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

## Objective

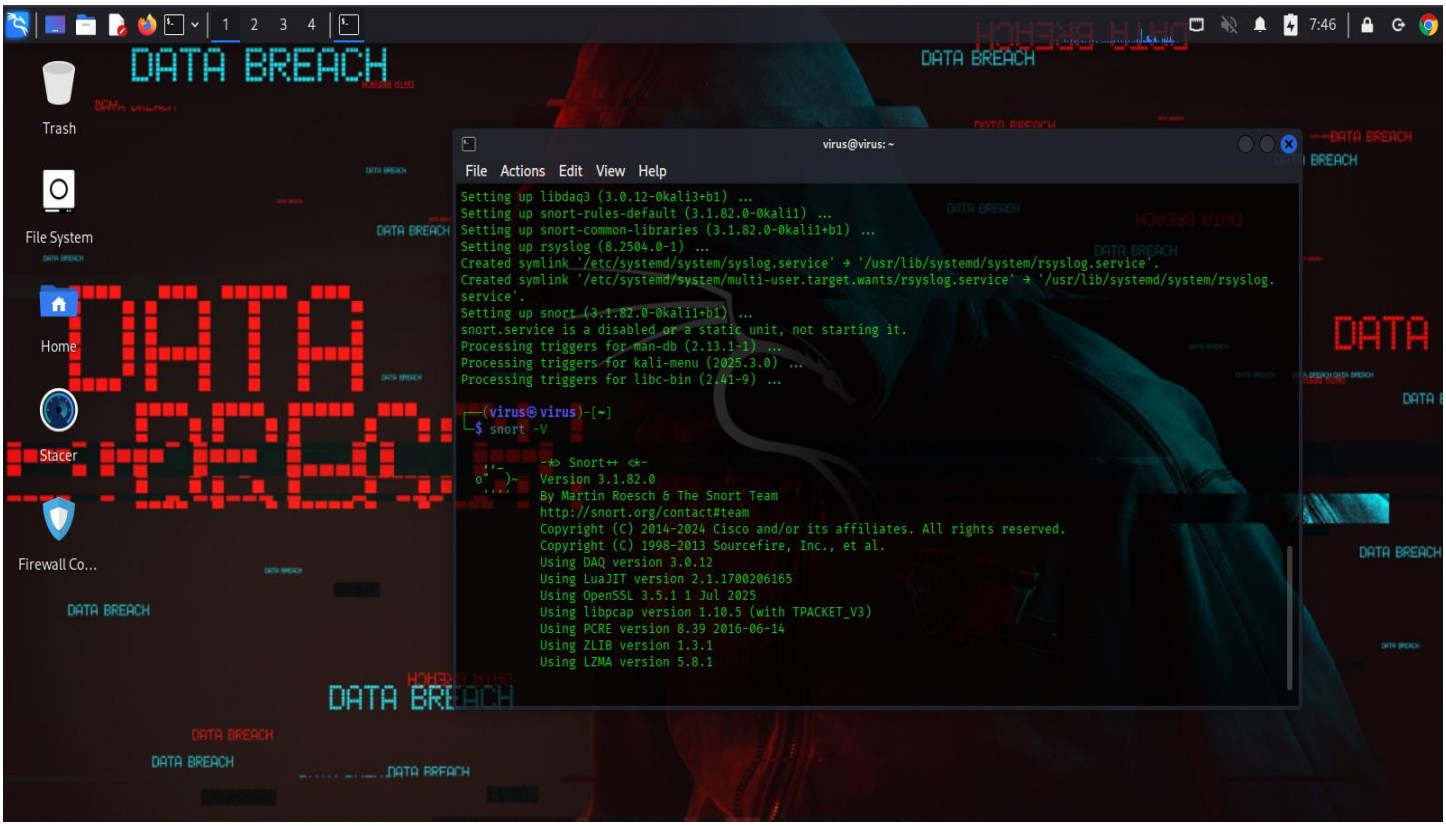
Deploy and configure **Snort 3** (an Intrusion Detection System) on **Kali Linux**, test its functionality by detecting ICMP traffic (ping), and verify real-time detection through console alerts.

