



Task 5 Report: Intrusion Detection Using Snort 3 (Kali Linux)

Objective

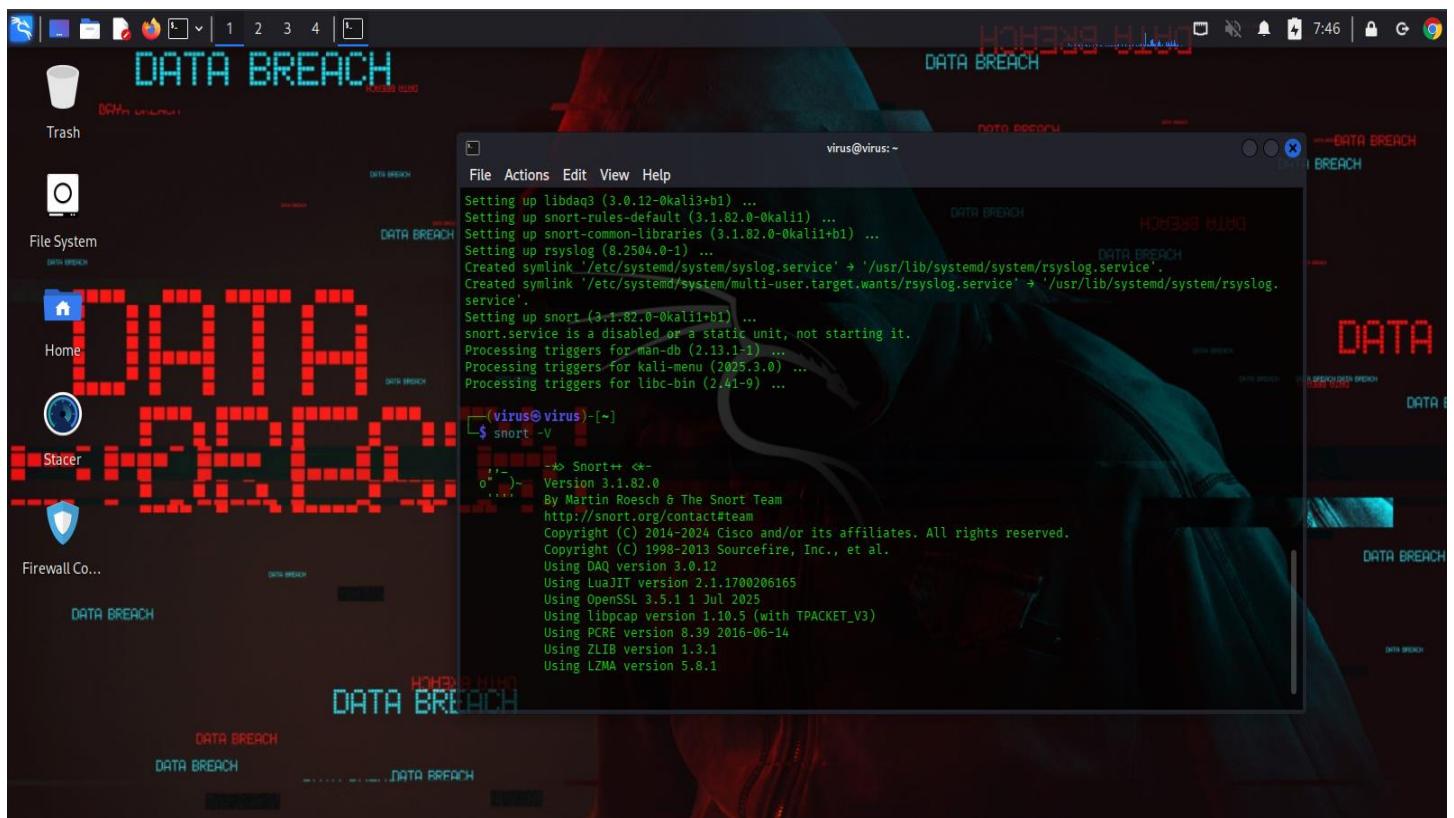
Deploy and configure **Snort 3** (an Intrusion Detection System) on **Kali Linux**, test its functionality by detecting ICMP traffic (ping), and verify real-time detection through console alerts.

