|  |  |
| --- | --- |
| **Full Name** | Nasr edine ABDELLI |
| **Class** | 2MSIR |
| **Github Repo** | <https://github.com/AbdelliNasredine/INF_SEC_WORK> |

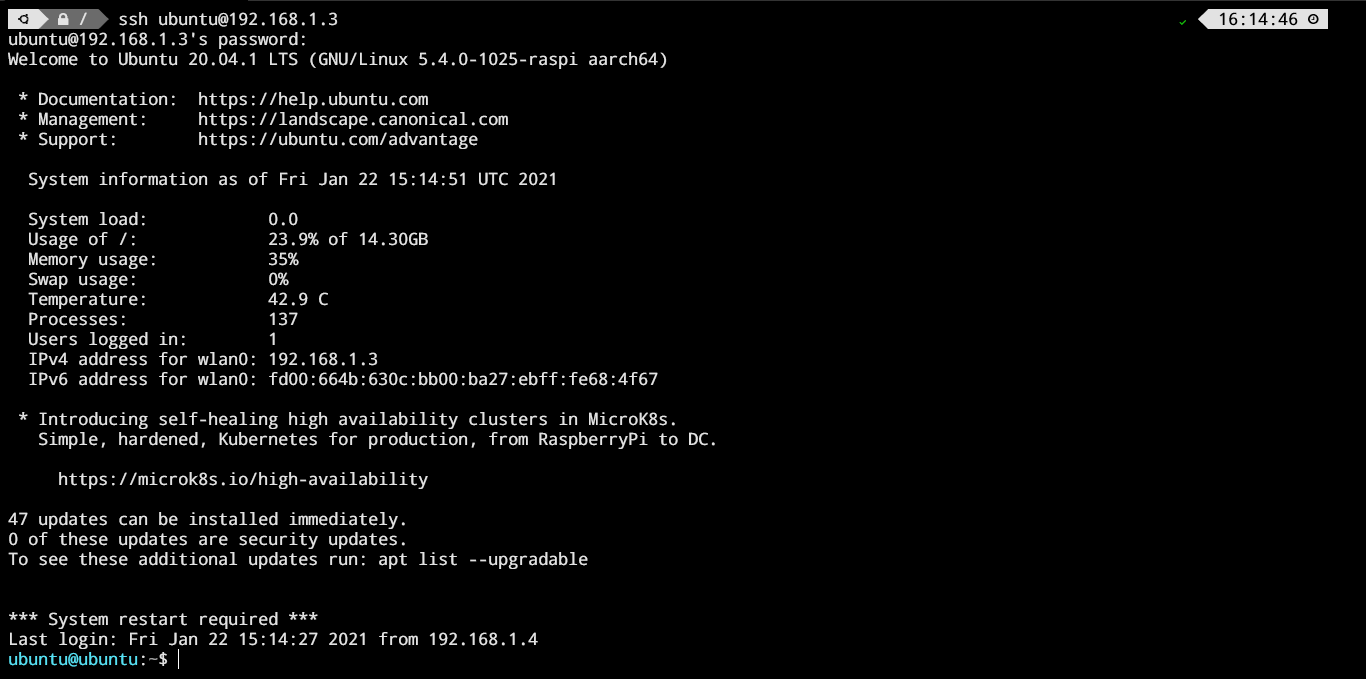
## Introduction

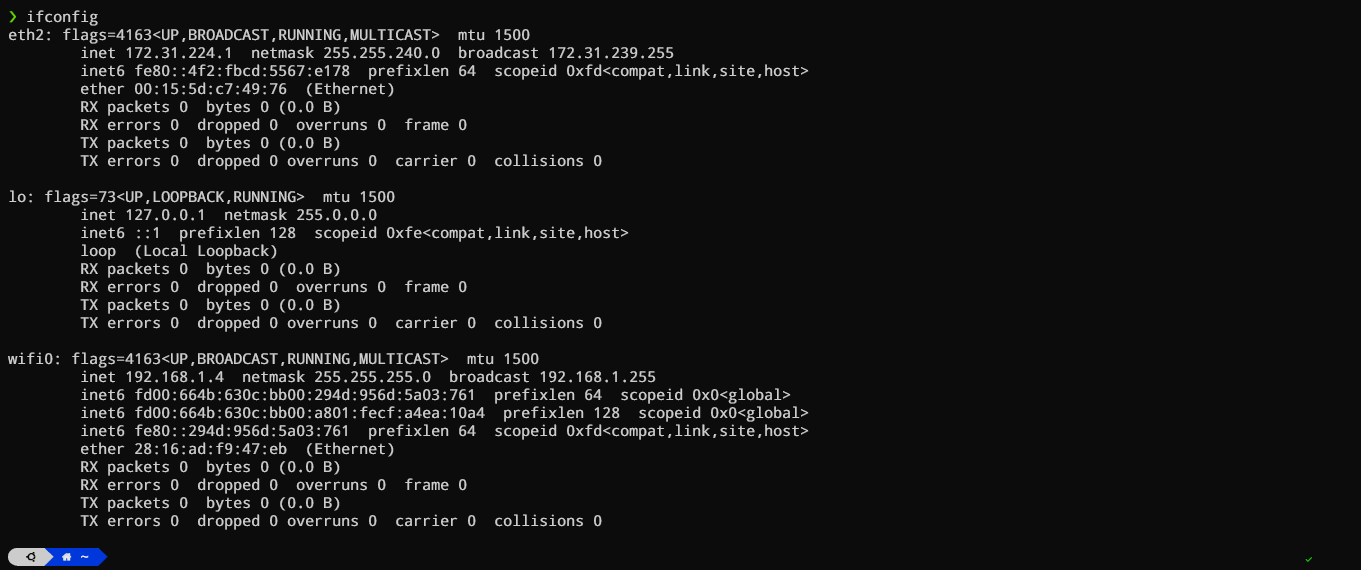
Intrusion Detection Systems play an important role in any computer system security where they monitor network traffic to search suspicious activities and threats through sending alerts when they find such behavior.