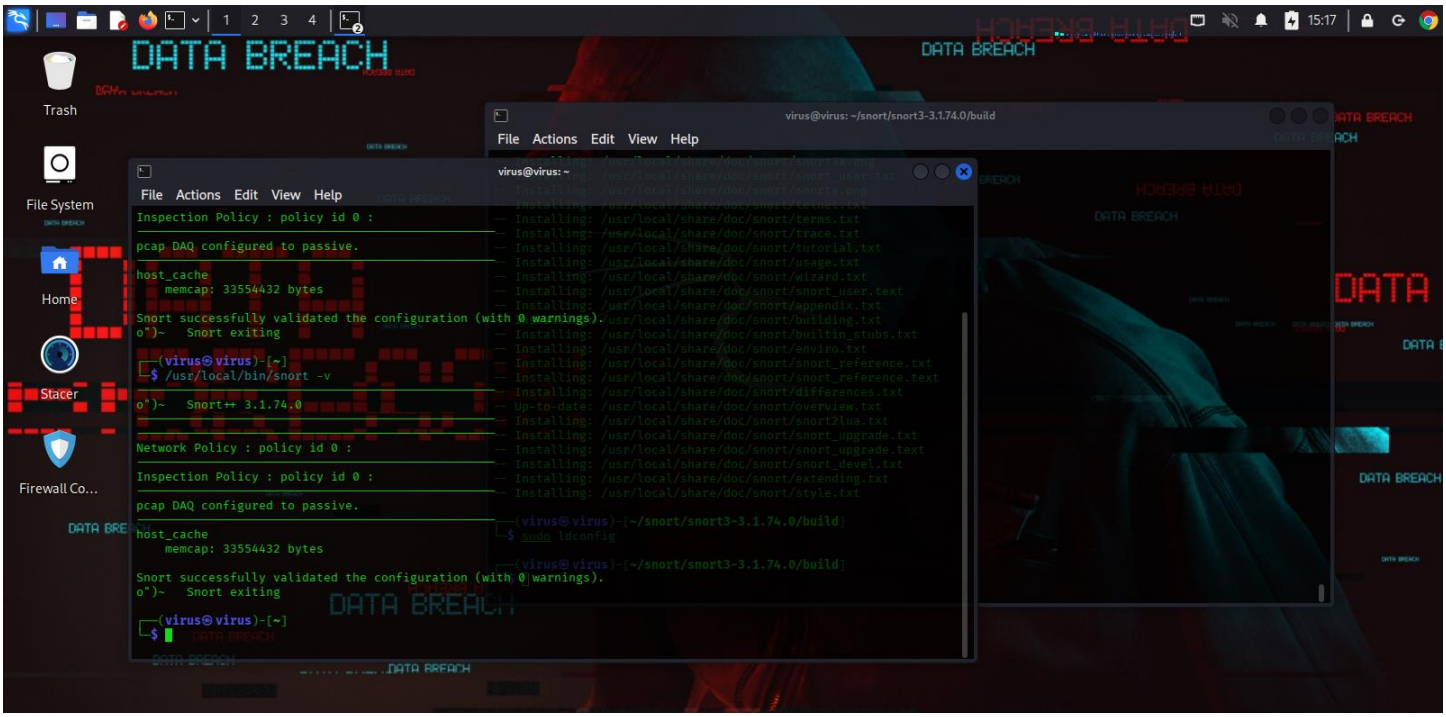
## System Details

- **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

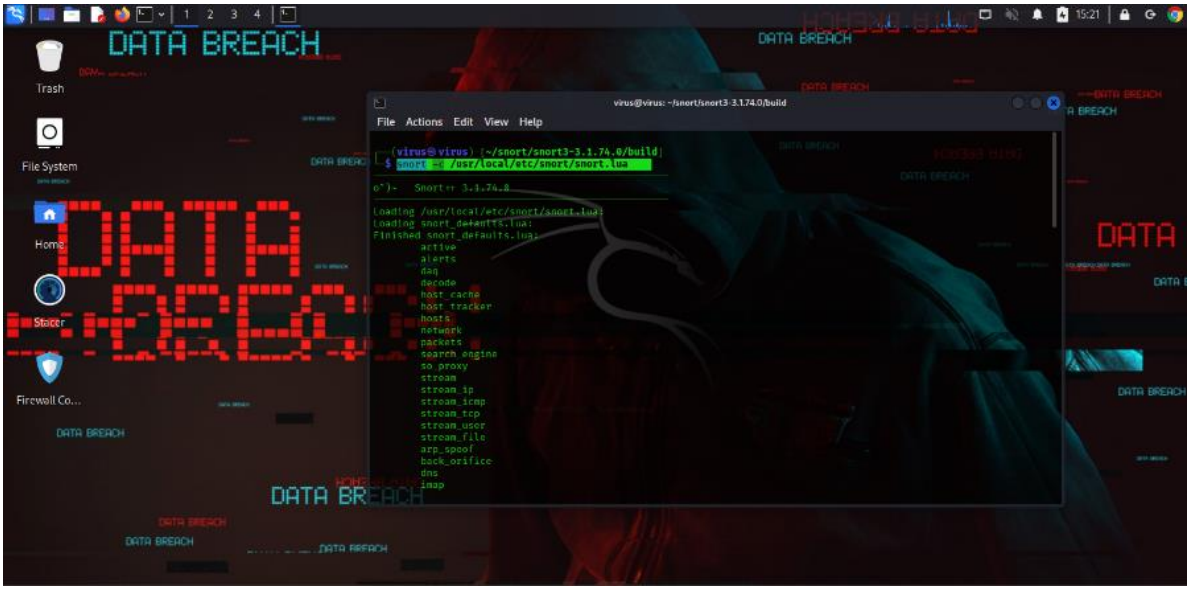
**Mentioned in file : Snort3-installation.docx**

