Ubuntu Snort – IDS Project

- The **Snort Project** is an open-source network intrusion detection and prevention system (IDS/IPS) developed by **Martin Roesch** in 1998 and maintained by **Cisco** since its acquisition of Sourcefire in 2013. Snort is widely used for real-time traffic analysis and packet logging to detect and prevent cyber threats.

Key Features of Snort

1. **Packet Sniffing & Logging**
   - Captures and logs network traffic for detailed analysis.
2. **Intrusion Detection System (IDS)**
   - Analyzes traffic in real-time to detect malicious activity based on predefined rules.
3. **Intrusion Prevention System (IPS)**
   - Blocks or alerts on suspicious activity, preventing cyber threats from reaching the system.
4. **Signature-Based Detection**
   - Uses a vast database of attack signatures to identify known threats.
5. **Protocol Analysis & Anomaly Detection**
   - Inspects traffic for irregular behavior, helping to detect zero-day attacks.
6. **Flexible Rule-Based Language**
   - Allows users to define custom detection rules.

How Snort Works

1.Traffic Capture:

1. Snort captures packets from the network interface.

2.Packet Decoding:

1. It decodes the captured data to extract headers and payloads.

3.Rule Matching:

1. Compares packet data against a set of predefined Snort rules.

4.Action Execution:

1. Based on rules, Snort can log, alert, or block suspicious traffic.

Snort Modes

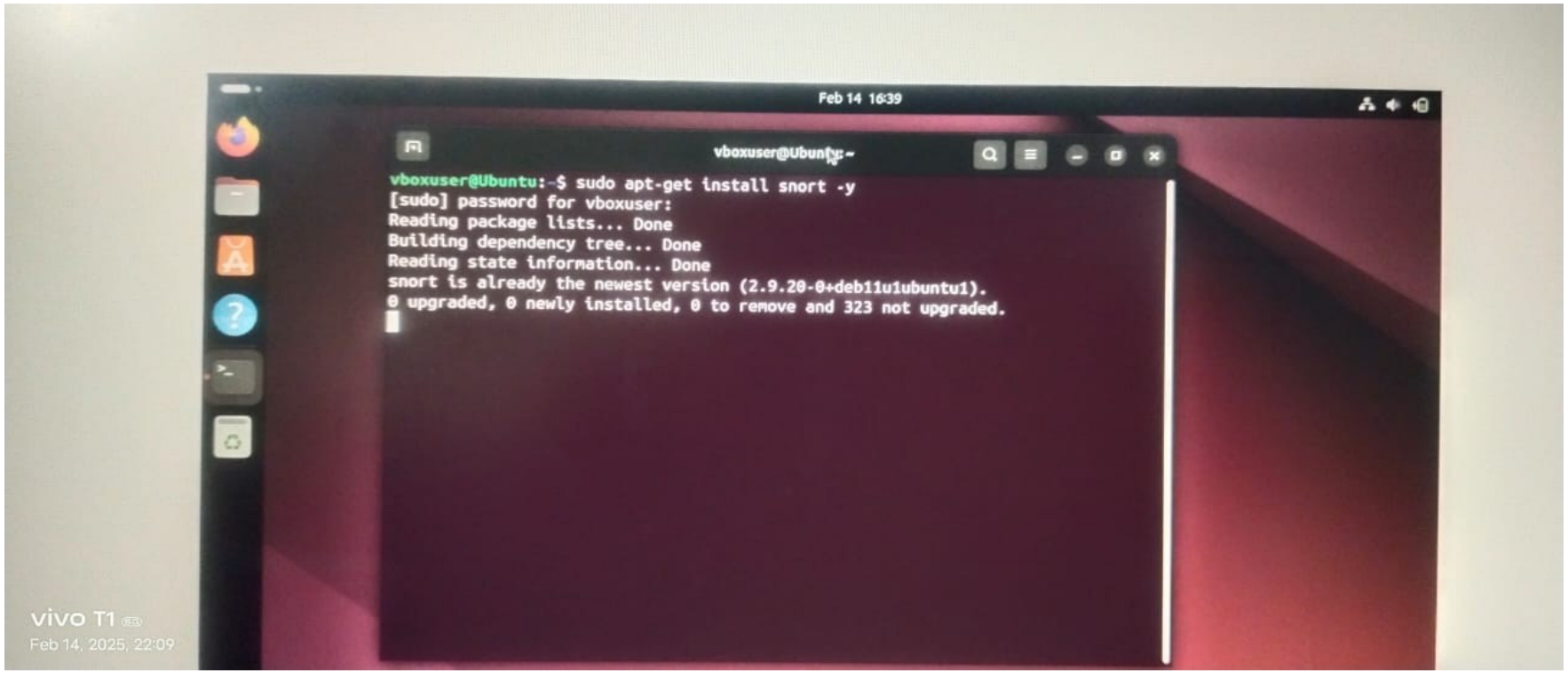
•**Sniffer Mode:** Reads network packets and displays them in real time.

•**Packet Logger Mode:** Logs packets for later analysis.