System Details

- **Operating System:** Kali Linux (x86_64)
- **Snort Version:** Snort++ 3.1.82.0
- **Network Interface Used:** eth0 (or auto-detected based on system)
- **Root Access:** Yes

Installation & Setup Summary

Mentioned in file : Snort3-installation.docx



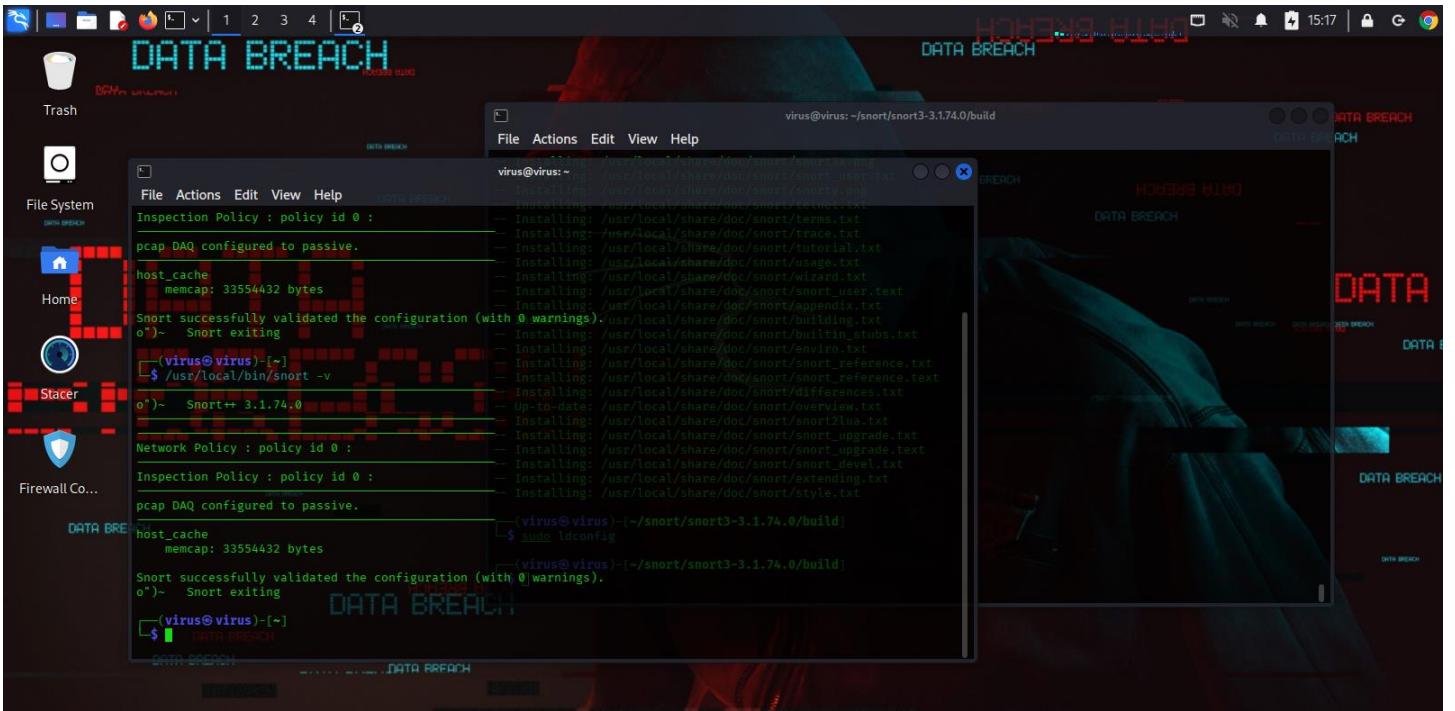
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'virus@virus:~' and contains the following text:

```

File Actions Edit View Help
Setting up libdaq3 (3.0.12-0kali3+b1) ...
Setting up snort-rules-default (3.1.82.0-0kali1) ...
Setting up snort-common-libraries (3.1.82.0-0kali1+b1) ...
Setting up rsyslog (8.2504.0-1) ...
Created symlink '/etc/systemd/system/syslog.service' → '/usr/lib/systemd/system/rsyslog.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/rsyslog.service' → '/usr/lib/systemd/system/rsyslog.service'.
