MIDTERM REPORT

**Subjects: Quản trị mạng và hệ thống**

**Topic : Snort**

*GVHD: Trần Thị Dung*

**1.GENERAL INFORMATION:**

Class : NT132.N12.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trương Văn Rồng | 20521831 | 20521831@gm.uit.edu.vn |
| 2 | Lương Mạnh Tiến | 20522008 | 20522008@gm.uit.edu.vn |
| 3 | Phan Hoàng Nam | 20521635 | 20521635@gm.uit.edu.vn |

**2.CONTENTS:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | I.Introduction | **100%** |
| 2 | 1.1 Overview | **100%** |
| 3 | 1.2 Component | **100%** |
| 4 | 1.3 Operation | **100%** |
| 5 | II. Implementation | **100%** |
| 6 | 2.1 Topology | **100%** |
| 7 | 2.2 Installation | **100%** |
| 8 | 2.3 Configuration | **100%** |
| 9 | 1. Result | **100%** |

REPORT IN DETAIL

1. **Introduction**

**1.1 Overview**

Snort is a free open source Network Intrusion Detection System(NIDS) and Intrusion Prevention System (IPS) which is capable of performing real-time traffic analysis and packet logging on IP networks. It helps define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

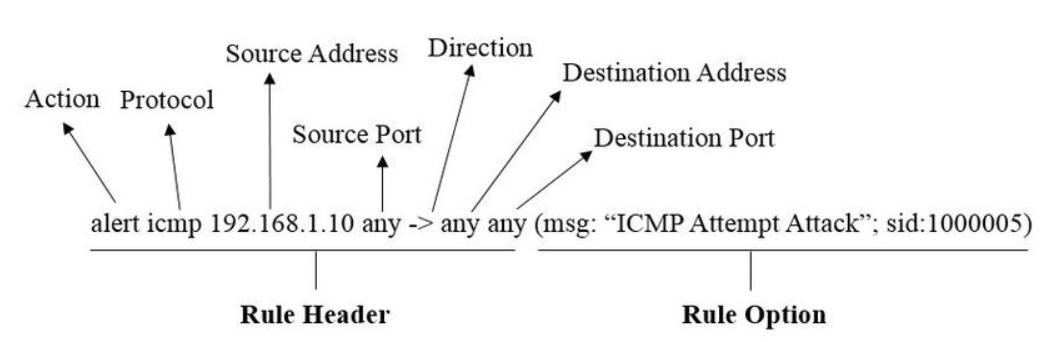
**1.2 Component**

Snort is comprised of two major components: a detection engine that utilizes modular plug-in architecture (the “Snort Engine”) and a flexible rule language to describe traffic to be collected (the “Snort Rules”)

**1.3 Operation**

Snort IPS uses rules that aids in the definition of malicious network activity and employs those rules to find packets that match against them, generating alerts for users

Each rule has a structure like this:



**In basic model**: Detect some network attack (using default rules)

* On the server side Ubuntu: I'm running Snort using default rules.
* On the attacker side Kali: I try to use the pingcommand or **nmap** tool to the IP of Ubuntu.
* According to the default rules, Snort will notify the user if it detects malicious network activity.

**In advanced model**: Separate Server and detect the attack to server

* On the attacker side Kali: I host a local website DVWA for example
* On the host machine: I'm launching a browser that connects to the internet as an external component and trying to connect to the DVWA website which is located on Kali machine.
* On the middle side - Ubuntu machine: I'm running Snort with the default rules and some custom rules I wrote.
* According to the rules, Snort will warn the user if it detects harmful network activity.

**II. Implementation**

**2.1 Topology**

**In basic model**:

Snort

server

Kali

Linux

Ubuntu

ping/nmap

* I configured the NAT network in VMware's Network Adapter in both Kali and Ubuntu machines.

**In advanced model:**

DVWA

Web

Snort

server

Web

Server

Host only

Bridge

Kali Linux

Ubuntu

Internet

* I configured the Bridge network in VMware's Network Adapter between the internet and Ubuntu machine
* In VMware's Network Adapter, I set up a Host-only network between the Ubuntu system and Kali Linux.

