Trường Đại học Công nghệ Thông tin (UIT)

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	3. Result	**100%**

Table Of Contents

REPORT IN DETAIL

I. 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.

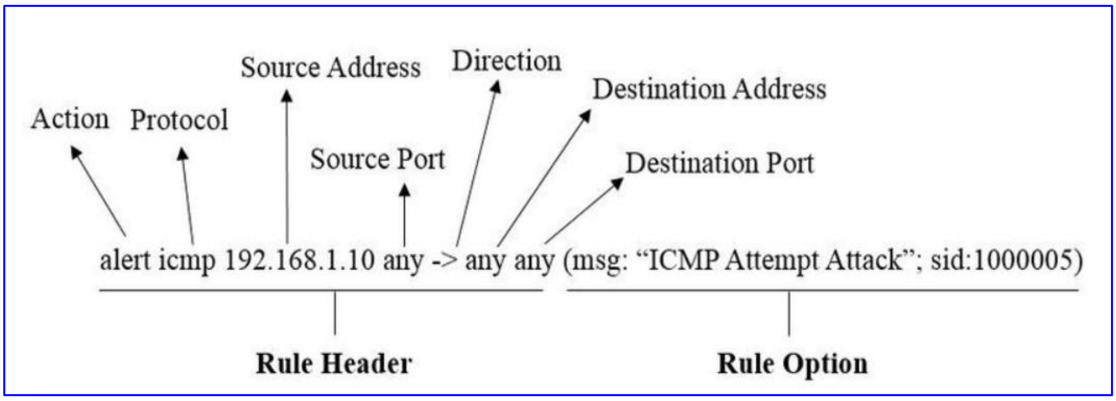
1.2 Component

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 ping command or **nmap** tool to the IP of Ubuntu.
- According to the default rules, Snort will notify the user if it detects malicious network activity.

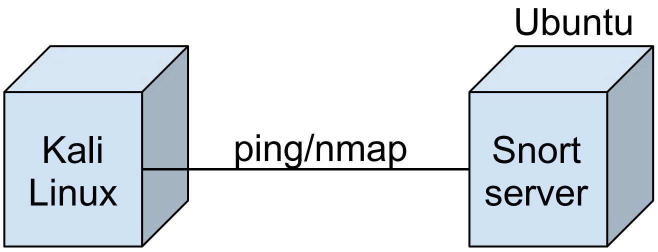
In advanced model: Separate Server and detect the attack to server

- 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

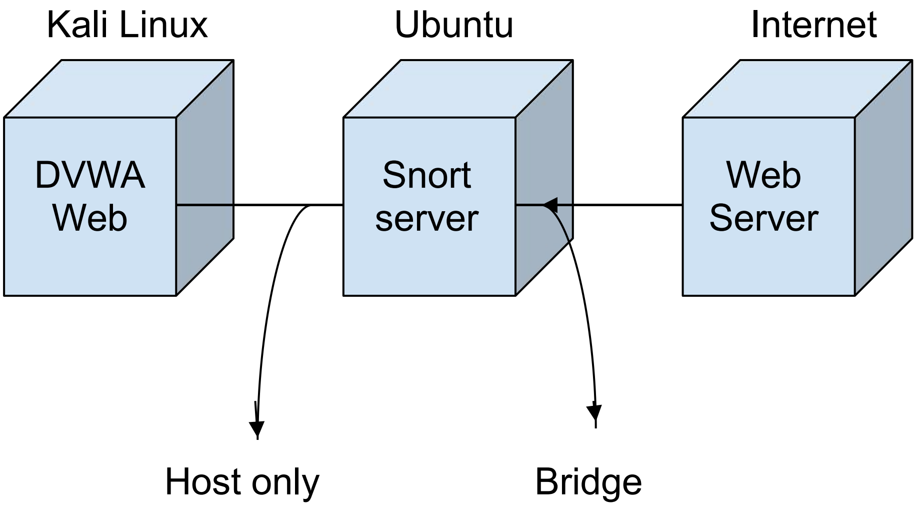
2.1 Topology

In basic model:



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

In advanced model:



- 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.

