128: icmp_seq=2971 ttl=64 time=0.028 ms
04/08-18:06:14.876695 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 060 ms
04/08-18:06:15.901320 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 024 ms
04/08-18:06:16.924700 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 061 ms
04/08-18:06:17.952646 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 050 ms
04/08-18:06:18.972537 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 023 ms
04/08-18:06:19.996537 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128 037 ms
04/08-18:06:21.020530 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 8.8.8.8 → 192.168.235.128
04/09-09:32:56.825669 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 10.40.0.73 → 192.168.235.128
04/09-09:33:00.328101 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 10.40.0.73 → 192.168.235.128
04/09-09:33:03.319277 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority:
0] {ICMP} 10.40.0.73 → 192.168.235.128
```

TASK 4: Running Snort in IPS Mode

- Modify the Snort rule to drop ICMP traffic:

```
(kali@kali)-[/home/kali]
PS> sudo nano /etc/snort/rules/local.rules

File Actions Edit View Help
GNU nano 8.3 /etc/snort/rules/local.rules
drop icmp any any -> any any (msg:"ICMP Packet Dropped"; sid:10000002; rev:1;)
```

- Configure iptables to redirect traffic to Snort:

```
(kali@kali)-[/home/kali]
PS> sudo nano /etc/snort/rules/local.rules

(kali@kali)-[/home/kali]
PS> sudo iptables -F from 8.8.8.8: icmp_seq=65 ttl=128 time

(kali@kali)-[/home/kali]
PS> sudo iptables -t nat -F 8.8.8.8: icmp_seq=68 ttl=128 time

(kali@kali)-[/home/kali]
PS> sudo iptables -t mangle -F 8.8.8.8: icmp_seq=71 ttl=128 time

(kali@kali)-[/home/kali]
PS> sudo sysctl -w net.ipv4.ip_forward=1
sudo: sysctl: command not found

(kali@kali)-[/home/kali]
PS> sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(kali@kali)-[/home/kali]
PS> sudo iptables -A FORWARD -j NFQUEUE --queue-num 0
```

- Run Snort in Inline IPS Mode:

```
(root@kali)-[~] # sudo snort -c /etc/snort/snort.lua -i eth0 --daq afpacket --daq-mode inline
235.128 icmp_seq=96 ttl=64 time=0.065 ms
o")~ 12 Snort++ 3.1.82.0
Loading /etc/snort/snort.lua: time=0.062 ms
Loading snort_defaults.lua: time=0.062 ms
Finished snort_defaults.lua: time=0.064 ms
235.128 smtp_seq=103 ttl=64 time=0.060 ms
235.128 ftp_server_seq=104 ttl=64 time=0.060 ms
235.128 ftp_client_seq=105 ttl=64 time=0.045 ms
235.128 ftp_data_seq=106 ttl=64 time=0.025 ms
235.128 output_seq=107 ttl=64 time=0.030 ms
235.128 http2_inspect_seq=108 ttl=64 time=0.062 ms
235.128 js_norm_seq=109 ttl=64 time=0.147 ms
235.128 appid_seq=110 ttl=64 time=0.057 ms
235.128 wizard_seq=111 ttl=64 time=0.035 ms
235.128 binder_seq=112 ttl=64 time=0.029 ms
235.128 ips_seq=113 ttl=64 time=0.065 ms
235.128 classifications_seq=114 ttl=64 time=0.061 ms
235.128 http_inspect_seq=115 ttl=64 time=0.060 ms
235.128 file_policy_seq=116 ttl=64 time=0.060 ms
235.128 file_id_seq=117 ttl=64 time=0.060 ms
235.128 references_seq=118 ttl=64 time=0.060 ms
```

```
= stopping
04/08-11:32:47.265318 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.1 → 192.168.235.128
04/08-11:32:47.265361 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.128 → 192.168.235.1
04/08-11:32:48.271169 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.1 → 192.168.235.128
04/08-11:32:48.271217 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.128 → 192.168.235.1
04/08-11:32:49.290829 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.1 → 192.168.235.128
04/08-11:32:49.290871 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.128 → 192.168.235.1
04/08-11:32:50.296148 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.1 → 192.168.235.128
04/08-11:32:50.296189 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 192.168.235.128 → 192.168.235.1
-- [0] eth0
```