**2.2 Installation**

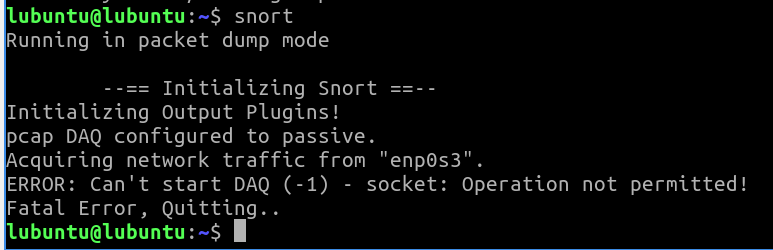
**Step 1**: Update the apt packet and find the appropriate package for the operating system and install.

sudo apt update

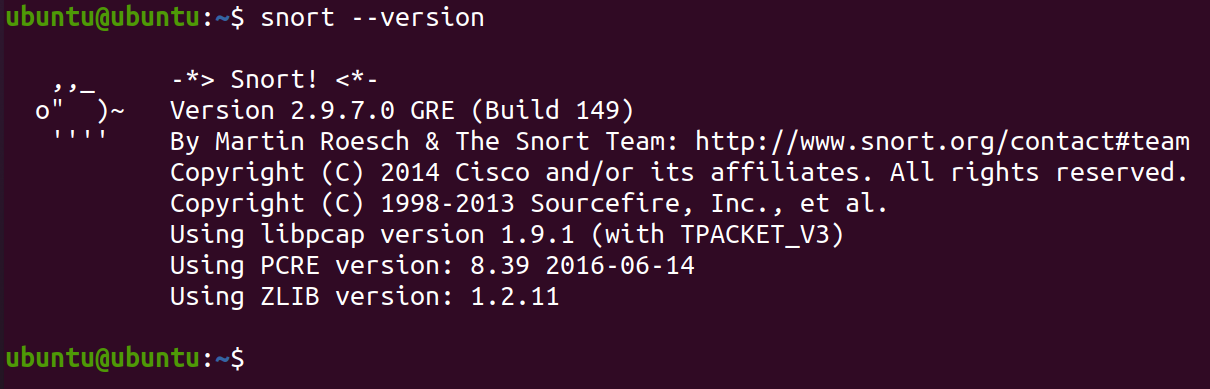
sudo apt install snort -y

Graphical user interface, text, application, email

Description automatically generated

Select the address range for the local network and click Ok.  