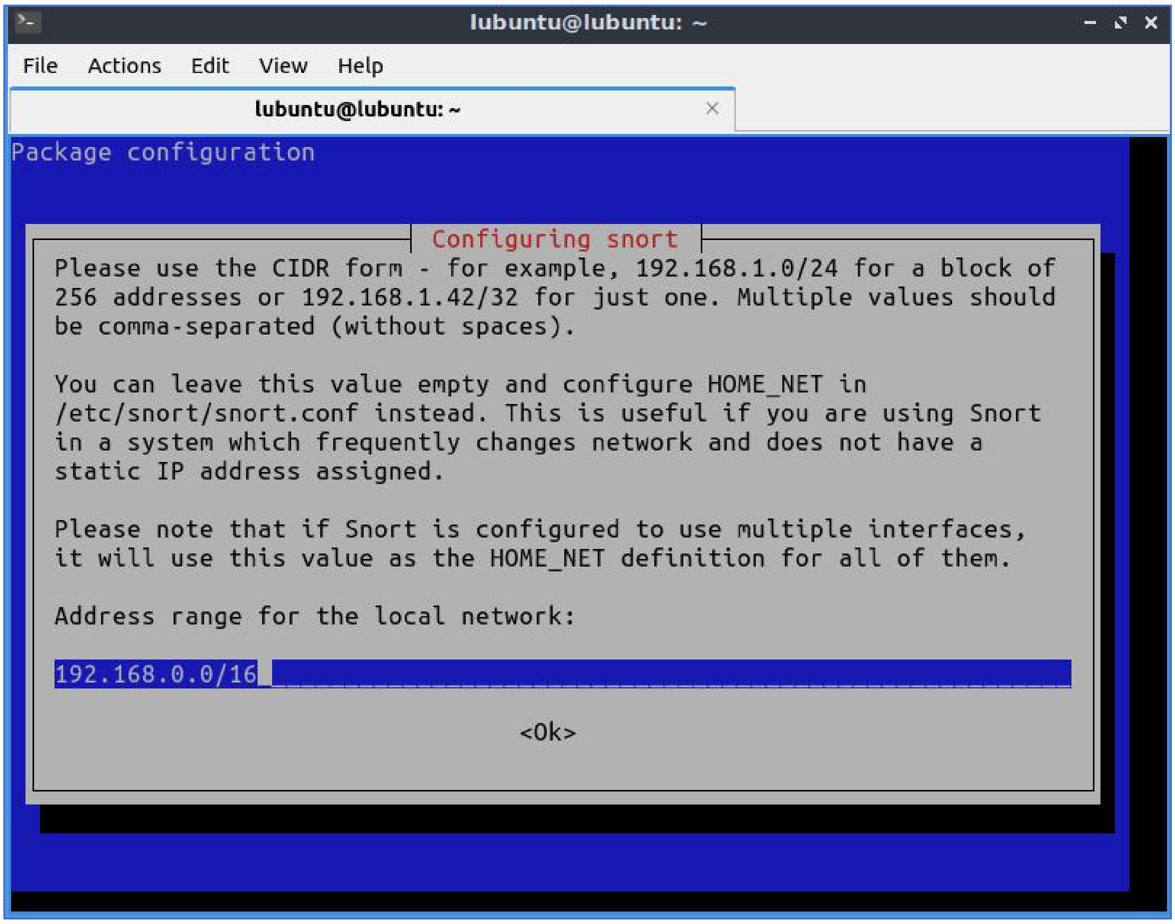
2.2 Installation

- **Server:** Lubuntu (install snort)
- **Attacker:** Kali (use malicious network attacks)