Setting up snort (3.1.82.0-0kali1+b1) ...
snort.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
Processing triggers for libc-bin (2.41-9) ...

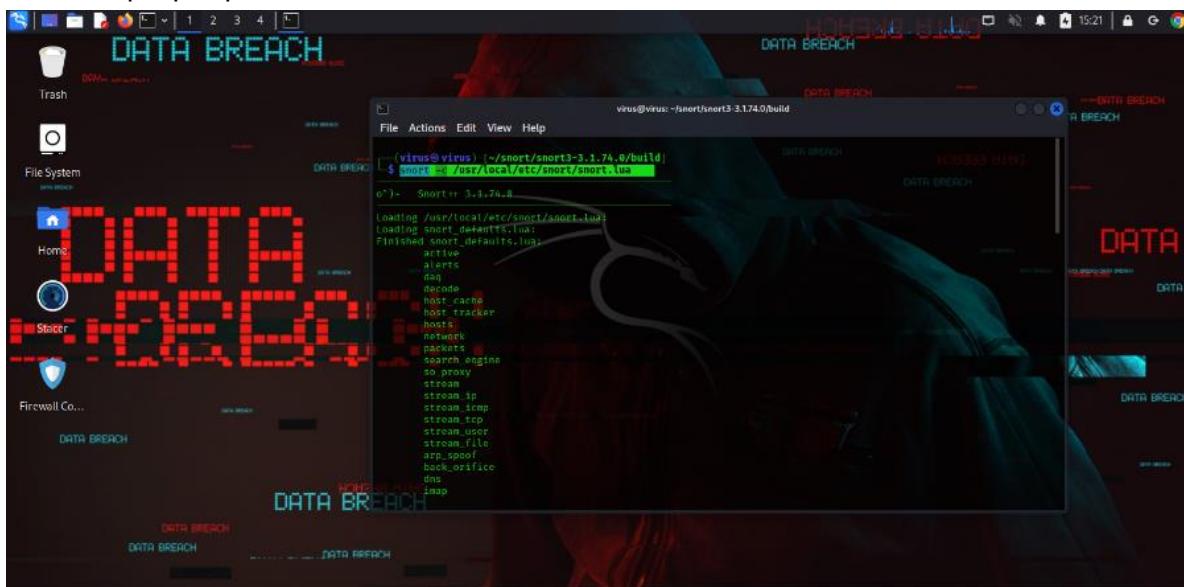
(virus@virus:~)-
$ snort -V
--> Snort++ <-
o'`-- Version 3.1.82.0
By Martin Roesch & The Snort Team
http://snort.org/contact#team
Copyright (C) 2014-2024 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using DAQ version 3.0.12
Using LuaIT version 2.1.1700206165
Using OpenSSL 3.5.1 1 Jul 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 5.8.1

```



⚙️ Configuration Summary

- Created a custom rule file at:
- /usr/local/etc/snort/snort.lua
- Added the following custom local rule to detect ICMP echo requests:
- alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)
- Ensured proper path to the rule file and rule activation in snort.lua.