After successful installation. Check Snort version

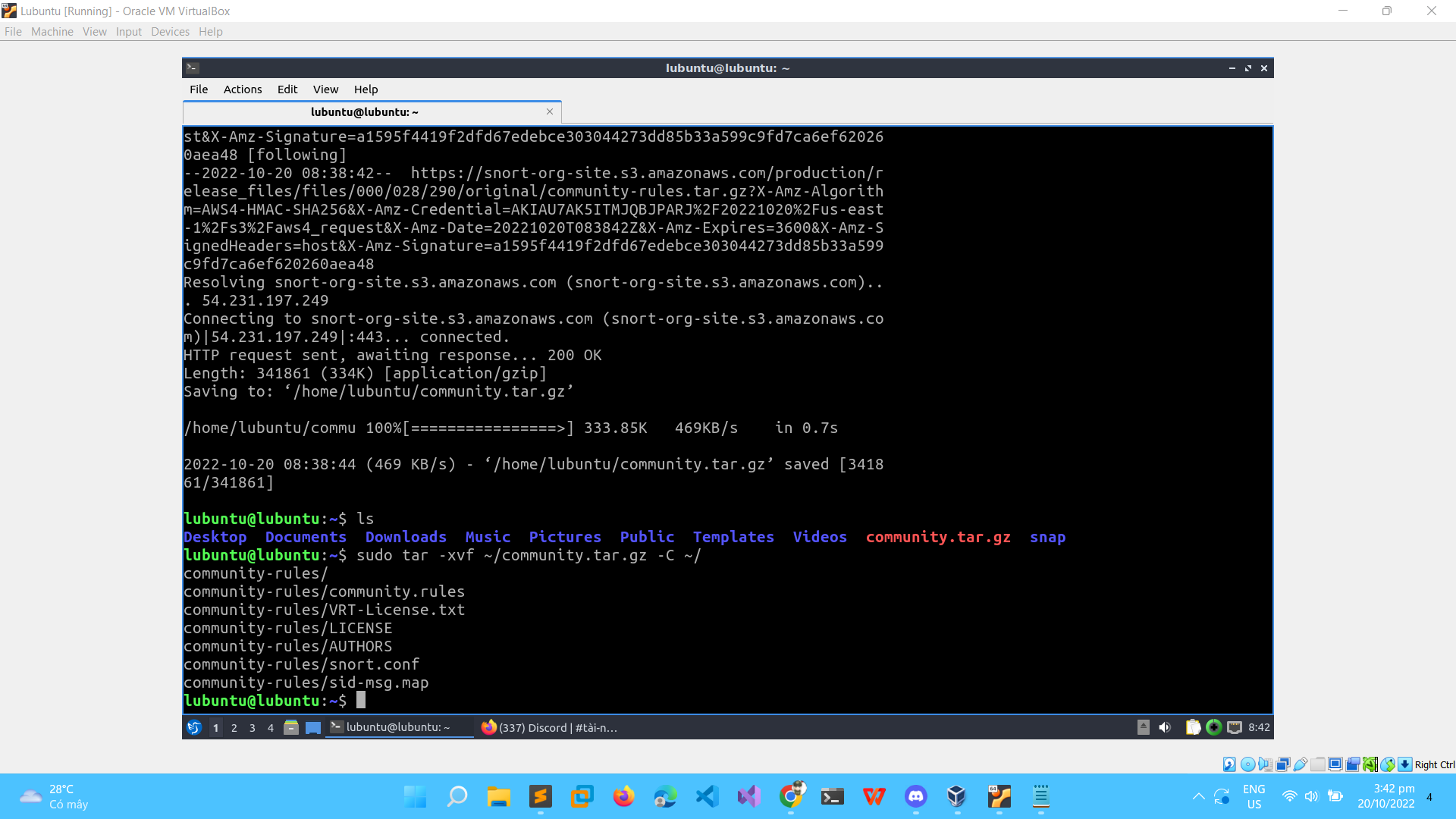


* **Next step**, Download and add snort rules
* To make the snort tool work, we add the rules of snort
* Can be downloaded directly on the snort site (supported by the community) using wget and saved and the communitu.tar.gz file