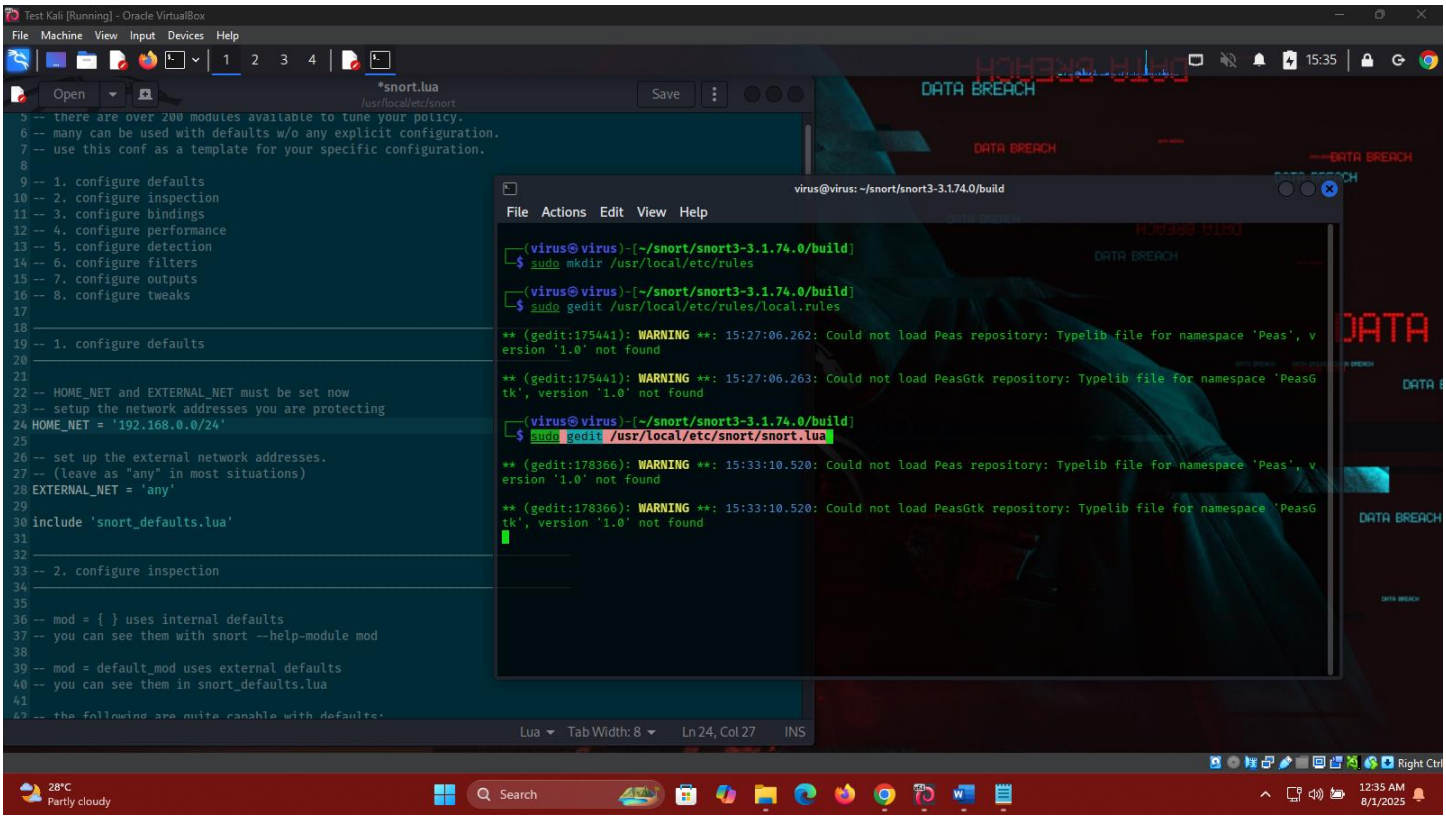


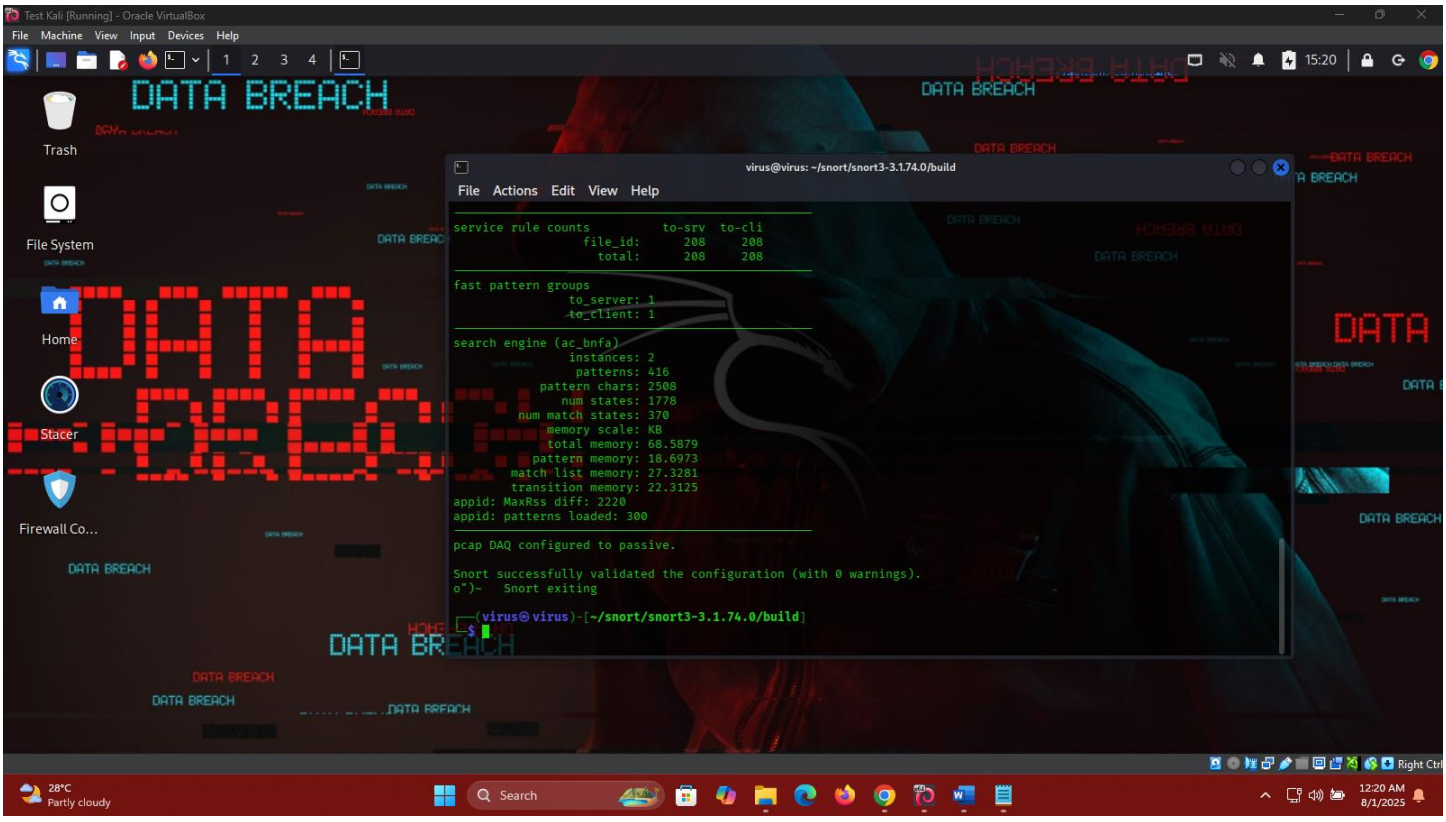


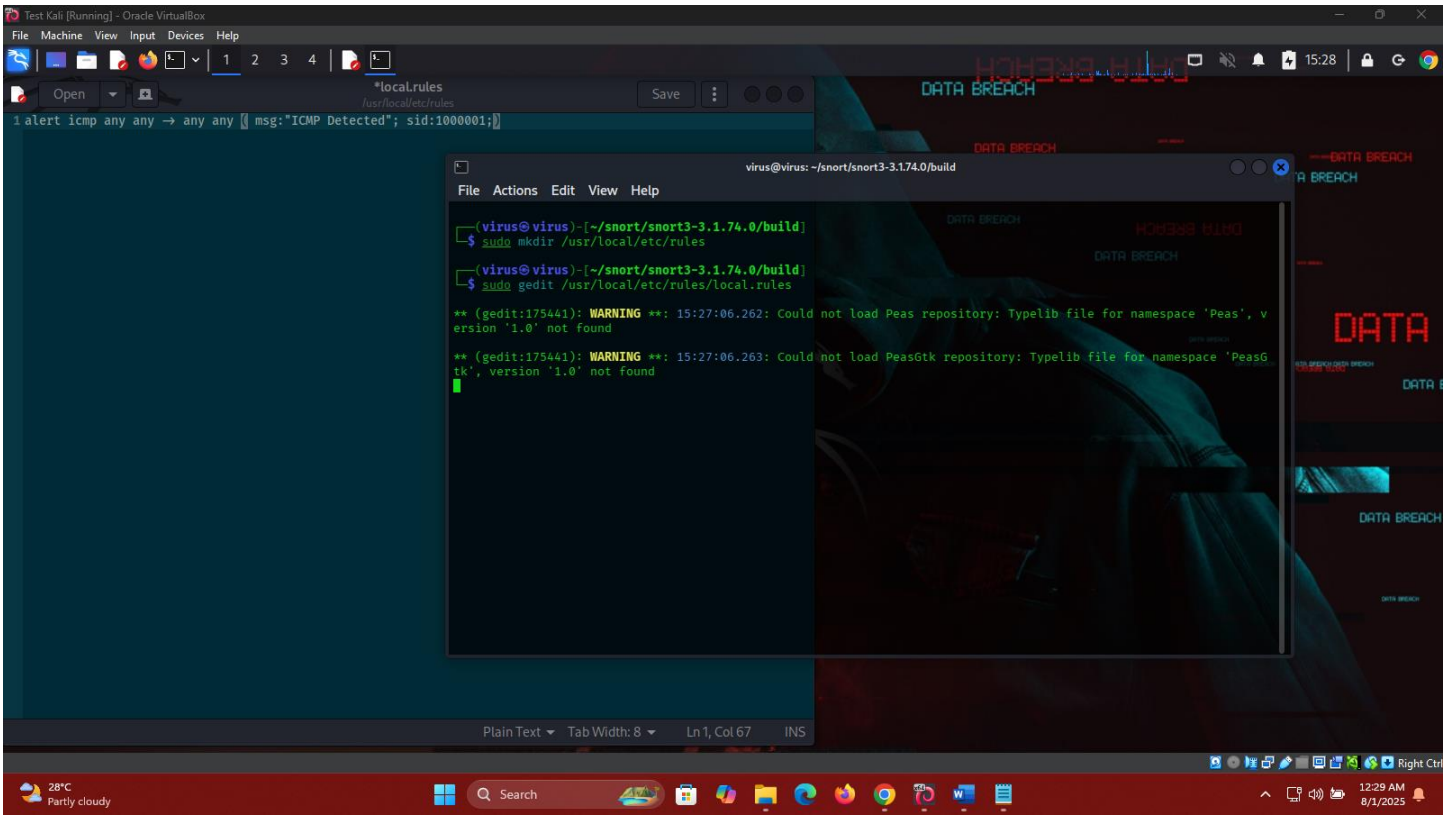

## ⚙ Configuration Summary

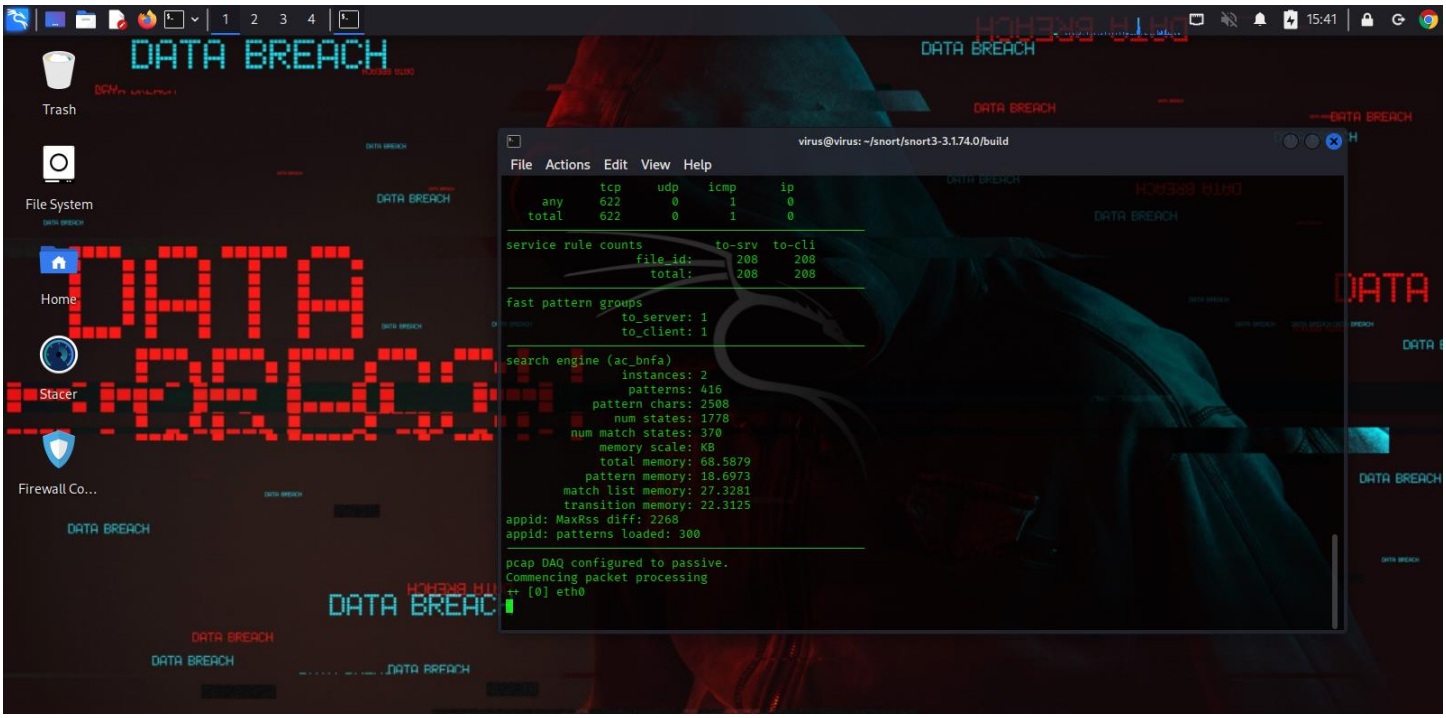
- Created a custom rule file at:
- /usr/local/etc/snort/snort.lua
- Added the following custom local rule to detect ICMP echo requests:
- alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)
- Ensured proper path to the rule file and rule activation in snort.lua.




Test Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
*snort.lua
/usr/local/etc/snort
Open
Save
-- there are over 200 modules available to tune your policy.
-- many can be used with defaults w/o any explicit configuration.
-- use this conf as a template for your specific configuration.
-- 1. configure defaults
-- 2. configure inspection
-- 3. configure bindings
-- 4. configure performance
-- 5. configure detection
-- 6. configure filters
-- 7. configure outputs
-- 8. configure tweaks
-- 1. configure defaults
-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = '192.168.0.0/24'
-- set up the external network addresses.
-- (leave as "any" in most situations)
EXTERNAL_NET = 'any'
include 'snort_defaults.lua'
-- 2. configure inspection
-- mod = { } uses internal defaults
-- you can see them with snort --help-module mod
-- mod = default_mod uses external defaults
-- you can see them in snort_defaults.lua
Lua Tab Width: 8 Ln 24, Col 27 INS
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
28°C Partly cloudy
Search
12:35 AM 8/1/2025