In the flowing document, I will show a use case scenario of using an SNORT as NIDS installed in a Linux box “Raspberry pi” and who it could detects threats.

## Machine Configuration:

|  |  |  |
| --- | --- | --- |
|  | **IP** | **OS** |
| **RPi box** | 192.168.1.3 | Ubuntu core 20.04 |
| **Attacker Machine** | 192.168.1.4 | WSL (Ubuntu 18.04) |

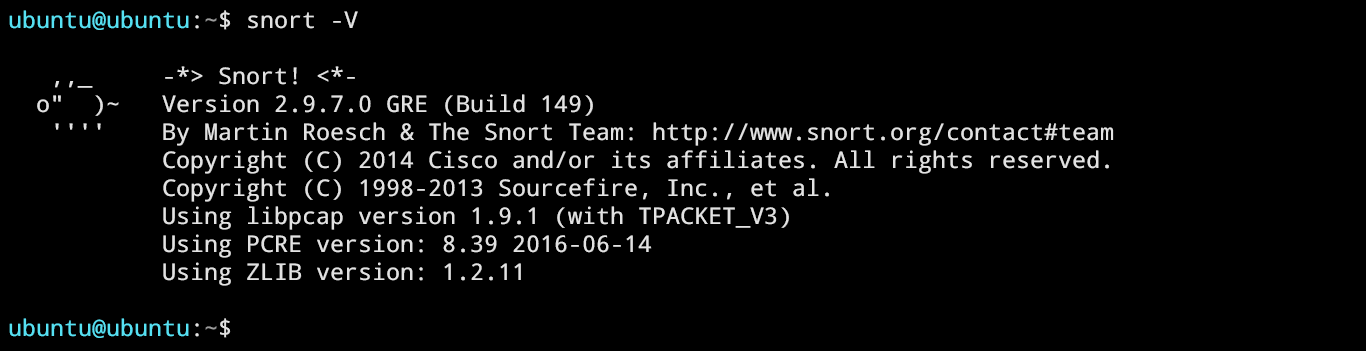




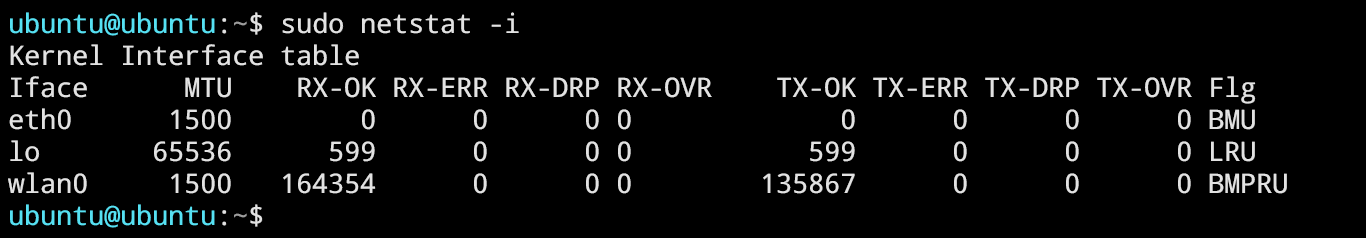
## Installation & Configuration of Snort