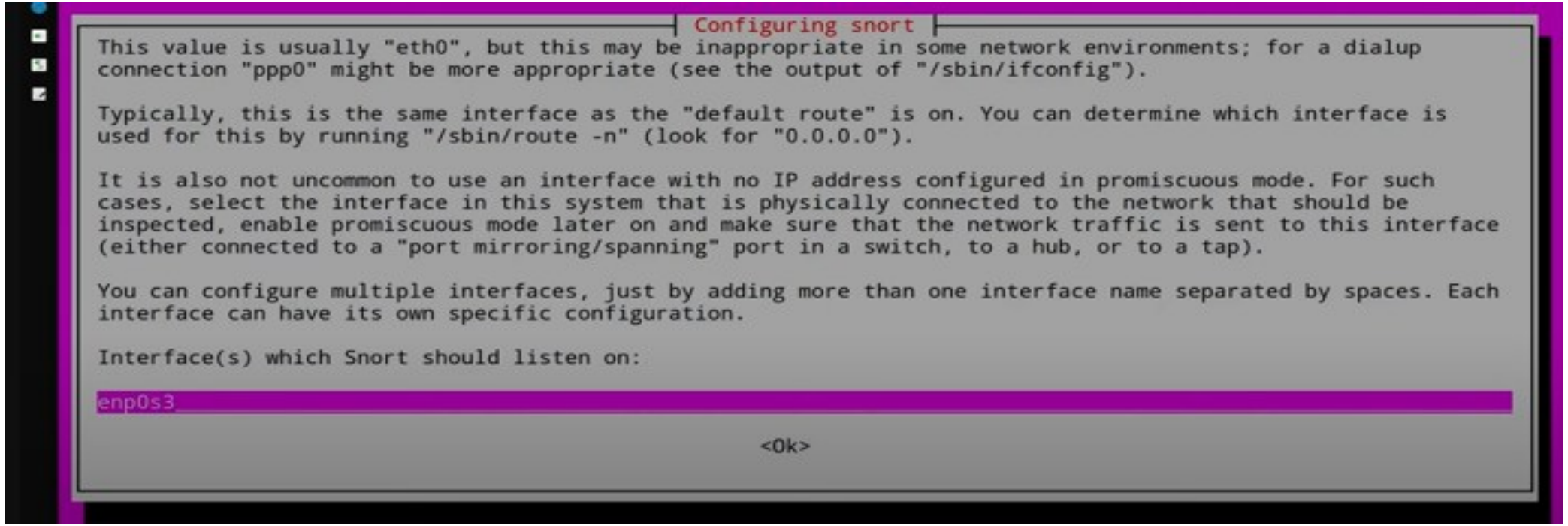
•**Network Intrusion Detection System (NIDS) Mode:** Detects and alerts on suspicious activity.

Getting Started With SNORT

- Download and Configure Linux or windows, here we using Ubuntu Linux system.
- Installing Snort -