Test Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
Stacer
Firewall Co...
virus@virus: ~/snort/snort3-3.1.74.0/build
File Actions Edit View Help
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)
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: 2220
appid: patterns loaded: 300
pcap DAQ configured to passive.
Snort successfully validated the configuration (with 0 warnings).
o")~ Snort exiting
(virus㉿virus)-[~/snort/snort3-3.1.74.0/build]
$
28°C Partly cloudy
Search
12:20 AM 8/1/2025



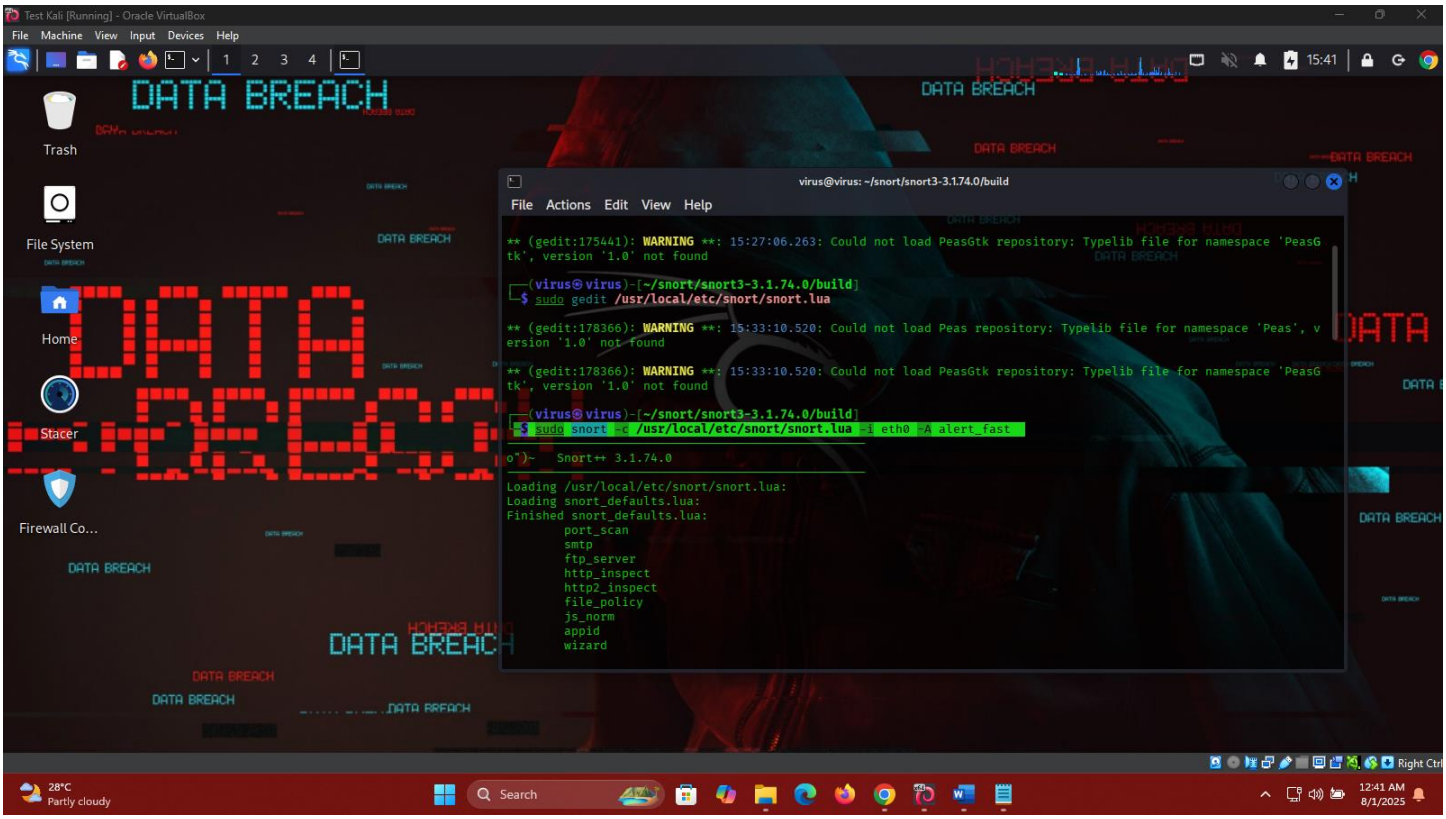



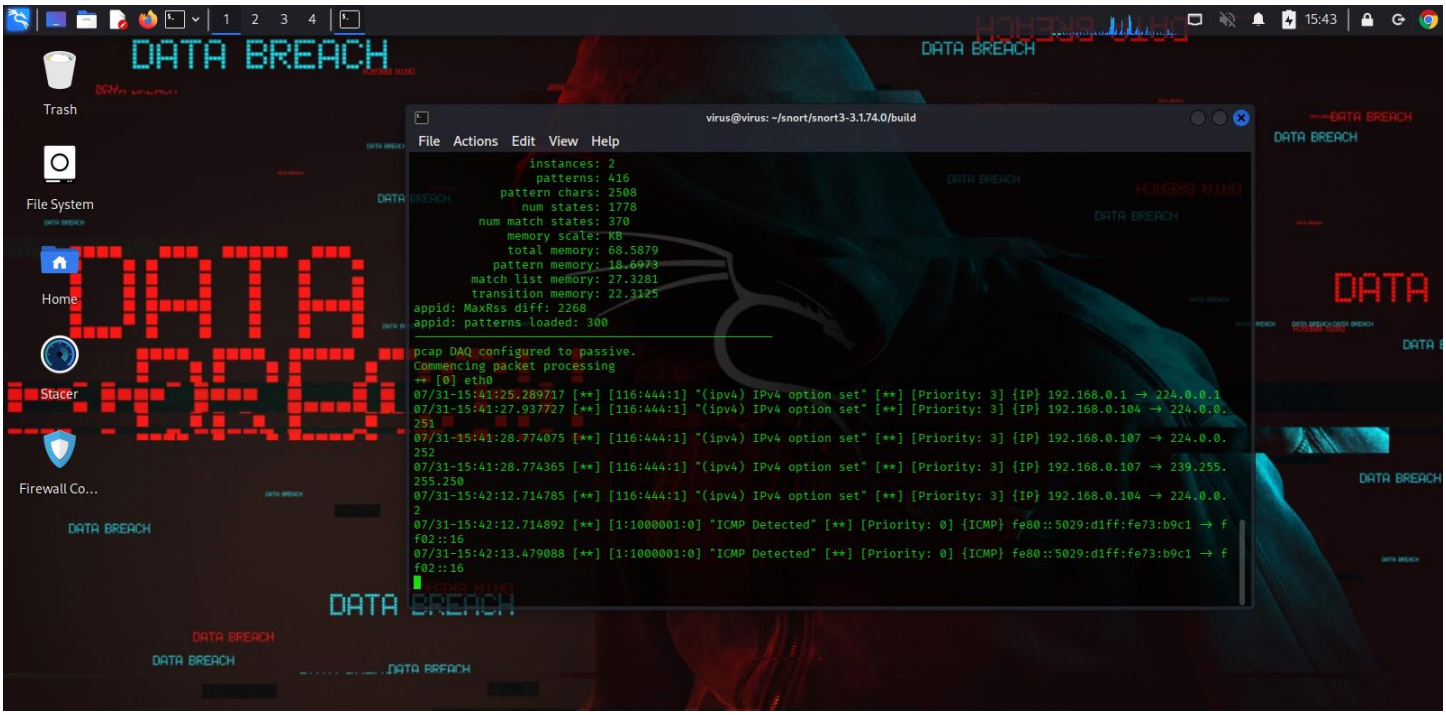

---

### 📡 Running Snort in IDS Mode

Used this command to start Snort on the correct interface:

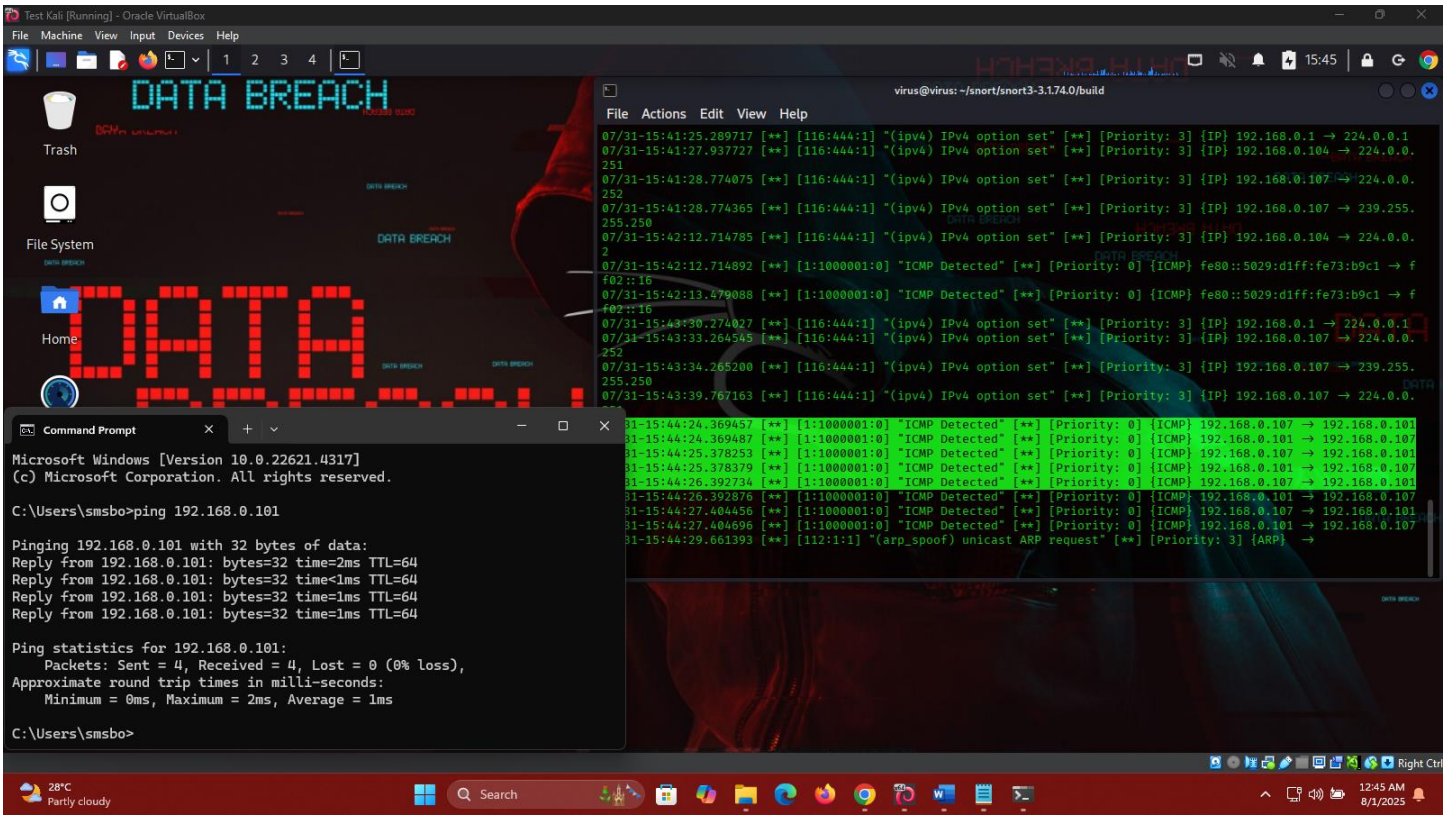
sudo snort -c /usr/local/etc/snort/snort.lua -i eth0 -A alert_fast