❖ In Lubuntu server

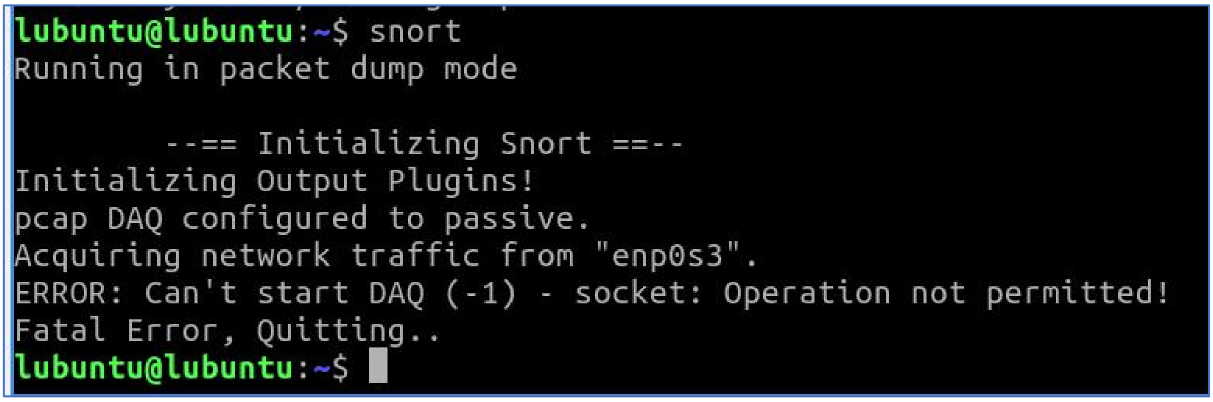
Step 1: Update the apt packet and find the appropriate package for the operating system and install.

```
sudo apt update
sudo apt install snort -y
```



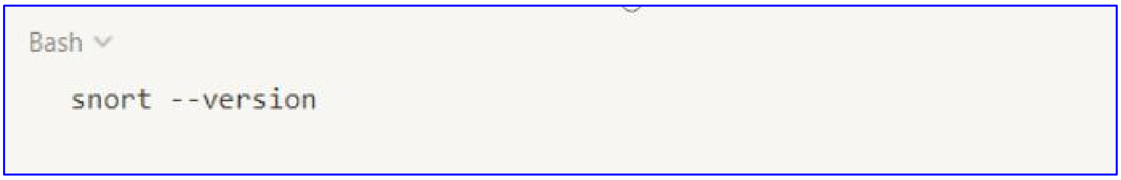
```
Package configuration

                     Configuring snort
 Please use the CIDR form - for example, 192.168.1.0/24 for a block of
 256 addresses or 192.168.1.42/32 for just one. Multiple values should
 be comma-separated (without spaces).

 You can leave this value empty and configure HOME_NET in
 /etc/snort/snort.conf instead. This is useful if you are using Snort
 in a system which frequently changes network and does not have a
 static IP address assigned.

 Please note that if Snort is configured to use multiple interfaces,
 it will use this value as the HOME_NET definition for all of them.

 Address range for the local network:

 192.168.0.0/16

                              <Ok>
```

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

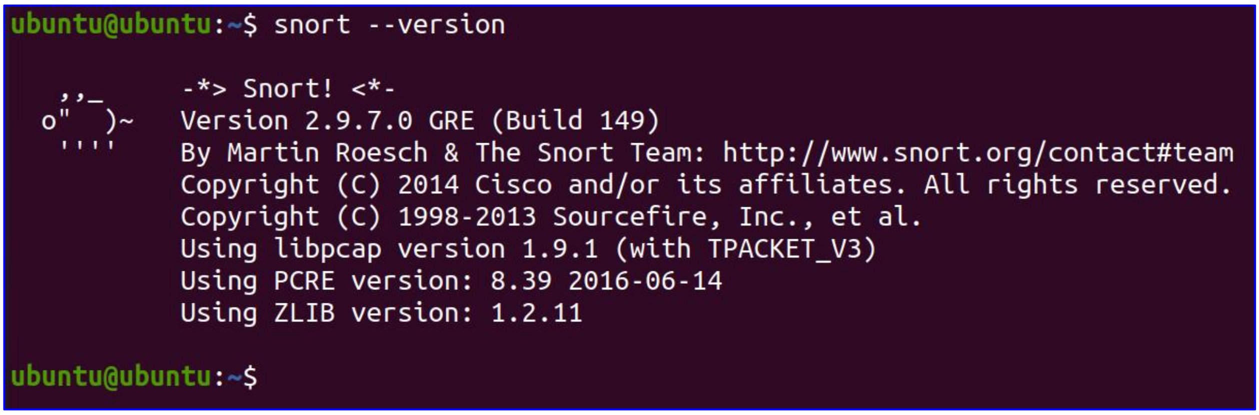


```
lubuntu@lubuntu:~$ snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
ERROR: Can't start DAQ (-1) - socket: Operation not permitted!
Fatal Error, Quitting..
lubuntu@lubuntu:~$
```