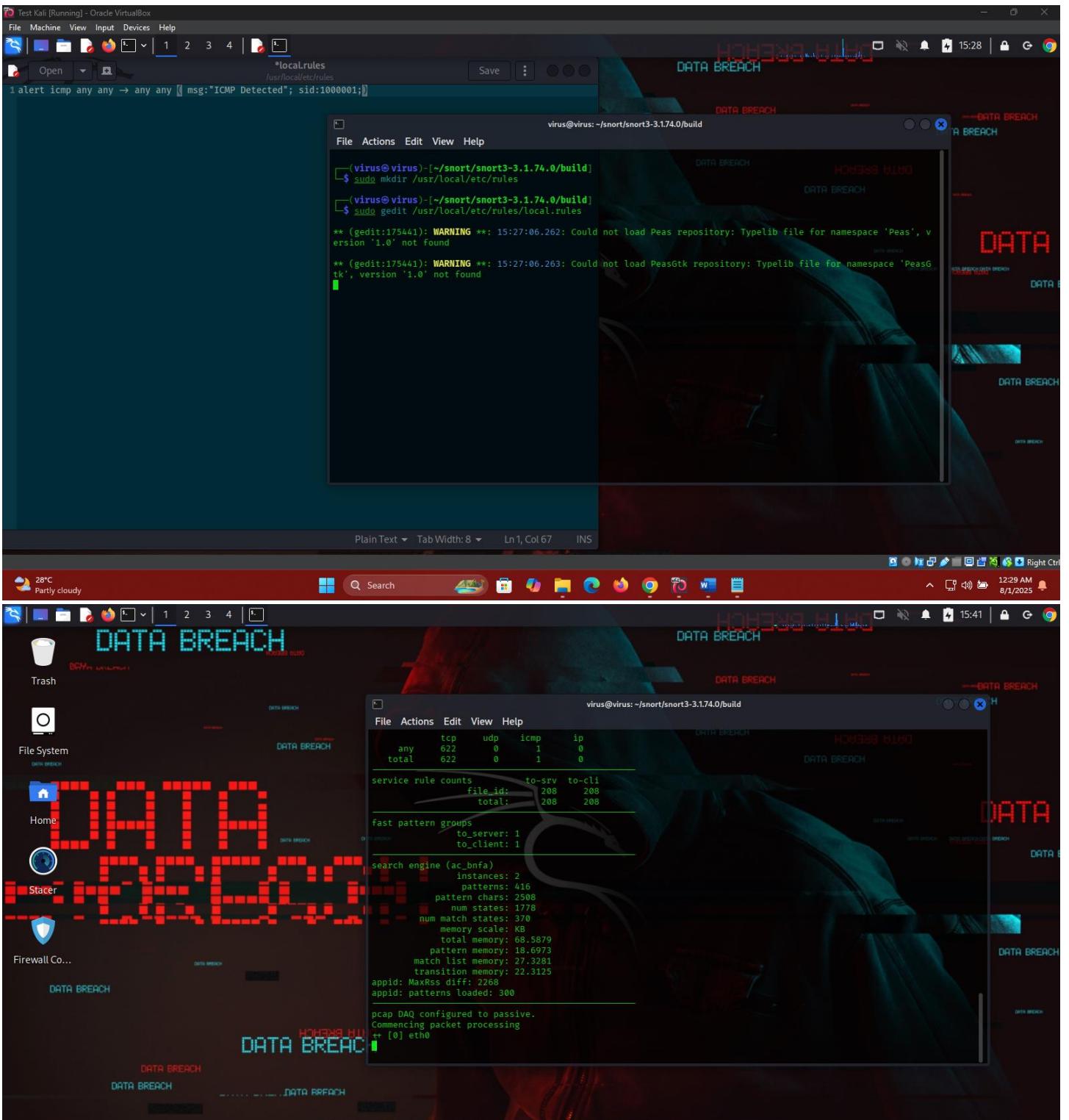
```
*snort.lua
/usr/local/etc/snort

5 -- there are over 200 modules available to tune your policy.
6 -- many can be used with defaults w/o any explicit configuration.
7 -- use this conf as a template for your specific configuration.
8
9 -- 1. configure defaults
10 -- 2. configure inspection
11 -- 3. configure bindings
12 -- 4. configure performance
13 -- 5. configure detection
14 -- 6. configure filters
15 -- 7. configure outputs
16 -- 8. configure tweaks
17
18 --
19 -- 1. configure defaults
20
21
22 -- HOME_NET and EXTERNAL_NET must be set now
23 -- setup the network addresses you are protecting
24 HOME_NET = '192.168.0.0/24'
25
26 -- set up the external network addresses.
27 -- (leave as "any" in most situations)
28 EXTERNAL_NET = 'any'
29
30 include 'snort_defaults.lua'
31
32 --
33 -- 2. configure inspection
34
35
36 mod = { } uses internal defaults
37 -- you can see them with snort --help-module mod
38
39 -- mod = default_mod uses external defaults
40 -- you can see them in snort_defaults.lua
41
42 -- the following are quite capable with defaults.
```

```
virus@virus: ~/snort/snort3-3.1.74.0/build
File Actions Edit View Help
[virus@virus:~/snort/snort3-3.1.74.0/build]$ sudo mkdir /usr/local/etc/rules
[virus@virus:~/snort/snort3-3.1.74.0/build]$ sudo gedit /usr/local/etc/rules/local.rules
** (gedit:175441): WARNING **: 15:27:06.262: Could not load Peas repository: Typelib file for namespace 'Peas', version '1.0' not found
** (gedit:175441): WARNING **: 15:27:06.263: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', version '1.0' not found
[virus@virus:~/snort/snort3-3.1.74.0/build]$ sudo gedit /usr/local/etc/snort/snort.lua
** (gedit:178366): WARNING **: 15:33:10.520: Could not load Peas repository: Typelib file for namespace 'Peas', version '1.0' not found
** (gedit:178366): WARNING **: 15:33:10.520: Could not load PeasGtk repository: Typelib file for namespace 'PeasGtk', version '1.0' not found
```