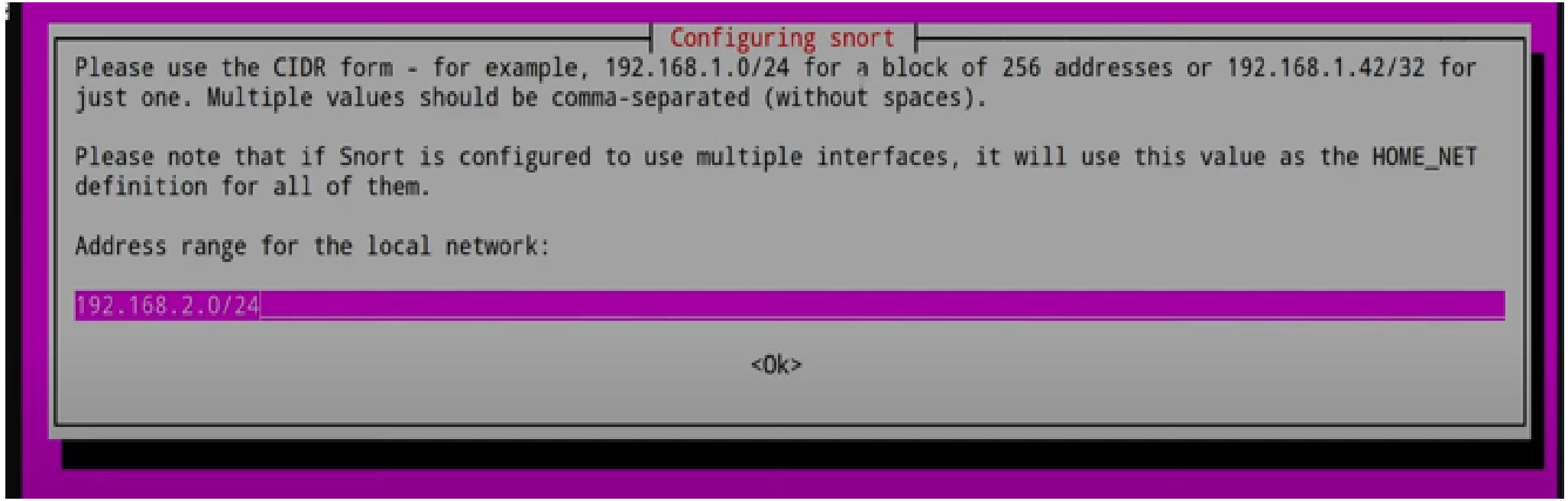


Config Interface while installing SNORT

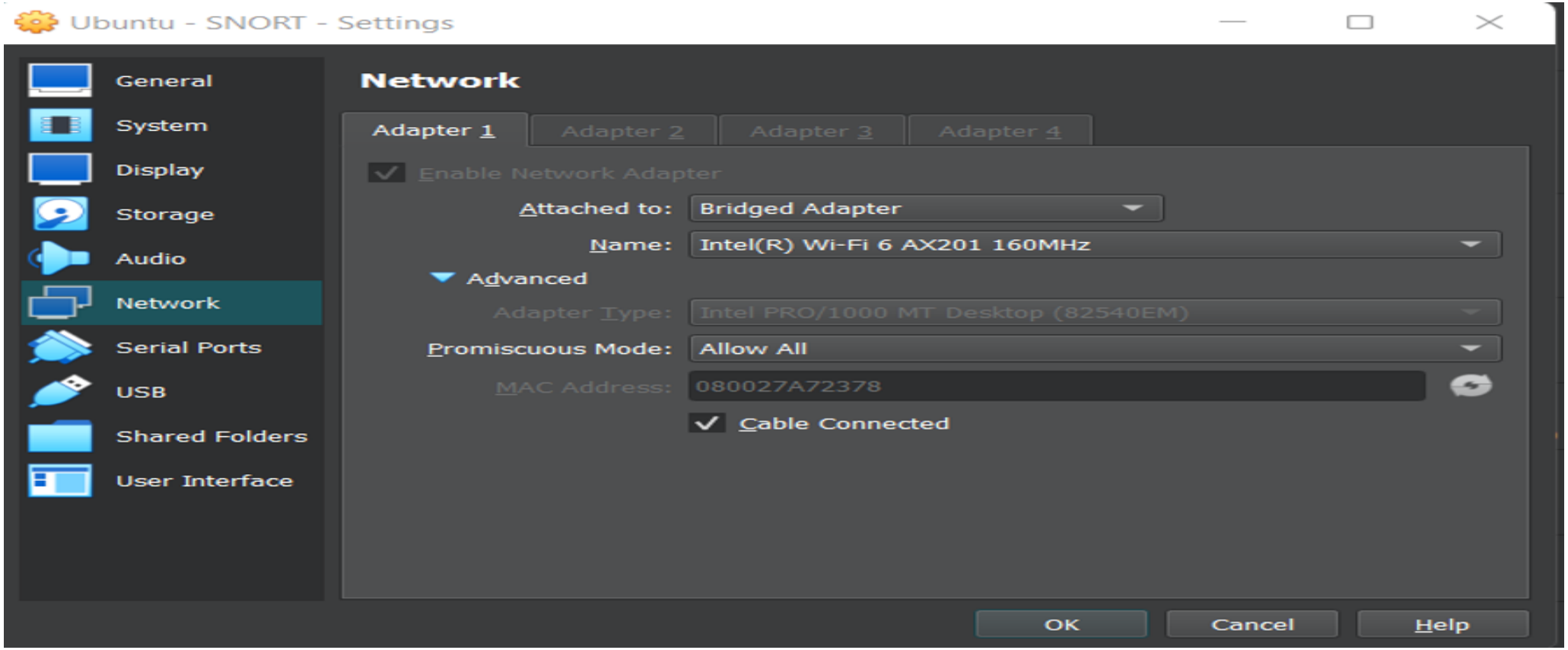


Config $HOME_NET while installing SNORT –

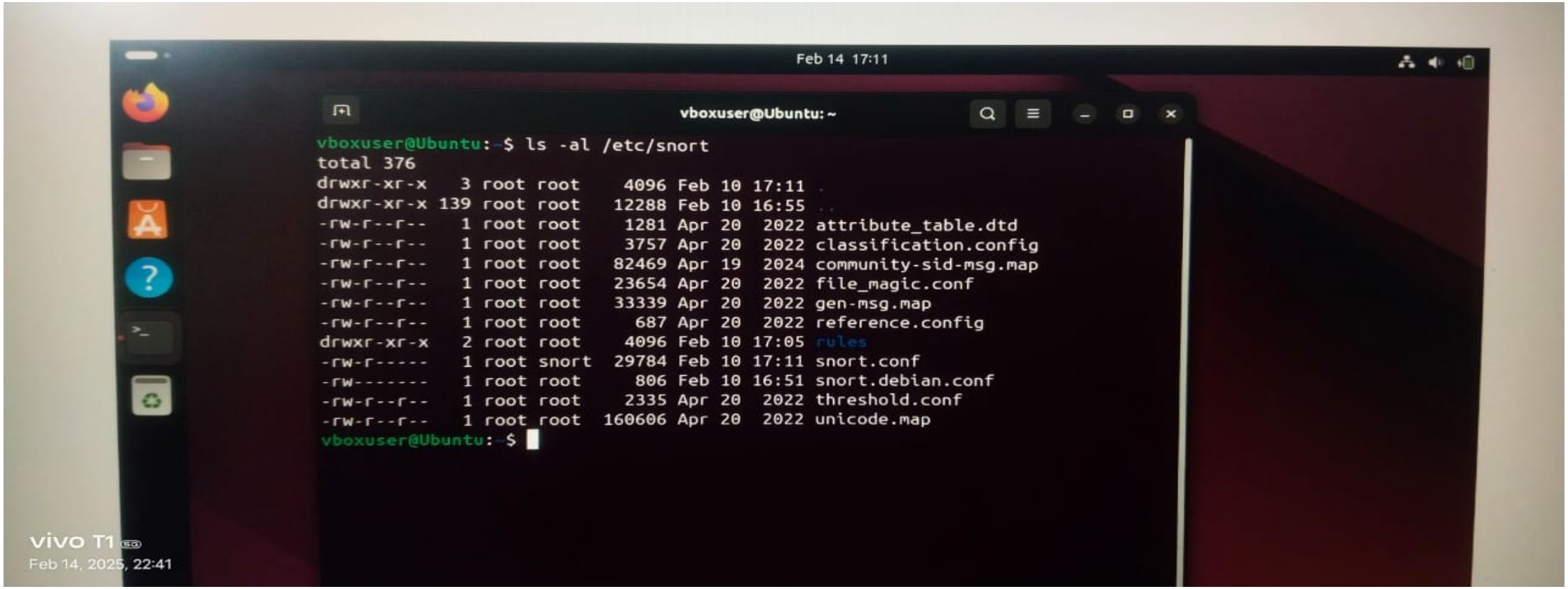
- Open another terminal, type **ifconfig** and note the **inet** in **enp0s3.** Enter the IP in configuring snort given down the example.