## Testing & Validation

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




---

## 📌 Observations & Notes

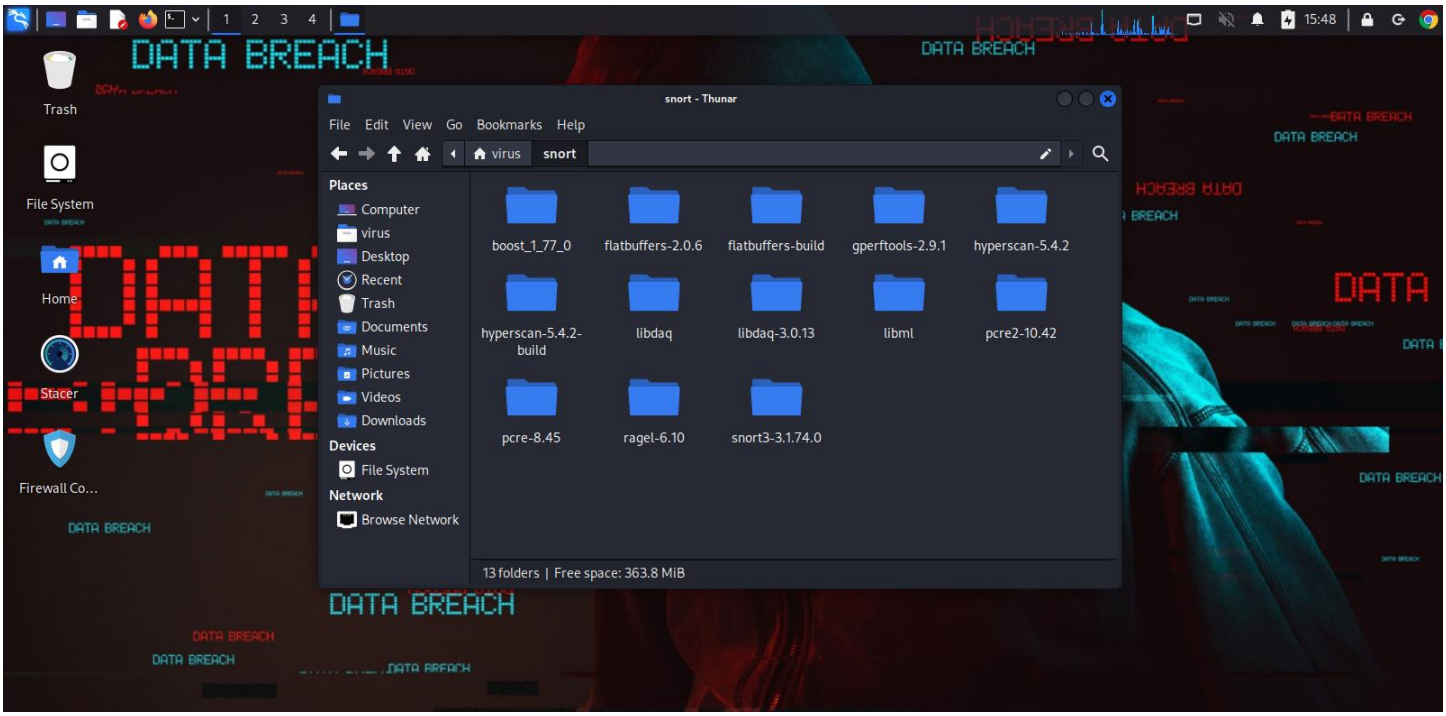
- Snort 3 offers modular Lua-based configuration and better performance over Snort 2.x.
- Manual compilation ensures the latest version with custom tuning.
- Rule writing is simple and powerful — even a single-line rule can detect critical traffic types.
- ICMP was used here for demonstration; however, 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