After successful installation. Check Snort version



```
Bash
  snort --version
```

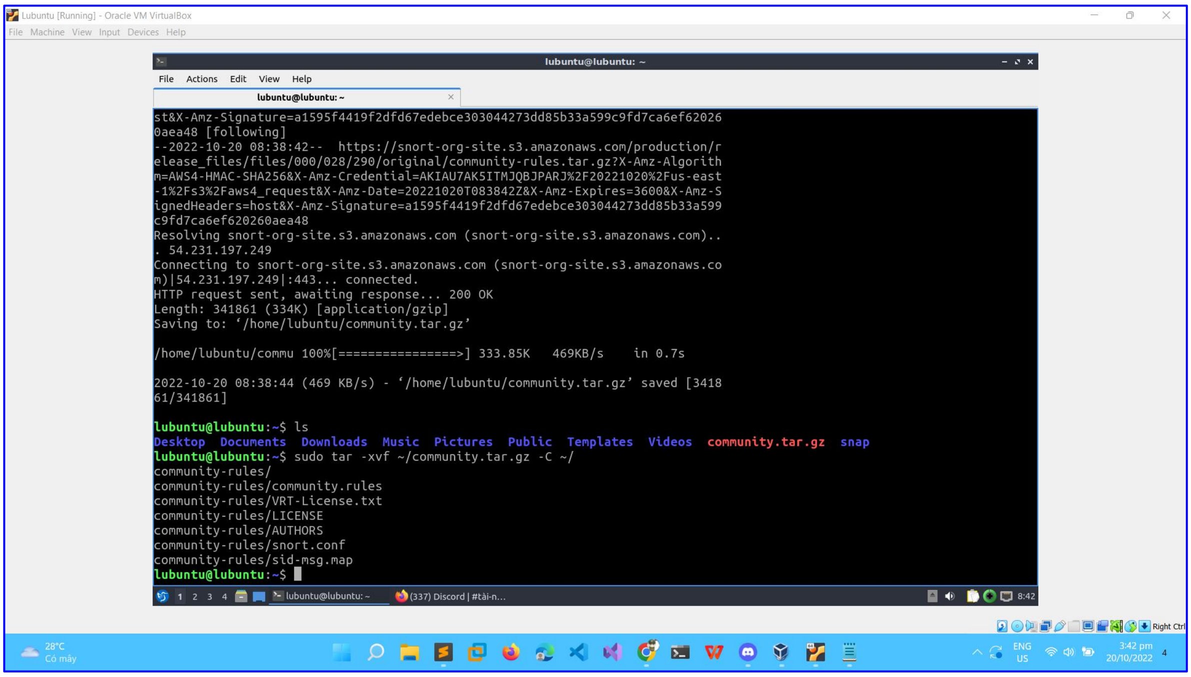


```
ubuntu@ubuntu:~$ snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

ubuntu@ubuntu:~$
```