Promiscuous mode in SNORT -

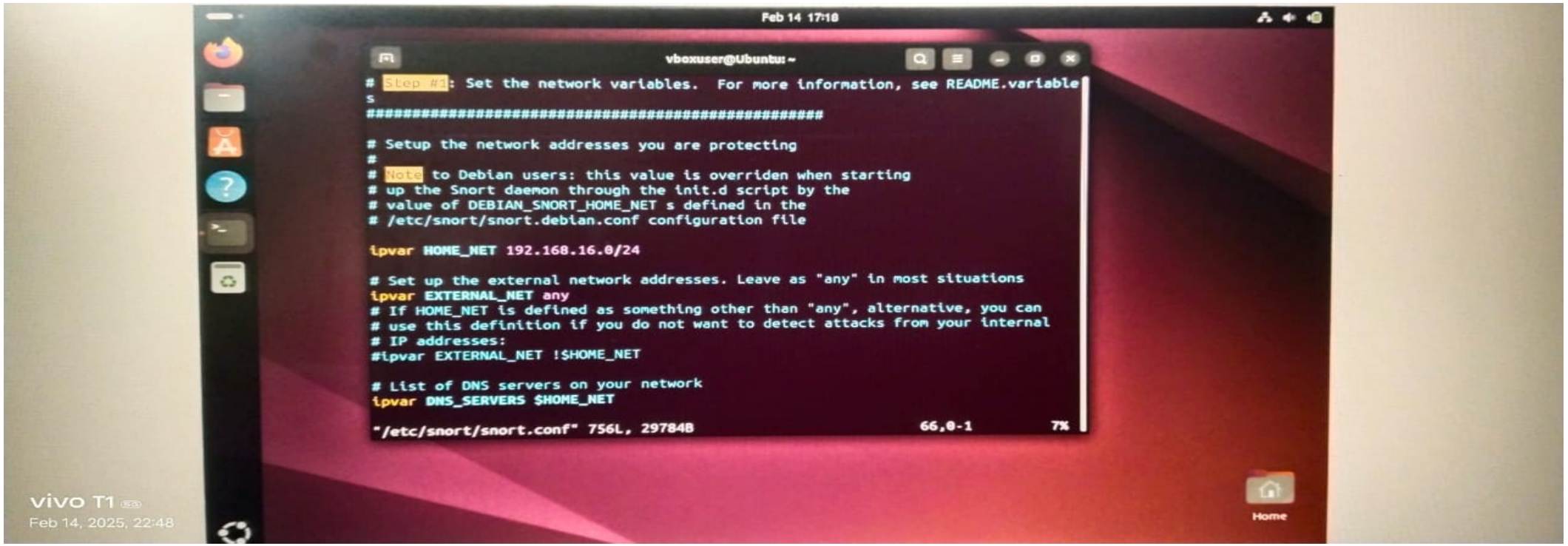


Config file –


Feb 14 17:11
vboxuser@Ubuntu: ~
vboxuser@Ubuntu:~$ ls -al /etc/snort
total 376
drwxr-xr-x 3 root root 4096 Feb 10 17:11 .
drwxr-xr-x 139 root root 12288 Feb 10 16:55 ..
-rw-r--r-- 1 root root 1281 Apr 20 2022 attribute_table.dtd
-rw-r--r-- 1 root root 3757 Apr 20 2022 classification.config
-rw-r--r-- 1 root root 82469 Apr 19 2024 community-sid-msg.map
-rw-r--r-- 1 root root 23654 Apr 20 2022 file_magic.conf
-rw-r--r-- 1 root root 33339 Apr 20 2022 gen-msg.map
-rw-r--r-- 1 root root 687 Apr 20 2022 reference.config
drwxr-xr-x 2 root root 4096 Feb 10 17:05 rules
-rw-r----- 1 root snort 29784 Feb 10 17:11 snort.conf
-rw------- 1 root root 806 Feb 10 16:51 snort.debian.conf
-rw-r--r-- 1 root root 2335 Apr 20 2022 threshold.conf
-rw-r--r-- 1 root root 160606 Apr 20 2022 unicode.map
vboxuser@Ubuntu:~$
vivo T1
Feb 14, 2025, 22:41

Install vim editor – sudo apt-get install vim
Now type **sudo vim /etc/snort/snort.conf**

Inside snort.conf, set ipvar to home subnet –



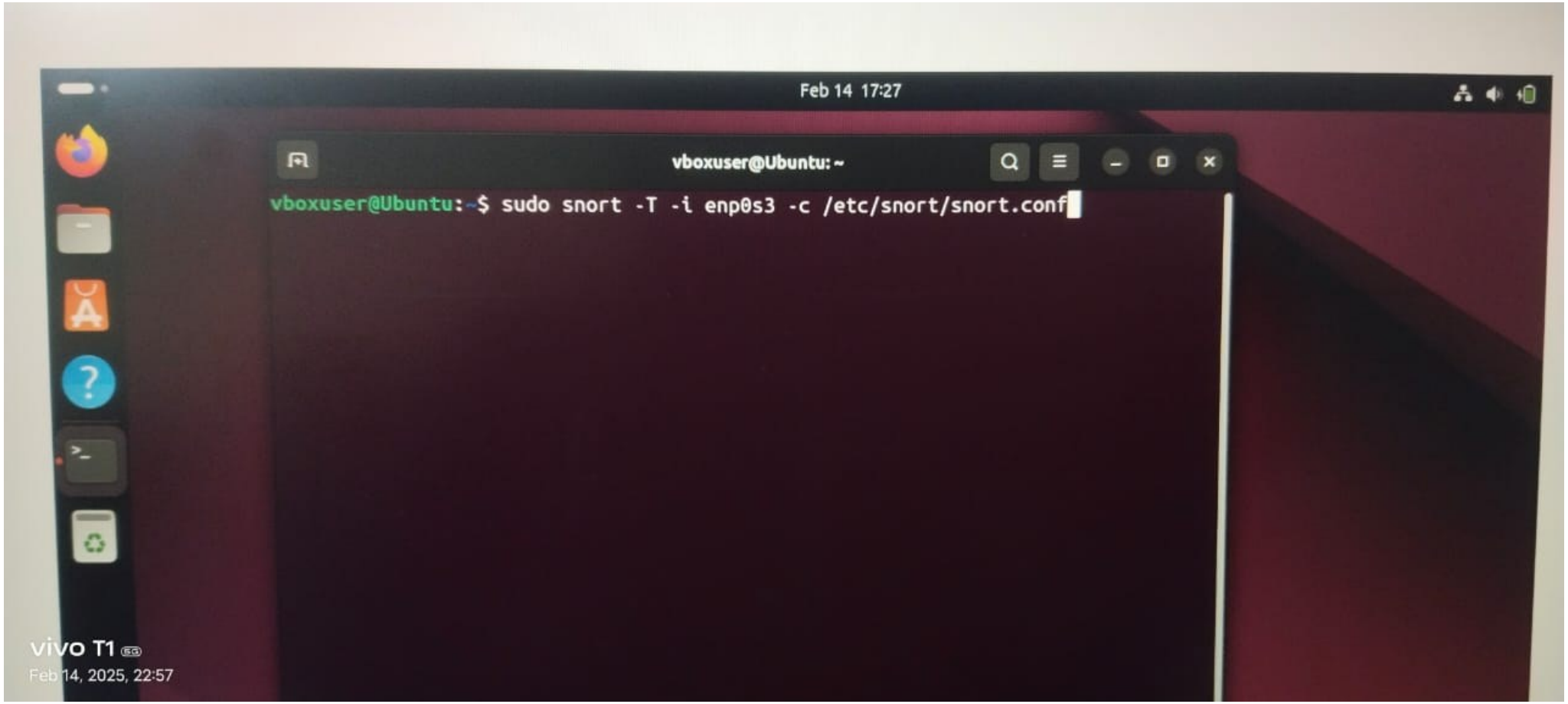
Local.rules file contains rules that we will create -

```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# Note to Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review
# configuration file and re-enable (remove the comment in the fir
# rules files that are available in your system (in the /etc/snor
# directory)

# site specific rules
include $RULE_PATH/local.rules
```