```
Packet Statistics 1:1000001:1 has no fast pattern
```

```
daqvce rule counts to-srv to-clt
received: 17 208 208
analyzed: 17 208 208
allow: 17
fast pattern group rx_bytes: 1096
codec to-client: 1
total: 17 (100.000%)
search engine (ac_bnf_arp: 9 ( 52.941%)
instance: 17 (100.000%)
pattern icmp4: 8 ( 47.059%)
pattern ipv4: 8 ( 47.059%)
```

```
Module Statistics states: 378
```

```
appid total memory: 68.5879
pattern packets: 8.6973
processed_packets: 8.3281
total_sessions: 1.3125
```

```
arp_spoof terms loaded: 308
packets: 9
```

```
binder
```

```
snort success raw_packets: 9 the configuration (with 3 warnings).
o")~ Snort++ new_flows: 1
inspects: 10
```

```
detection /etc/snort/snort.lua -i lo -A alert_fast -l /var/log/snort
analyzed: 17
```

TASK 5: Testing and logging

- Generate ICMP Traffic:

```
(root@kali)-[~]
# ping 192.168.235.128
PING 192.168.235.128 (192.168.235.128) 56(84) bytes of data:
64 bytes from 192.168.235.128: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 192.168.235.128: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from 192.168.235.128: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 192.168.235.128: icmp_seq=4 ttl=64 time=0.171 ms
64 bytes from 192.168.235.128: icmp_seq=5 ttl=64 time=0.060 ms
64 bytes from 192.168.235.128: icmp_seq=6 ttl=64 time=0.056 ms
64 bytes from 192.168.235.128: icmp_seq=7 ttl=64 time=0.024 ms
64 bytes from 192.168.235.128: icmp_seq=8 ttl=64 time=0.025 ms
64 bytes from 192.168.235.128: icmp_seq=9 ttl=64 time=0.024 ms
64 bytes from 192.168.235.128: icmp_seq=10 ttl=64 time=0.023 ms
64 bytes from 192.168.235.128: icmp_seq=11 ttl=64 time=0.061 ms
64 bytes from 192.168.235.128: icmp_seq=12 ttl=64 time=0.061 ms
64 bytes from 192.168.235.128: icmp_seq=13 ttl=64 time=0.063 ms
64 bytes from 192.168.235.128: icmp_seq=14 ttl=64 time=0.026 ms
64 bytes from 192.168.235.128: icmp_seq=15 ttl=64 time=0.025 ms
64 bytes from 192.168.235.128: icmp_seq=16 ttl=64 time=0.023 ms
64 bytes from 192.168.235.128: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 192.168.235.128: icmp_seq=18 ttl=64 time=0.023 ms
64 bytes from 192.168.235.128: icmp_seq=19 ttl=64 time=0.061 ms
64 bytes from 192.168.235.128: icmp_seq=20 ttl=64 time=0.060 ms
64 bytes from 192.168.235.128: icmp_seq=21 ttl=64 time=0.062 ms
64 bytes from 192.168.235.128: icmp_seq=22 ttl=64 time=0.030 ms
```

- Verify ICMP Packets are Being Dropped:

```
(root@kali)-[~]
# sudo tail -f /var/log/snort/alert_fast.txt
04/08-18:06:14.876695 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:15.901320 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:16.924700 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:17.952646 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:18.972537 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:19.996537 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/08-18:06:21.020530 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 192.168.235.128
04/09-09:32:56.825669 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 10.40.0.73 → 192.168.235.128
04/09-09:33:00.328101 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 10.40.0.73 → 192.168.235.128
04/09-09:33:03.319277 [**] [1:1000001:1] "ICMP Ping Detected" [**] [Priority: 0] {ICMP} 10.40.0.73 → 192.168.235.128
```

Conclusion:

Snort was successfully installed and configured to operate in both IDS and IPS modes:

- In **IDS mode**, it generated alerts upon detecting ICMP packets.
- In **IPS mode**, it effectively **blocked ICMP traffic**, as verified through ping failure and corresponding log entries.