A screenshot of a Kali Linux desktop environment. The desktop background features a dark, abstract design with the word "DATA BREACH" repeated in red and blue. The desktop icons include a trash can, file system, Home, Stacer, and Firewall Co... The taskbar at the bottom shows various application icons like FileZilla, Firefox, and terminal. A central terminal window is open with the command "virus@virus: ~/snort/snort3-3.1.74.0/build" and displays the following output:

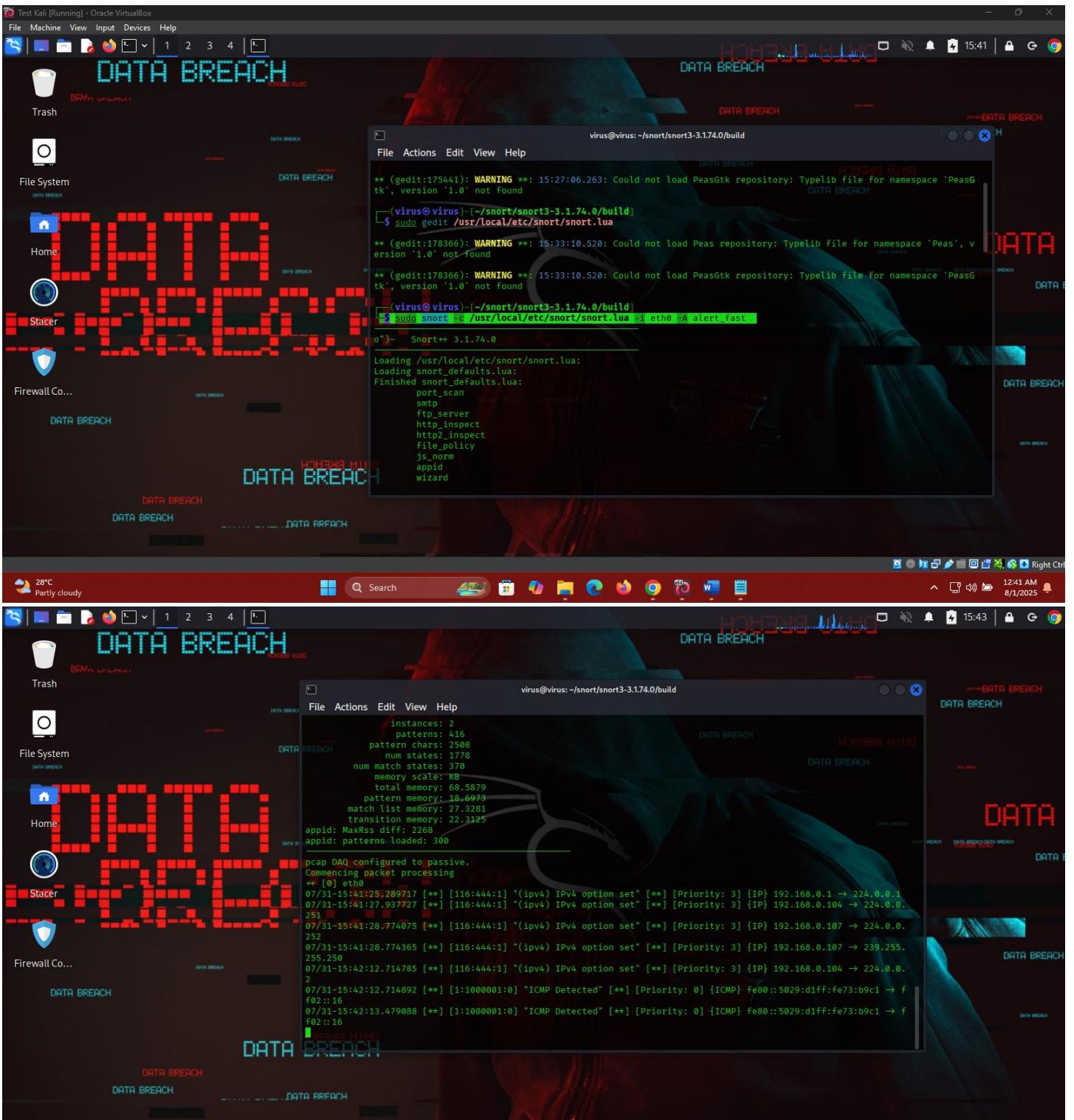
```
service rule counts          to-srv   to-clt  
                                file_id: 208    208  
                                total: 208    208  
  
fast pattern groups           to_server: 1  
                                to_client: 1  
  
search engine (ac_bnfa)       instances: 2  
                                patterns: 416  
                                pattern chars: 2508  
                                num states: 1778  
                                num match states: 370  
                                memory scale: K0  
                                total memory: 68.5879  
                                pattern memory: 18.6973  
                                match_list memory: 27.3281  
                                transition memory: 22.3125  
appid: MaxRss diff: 2220  
appid: patterns loaded: 300  
  
pcap DAQ configured to passive.  
  
Snort successfully validated the configuration (with 0 warnings).  
o")- Snort exiting
```