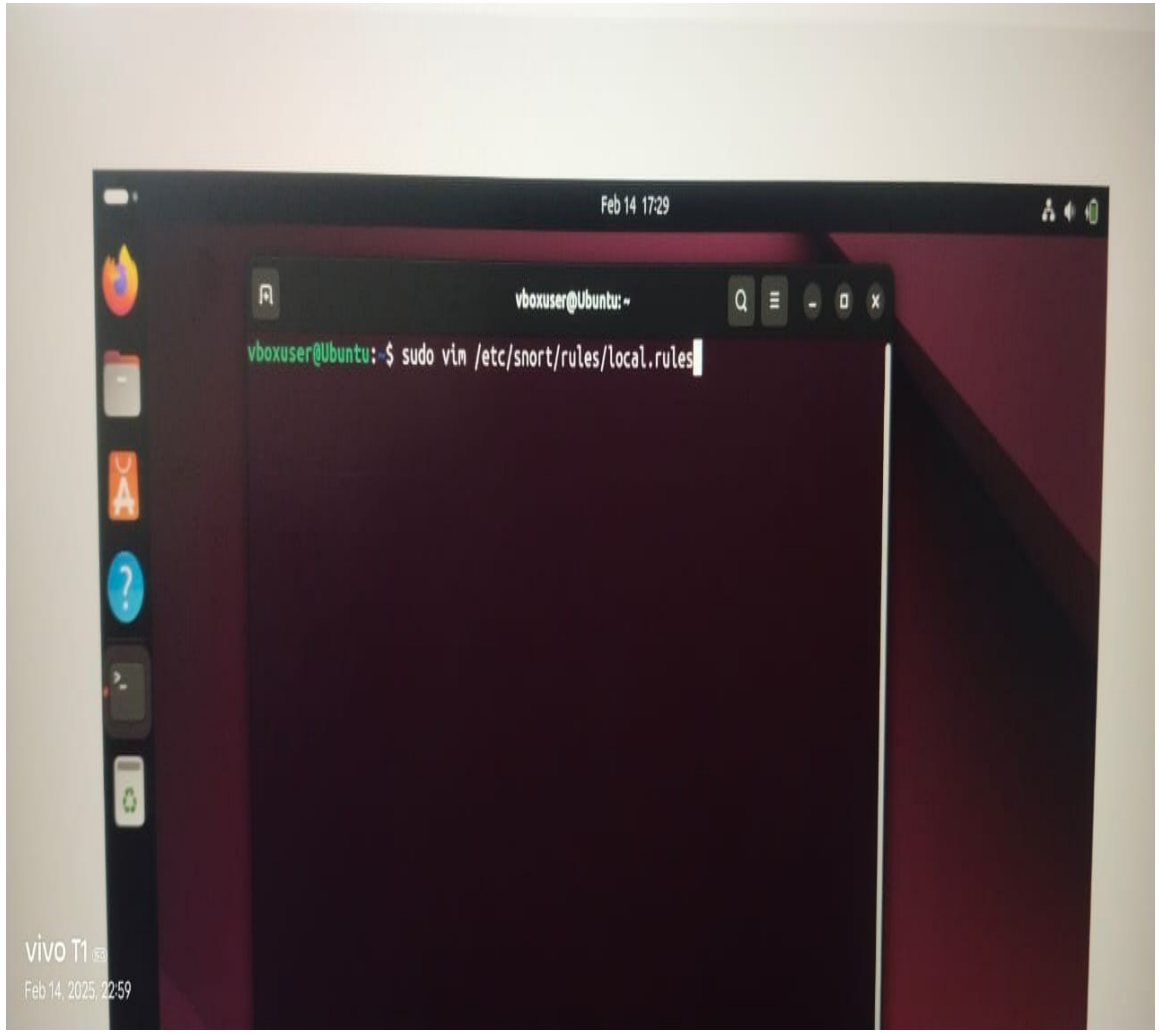
Community rules are disabled and other rules-