**Note: I used SSH to access the RPi machine**

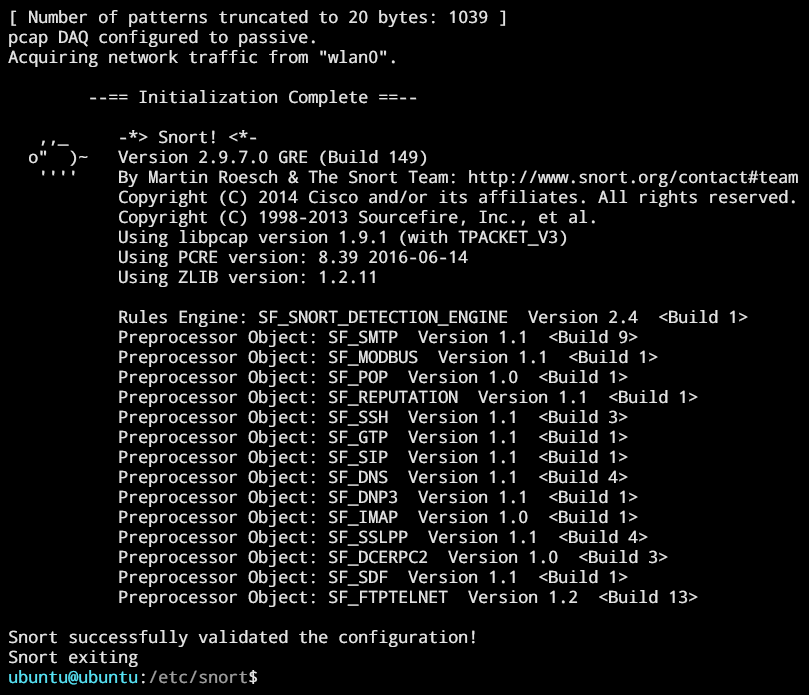
The installation of Snort is done using ***apt install snort -y*** *:*



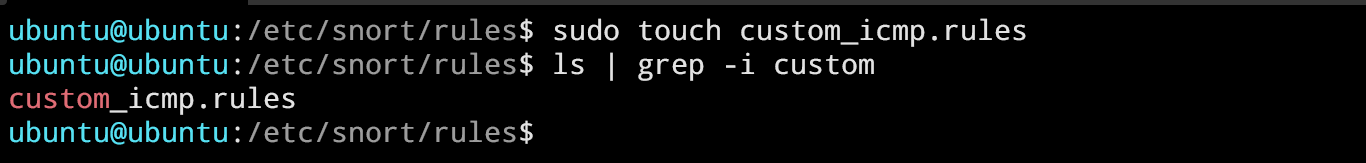
The network interface is ***wlan0*** andit’s on **promiscuous mode**:

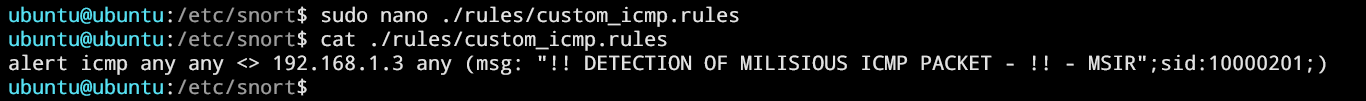


After running ***sudo snort –T –i wlan0 –c /etc/snort/snort.conf*** , snort is successfully validated using the included config file.