Running Snort in IDS Mode

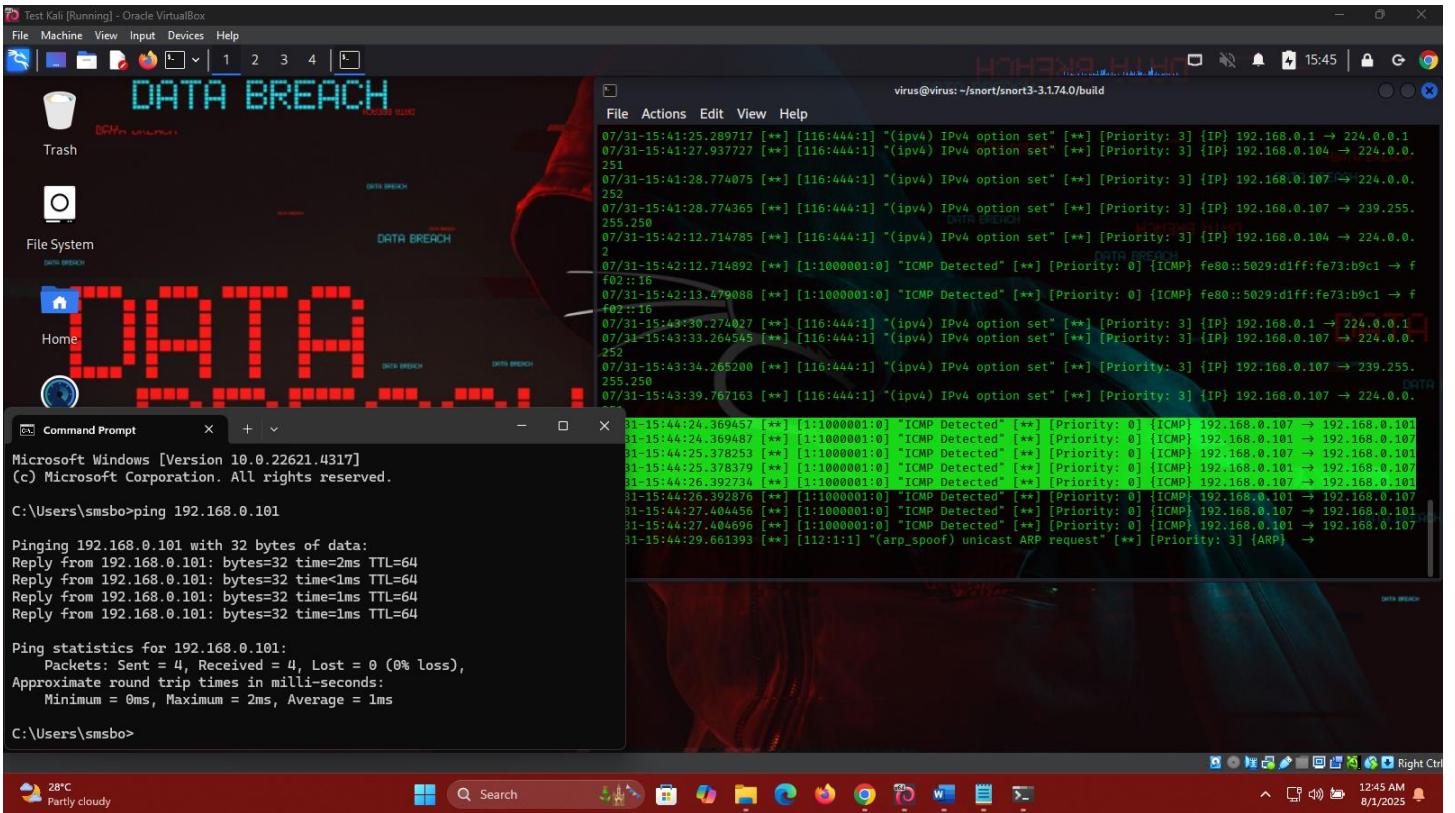
Used this command to start Snort on the correct interface:

```
sudo snort -c /usr/local/etc/snort/snort.lua -i eth0 -A alert_fast
```



Testing & Validation

- **Test Performed:** ICMP Echo Request (ping) from another machine or localhost.
- **Result:** Snort detected ICMP traffic as expected.