- **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
```

Extract the file with the tar . command

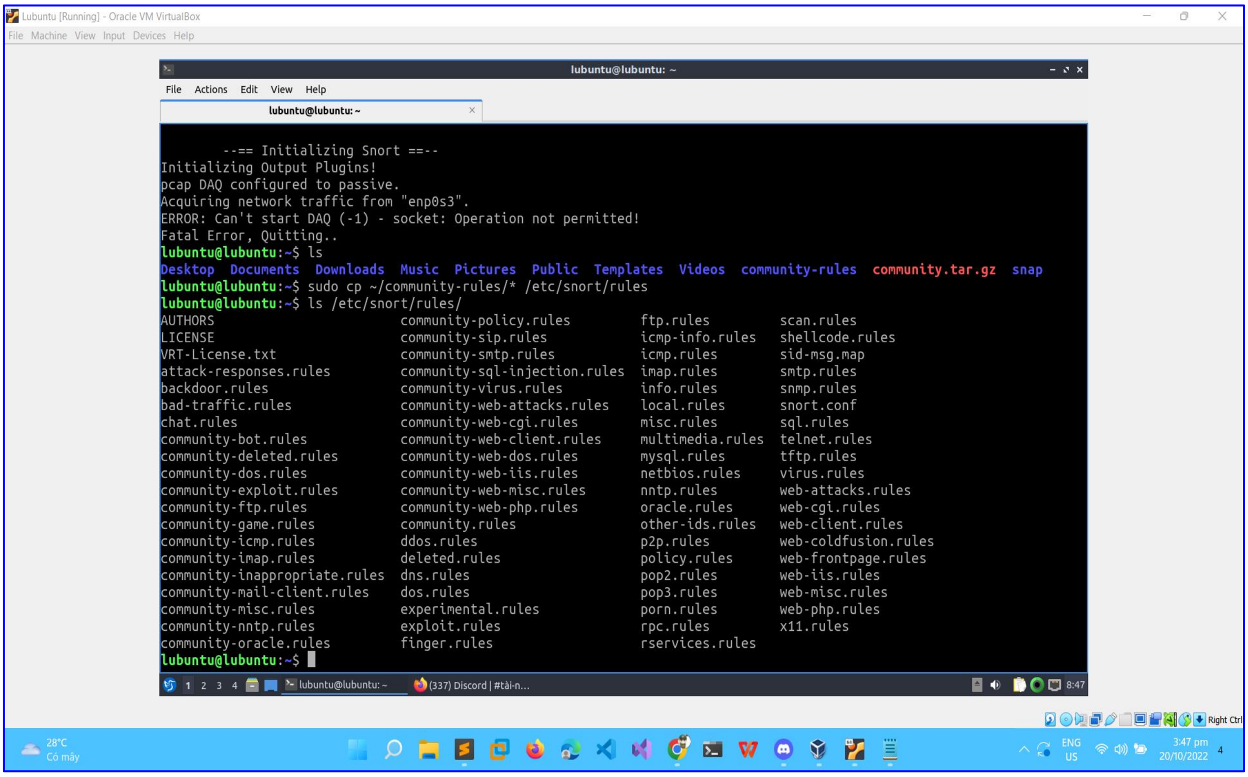


```
st&X-Amz-Signature=a1595f4419f2dfd67edebce303044273dd85b33a599c9fd7ca6ef62026
0aea48 [following]
--2022-10-20 08:38:42--  https://snort-org-site.s3.amazonaws.com/production/r
elease_files/files/000/028/290/original/community-rules.tar.gz?X-Amz-Algorith
m=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMJQBJPARJ%2F20221020%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20221020T083842Z&X-Amz-Expires=3600&X-Amz-S
ignedHeaders=host&X-Amz-Signature=a1595f4419f2dfd67edebce303044273dd85b33a599
c9fd7ca6ef620260aea48
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)..
. 54.231.197.249
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.co
m)|54.231.197.249|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 341861 (334K) [application/gzip]
Saving to: ‘/home/lubuntu/community.tar.gz’

/home/lubuntu/commu 100%[===============>] 333.85K   469KB/s    in 0.7s

2022-10-20 08:38:44 (469 KB/s) - ‘/home/lubuntu/community.tar.gz’ saved [3418
61/341861]

lubuntu@lubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  community.tar.gz  snap
lubuntu@lubuntu:~$ sudo tar -xvf ~/community.tar.gz -C ~/
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
lubuntu@lubuntu:~$
```

Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
1 2 3 4
lubuntu@lubuntu: ~
(337) Discord | #tài-n...
8:42
Right Ctrl
28°C
Có mây
ENG
US
3:42 pm
20/10/2022

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