wget https://www.snort.org/rules/community -O ~/community.tar.gz

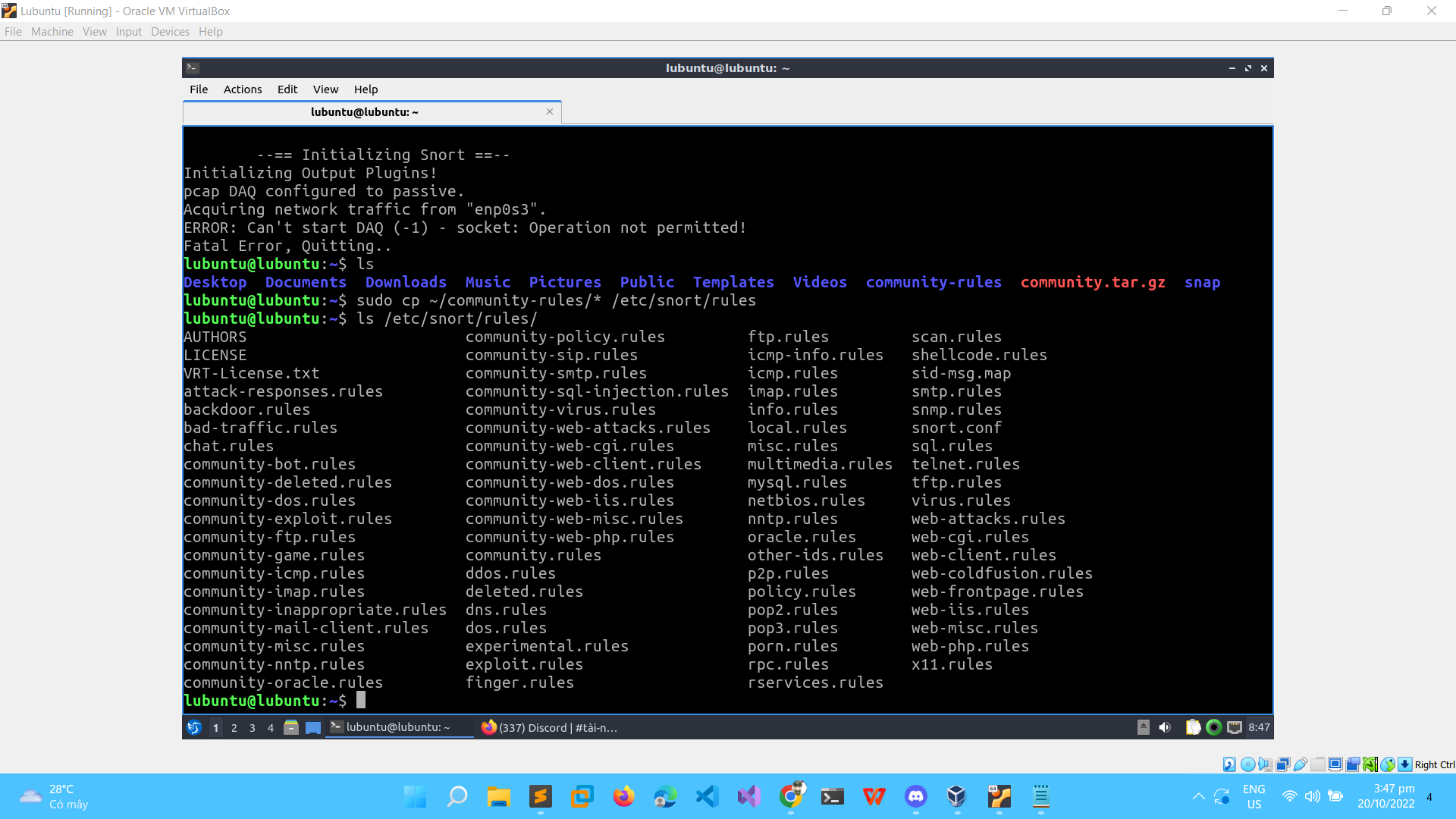
sudo tar -xvf ~/community.tar.gz -C ~/