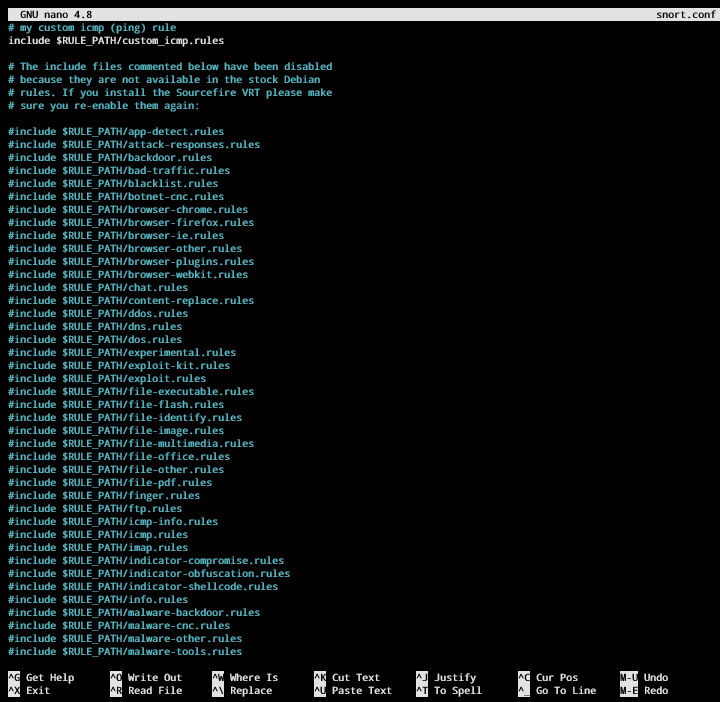


## Adding a custom Rule:



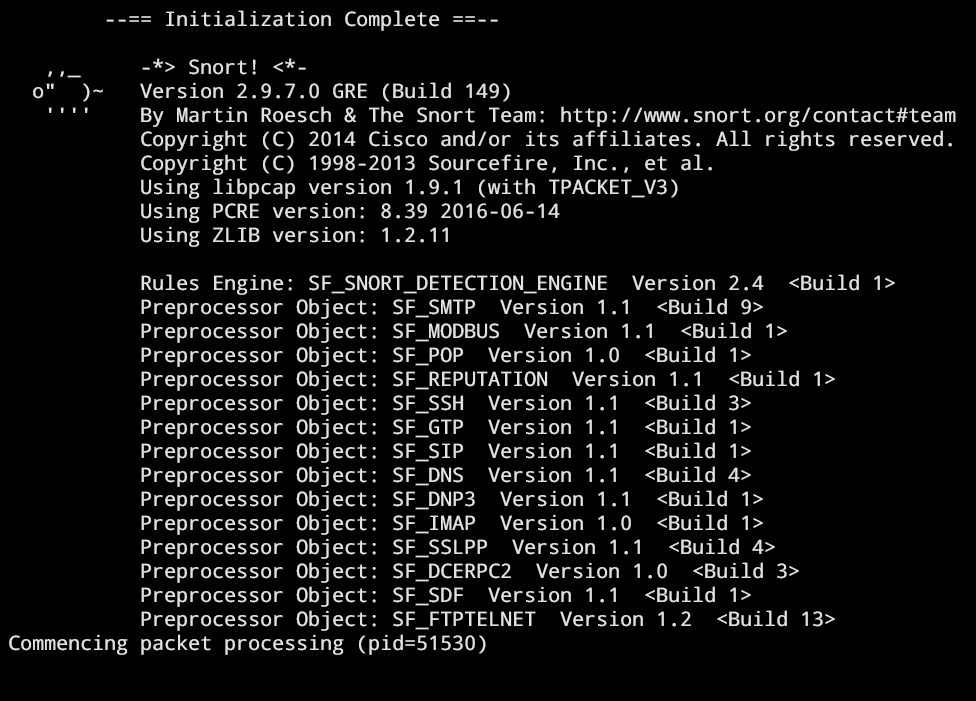


Before adding the custom rule to configuration, I commented out all the used rules in ***snort.conf*** file and add the rule using ***include $RULE\_PATH custom\_icmp.rules***

****

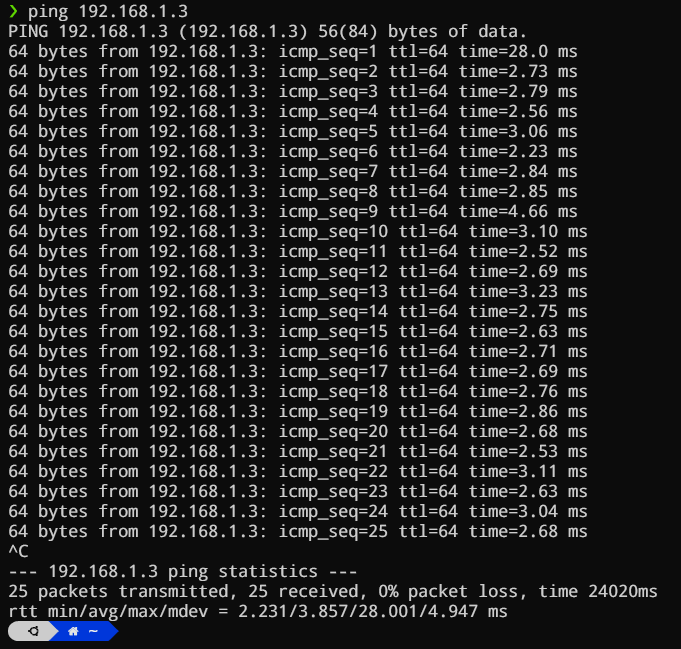
**NEW RULE**

**Running snort with the new configuration file:**

****

## Attack Phase:

The attack is a simple ***ping*** request:

****

Snort is successfully detection the ping packets from attacker machine (192.168.1.4)