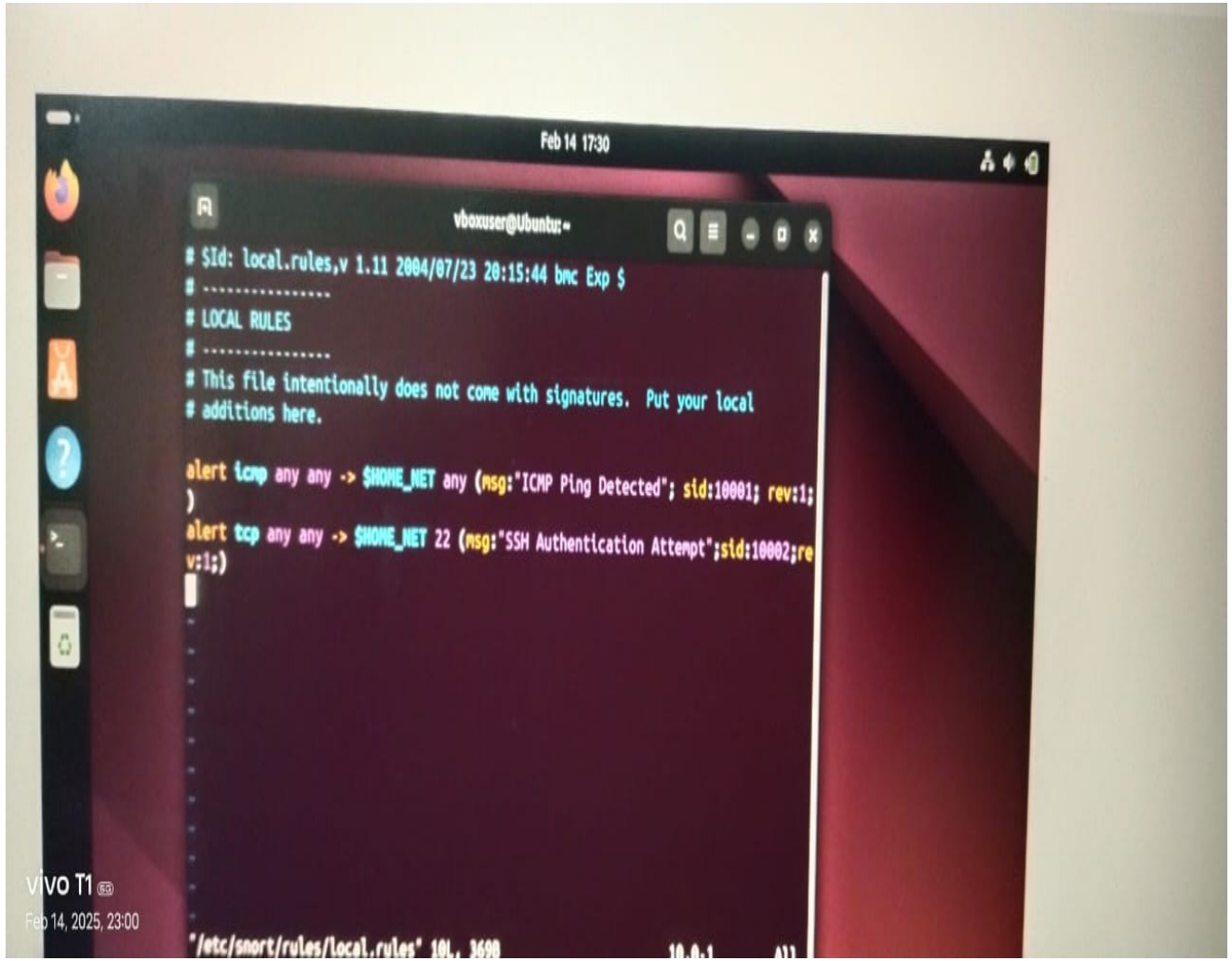
```
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
```