Extract the file with the tar . command



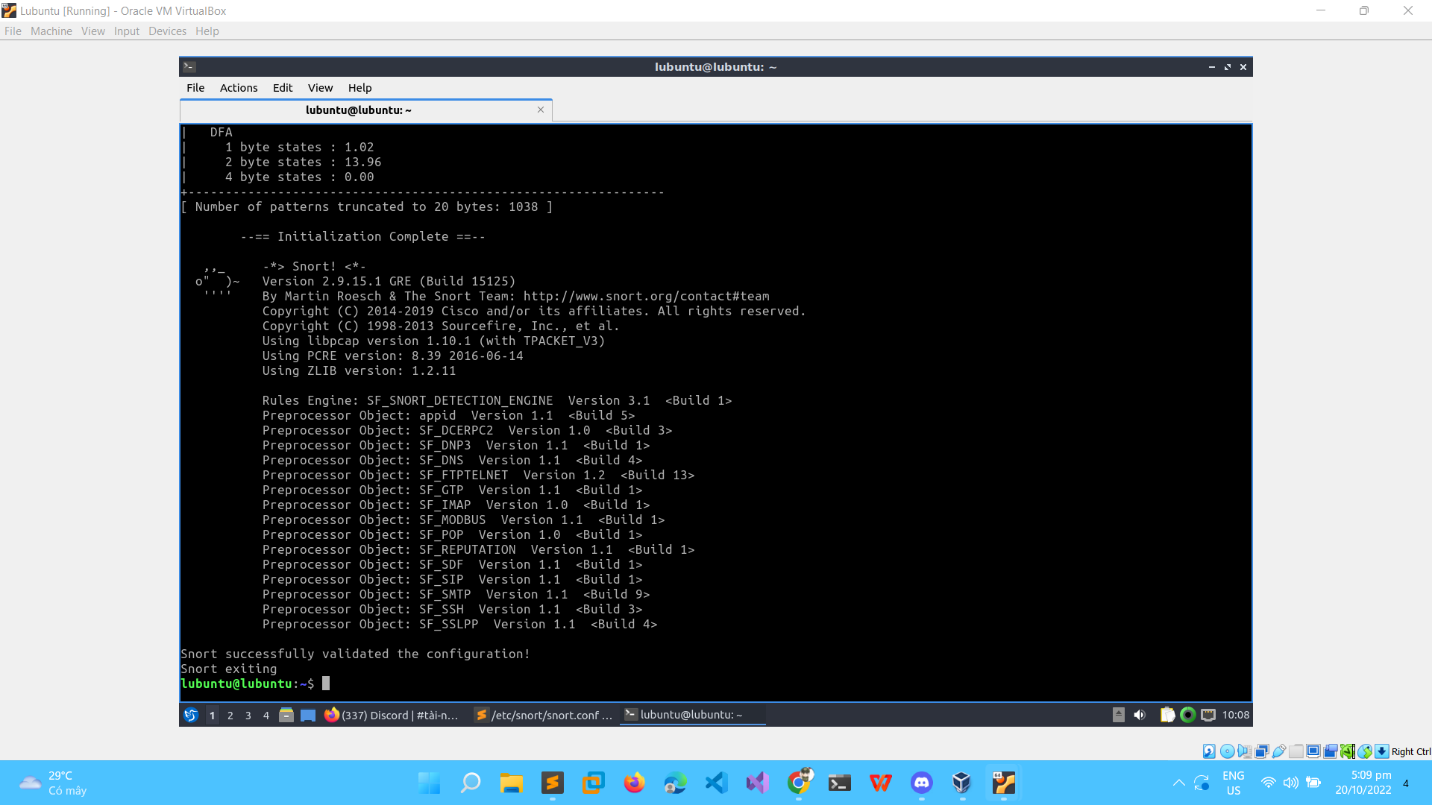
As a result, we can have the community-rules . directory:

sudo cp ~/community-rules/\* /etc/snort/rules



Test Snort:

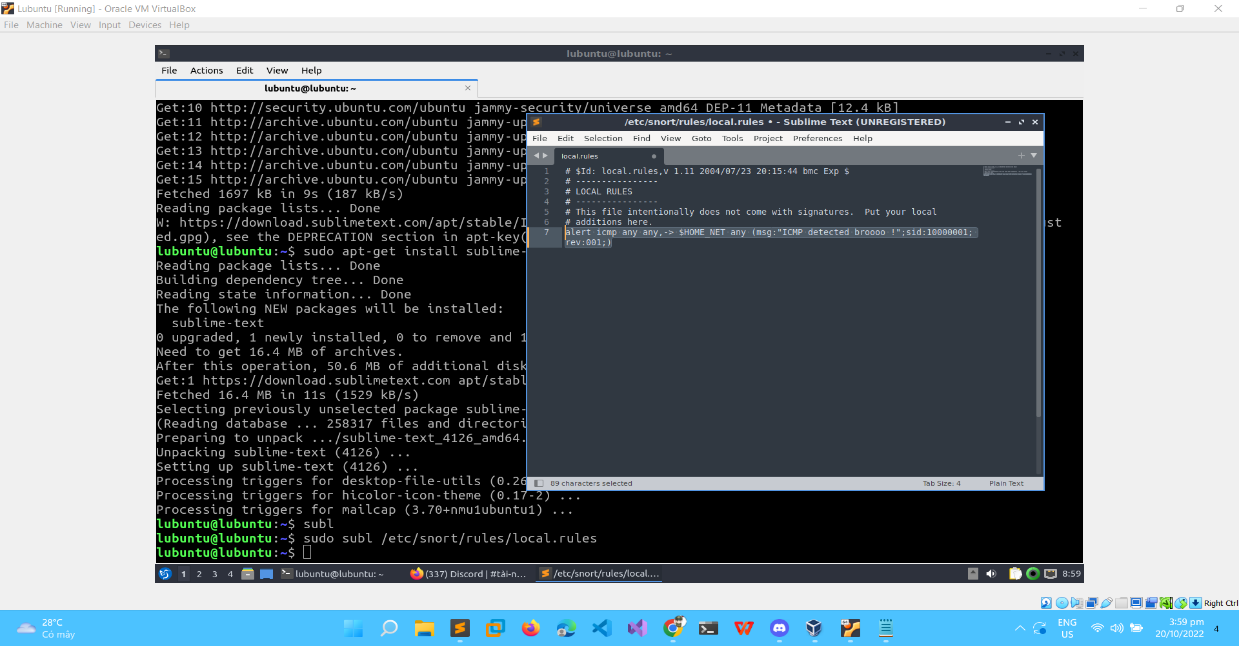
sudo snort -T -c /etc/snort/snort.conf



**2.3 Configuration**

Add this rule to file locals.local

alert icmp any any -> $HOME\_NET any (msg:"ICMP detected!";sid:10000001; rev:001;)



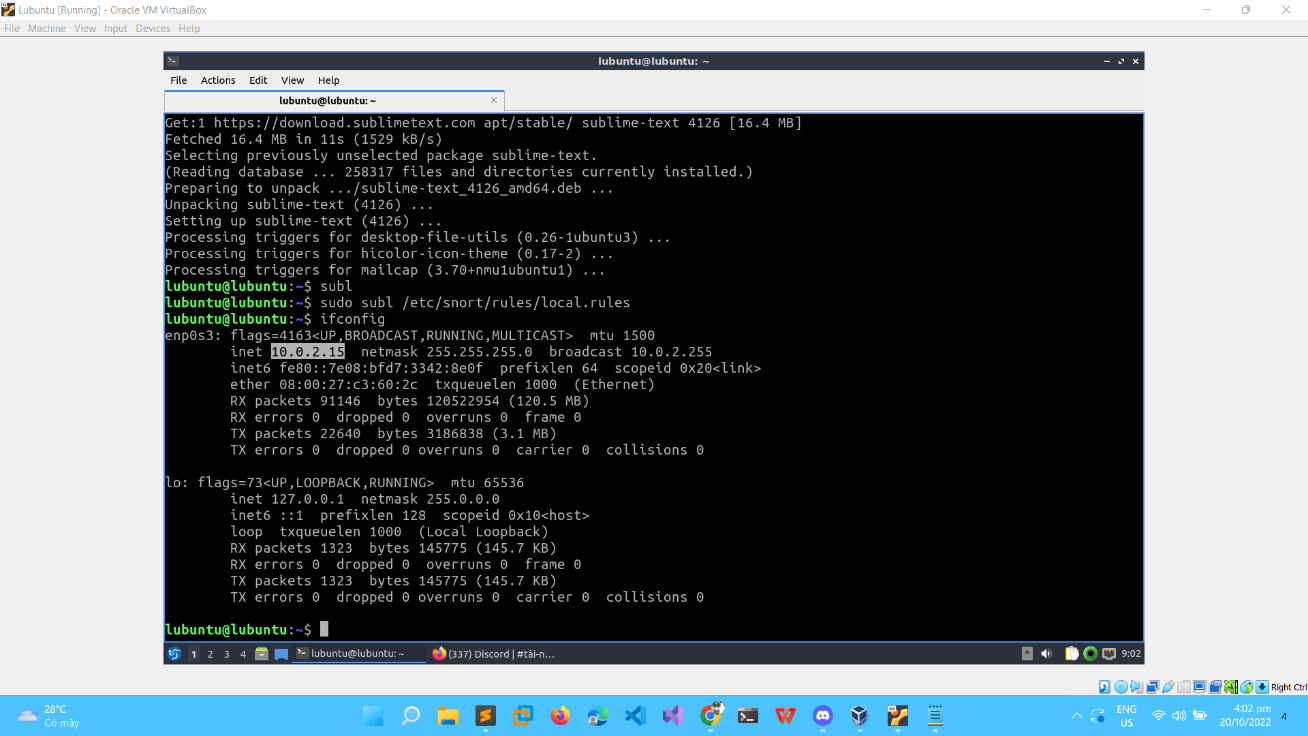
Now use a VM kali ping to VM Ubuntu. Make sure that Use NAT network both machine. Graphical user interface, application

Description automatically generatedGraphical user interface, application

Description automatically generated

Use ifconfig to know the IP:

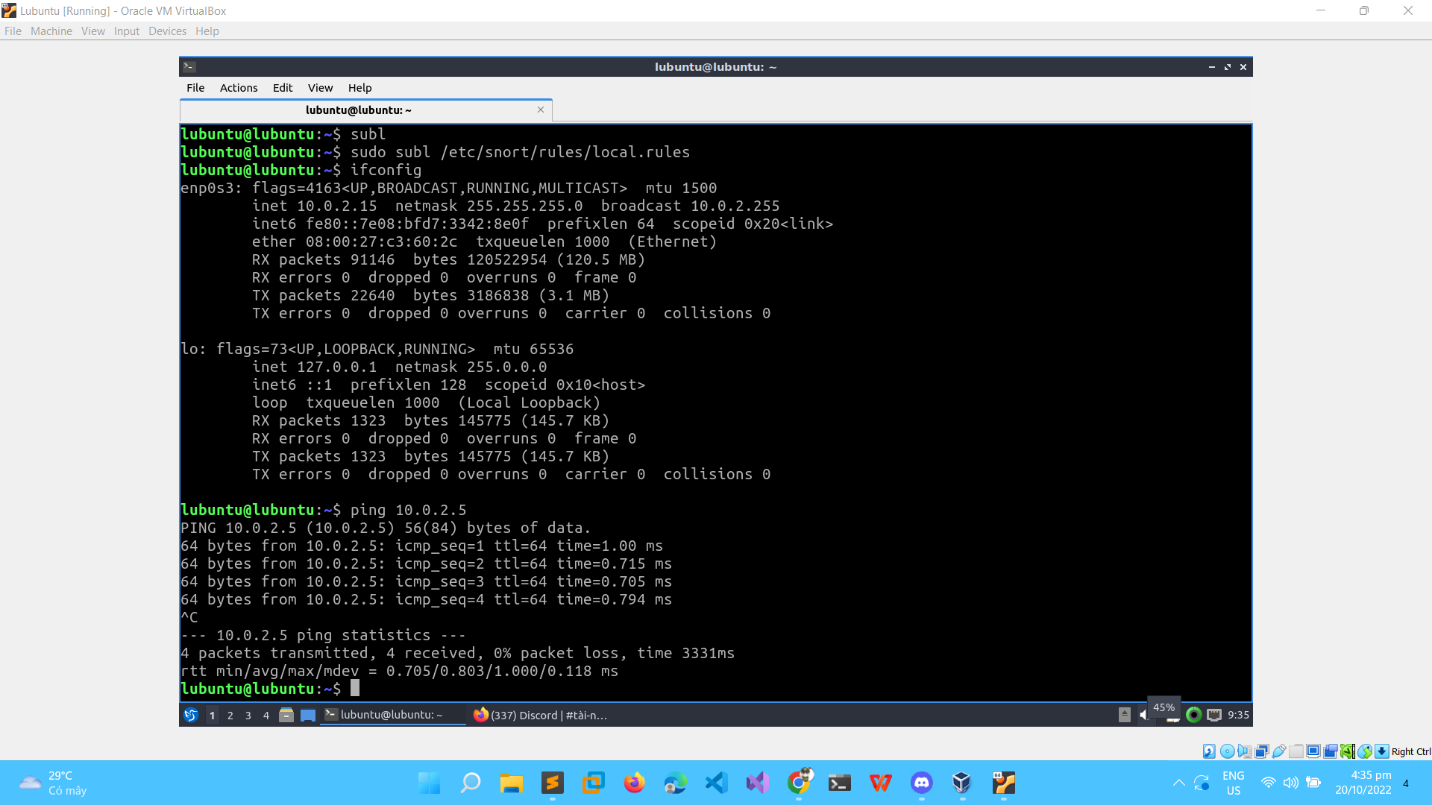
Lubuntu machine → 10.0.2.15



Kali → 10.0.2.5  
A screenshot of a computer

Description automatically generated

After setting up NAT, we try to ping and see success



**3.Result**

Kali VM:

A screen shot of a computer

Description automatically generated with medium confidence

Lubuntu VM:

A computer screen capture

Description automatically generated with medium confidence

Thus, we have successfully detected the attack using the ping command

---

**END**