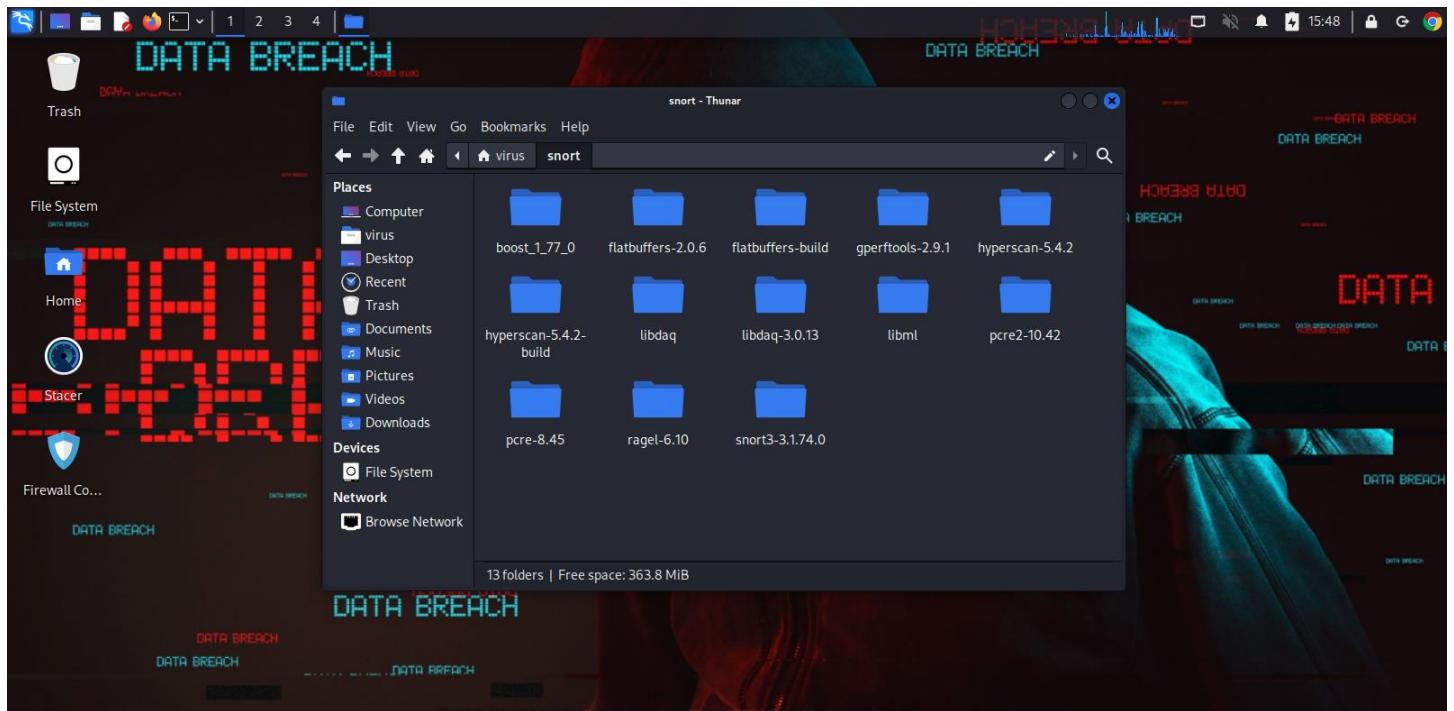


Observations & Notes

- Snort 3 offers modular Lua-based configuration and better performance over Snort 2.x.
- Manual compilation ensures the latest version with custom tuning.
- Rule writing is simple and powerful — even a single-line rule can detect critical traffic types.
- ICMP was used here for demonstration; however, Snort can detect thousands of attacks with the right rule sets (e.g., community or ET rules).
- For production use, Snort should be integrated with a logging backend or GUI (e.g., PulledPork, Snorby, Wazuh).

Conclusion

The task was successfully completed by installing, configuring, and testing **Snort 3** as a basic IDS on Kali Linux. ICMP traffic detection confirms functional setup. This lays the foundation for more advanced intrusion detection and network monitoring in future tasks.



THE END

SYED MUHAMMAD SHAH