Test config file by running SNORT in self-test mode



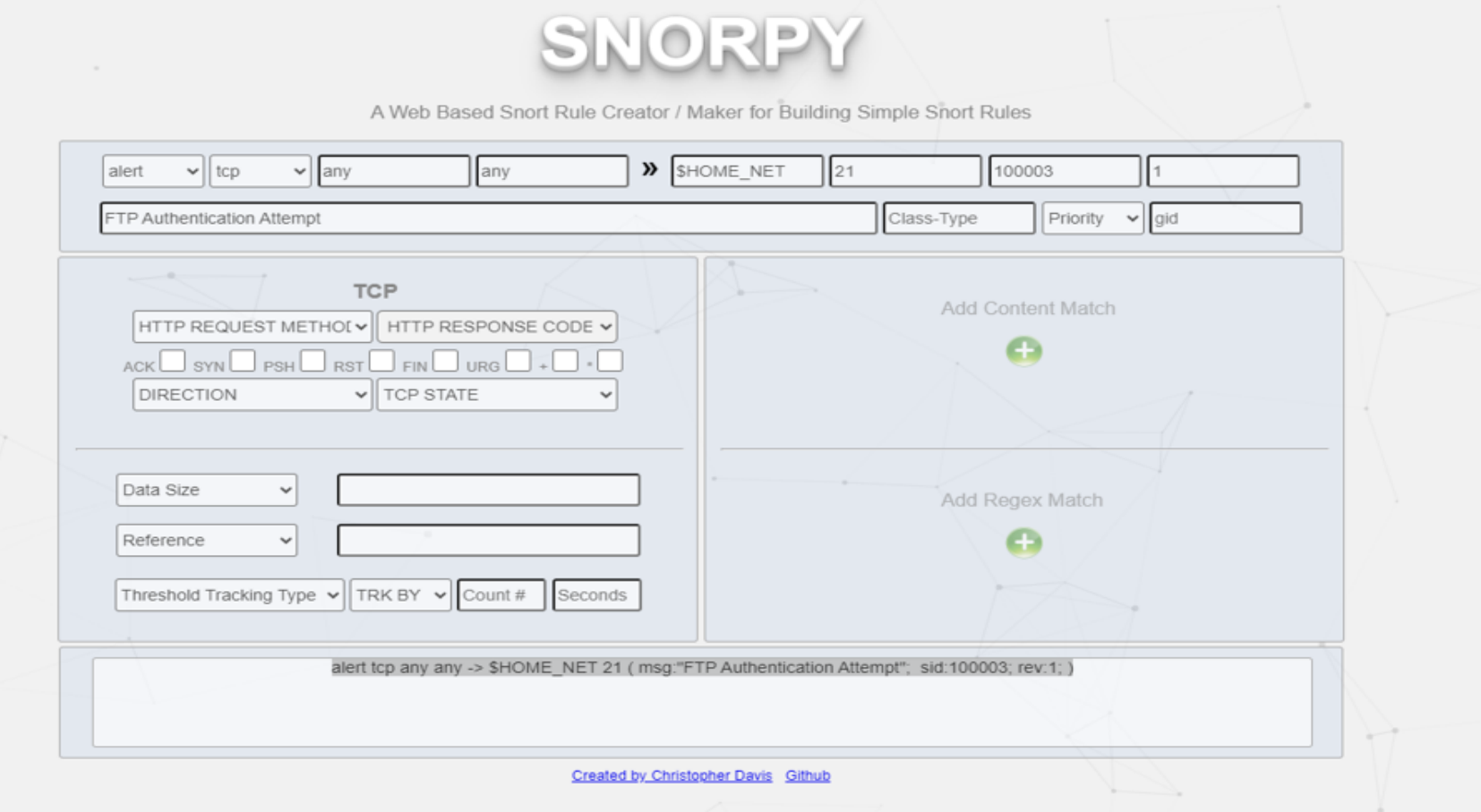
Lets create custom rules



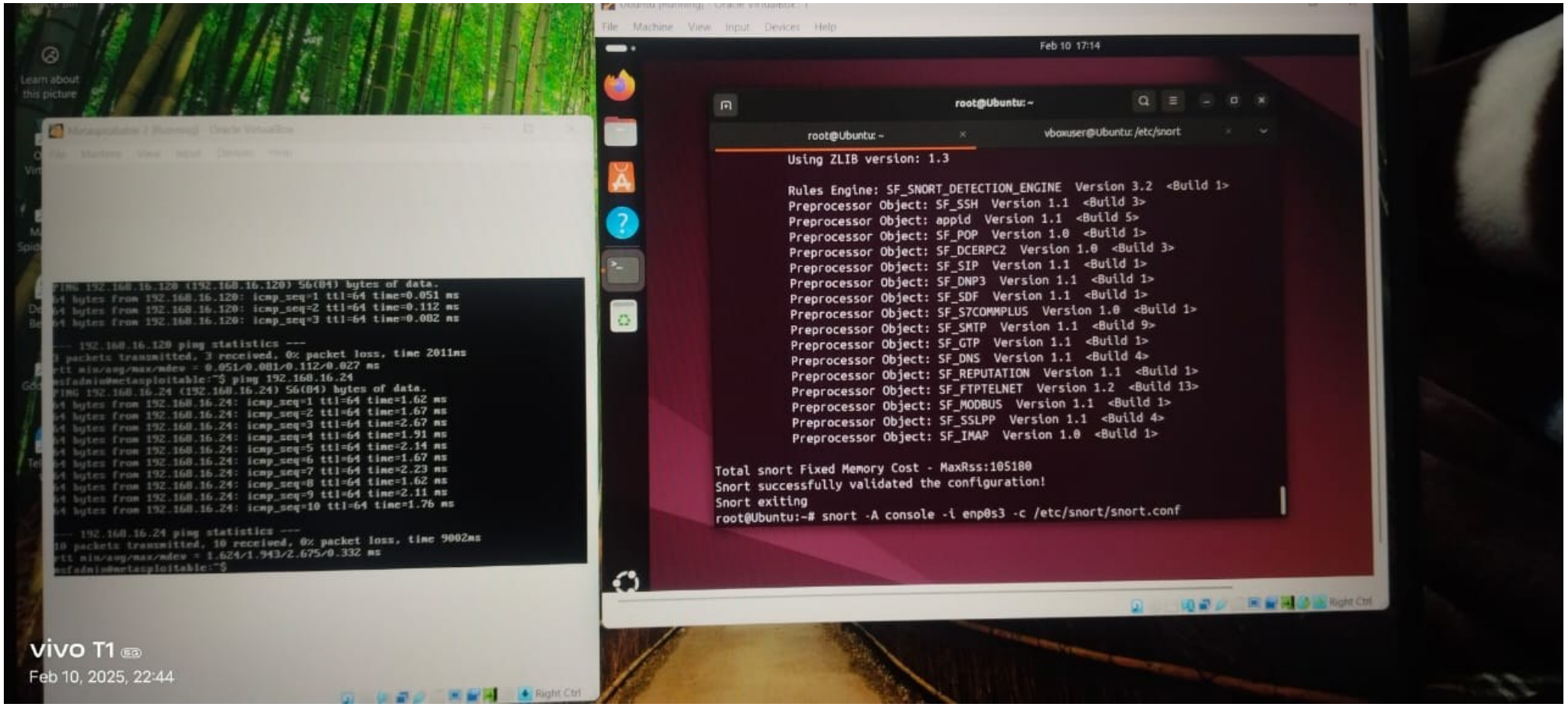


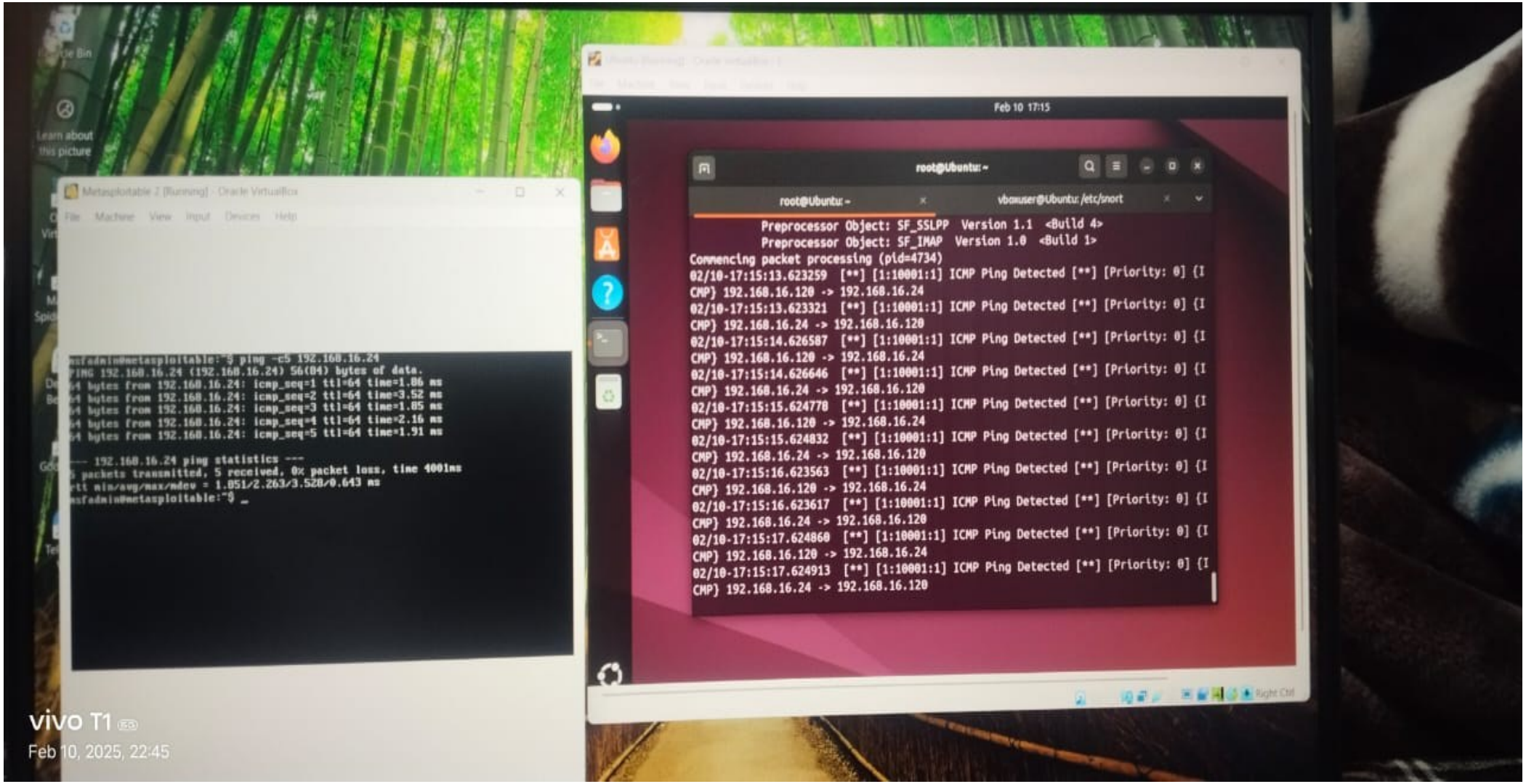
[Snorpy 2.0 - Web Based Snort Rule Creator]

- Using Sorpy to create alert rules -



Run Snort


Learn about this picture
PING 192.168.16.120 (192.168.16.120) 56(84) bytes of data.
64 bytes from 192.168.16.120: icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from 192.168.16.120: icmp_seq=2 ttl=64 time=0.112 ms
64 bytes from 192.168.16.120: icmp_seq=3 ttl=64 time=0.082 ms
--- 192.168.16.120 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 0.051/0.081/0.112/0.027 ms
msfadmin@metasploitable:~$ ping 192.168.16.24
PING 192.168.16.24 (192.168.16.24) 56(84) bytes of data.
64 bytes from 192.168.16.24: icmp_seq=1 ttl=64 time=1.62 ms
64 bytes from 192.168.16.24: icmp_seq=2 ttl=64 time=1.67 ms
64 bytes from 192.168.16.24: icmp_seq=3 ttl=64 time=2.67 ms
64 bytes from 192.168.16.24: icmp_seq=4 ttl=64 time=1.91 ms
64 bytes from 192.168.16.24: icmp_seq=5 ttl=64 time=2.14 ms
64 bytes from 192.168.16.24: icmp_seq=6 ttl=64 time=1.67 ms
64 bytes from 192.168.16.24: icmp_seq=7 ttl=64 time=2.23 ms
64 bytes from 192.168.16.24: icmp_seq=8 ttl=64 time=1.62 ms
64 bytes from 192.168.16.24: icmp_seq=9 ttl=64 time=2.11 ms
64 bytes from 192.168.16.24: icmp_seq=10 ttl=64 time=1.76 ms
--- 192.168.16.24 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9002ms
rtt min/avg/max/mdev = 1.624/1.943/2.675/0.332 ms
msfadmin@metasploitable:~$
vivo T1
Feb 10, 2025, 22:44
File Machine View Input Devices Help
Feb 10 17:14
root@Ubuntu: ~
root@Ubuntu: ~
vboxuser@Ubuntu: /etc/snort
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Total snort Fixed Memory Cost - MaxRss:105180
Snort successfully validated the configuration!
Snort exiting
root@Ubuntu:~# snort -A console -i enp0s3 -c /etc/snort/snort.conf
Right Ctrl


Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable:~$ ping -c5 192.168.16.24
PING 192.168.16.24 (192.168.16.24) 56(84) bytes of data.
64 bytes from 192.168.16.24: icmp_seq=1 ttl=64 time=1.86 ms
64 bytes from 192.168.16.24: icmp_seq=2 ttl=64 time=3.52 ms
64 bytes from 192.168.16.24: icmp_seq=3 ttl=64 time=1.85 ms
64 bytes from 192.168.16.24: icmp_seq=4 ttl=64 time=2.16 ms
64 bytes from 192.168.16.24: icmp_seq=5 ttl=64 time=1.91 ms
--- 192.168.16.24 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 1.851/2.263/3.528/0.643 ms
msfadmin@metasploitable:~$
Feb 10 17:15
root@Ubuntu: ~
root@Ubuntu: ~
vboxuser@Ubuntu: /etc/snort
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Commencing packet processing (pid=4734)
02/10-17:15:13.623259 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.120 -> 192.168.16.24
02/10-17:15:13.623321 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.24 -> 192.168.16.120
02/10-17:15:14.626587 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.120 -> 192.168.16.24
02/10-17:15:14.626646 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.24 -> 192.168.16.120
02/10-17:15:15.624770 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.120 -> 192.168.16.24
02/10-17:15:15.624832 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.24 -> 192.168.16.120
02/10-17:15:16.623563 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.120 -> 192.168.16.24
02/10-17:15:16.623617 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.24 -> 192.168.16.120
02/10-17:15:17.624860 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.120 -> 192.168.16.24
02/10-17:15:17.624913 [**] [1:10001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.16.24 -> 192.168.16.120
vivo T1
Feb 10, 2025, 22:45