```
Bash
sudo cp ~/community-rules/* /etc/snort/rules
```

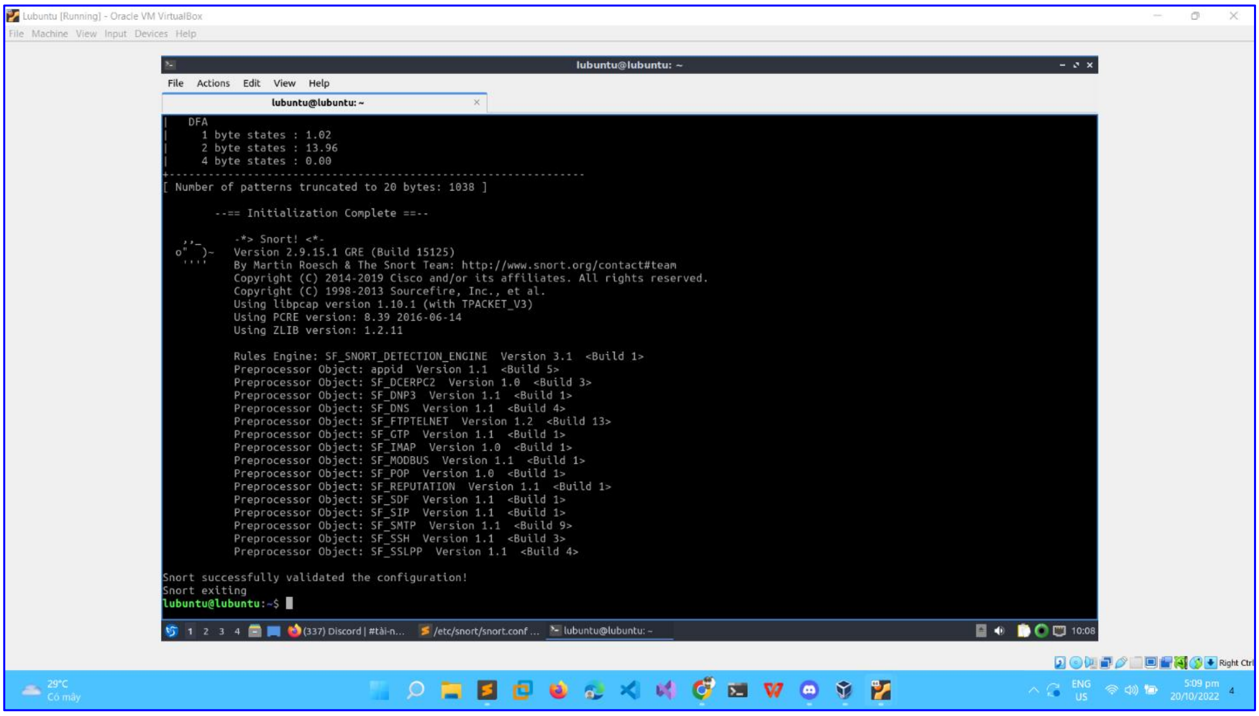


Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
lubuntu@lubuntu: ~
(337) Discord | #tài-n...
8:47
Right Ctrl
28°C
Có mây
ENG
US
3:47 pm
20/10/2022

```
        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
ERROR: Can't start DAQ (-1) - socket: Operation not permitted!
Fatal Error, Quitting..
lubuntu@lubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  community-rules  community.tar.gz  snap
lubuntu@lubuntu:~$ sudo cp ~/community-rules/* /etc/snort/rules
lubuntu@lubuntu:~$ ls /etc/snort/rules/
AUTHORS                         community-policy.rules         ftp.rules          scan.rules
LICENSE                         community-sip.rules            icmp-info.rules    shellcode.rules
VRT-License.txt                 community-smtp.rules           icmp.rules         sid-msg.map
attack-responses.rules          community-sql-injection.rules  imap.rules         smtp.rules
backdoor.rules                  community-virus.rules          info.rules         snmp.rules
bad-traffic.rules               community-web-attacks.rules    local.rules        snort.conf
chat.rules                      community-web-cgi.rules        misc.rules         sql.rules
community-bot.rules             community-web-client.rules     multimedia.rules   telnet.rules
community-deleted.rules         community-web-dos.rules        mysql.rules        tftp.rules
community-dos.rules             community-web-iis.rules        netbios.rules      virus.rules
community-exploit.rules         community-web-misc.rules       nntp.rules         web-attacks.rules
community-ftp.rules             community-web-php.rules        oracle.rules       web-cgi.rules
community-game.rules            community.rules                other-ids.rules    web-client.rules
community-icmp.rules            ddos.rules                     p2p.rules          web-coldfusion.rules
community-imap.rules            deleted.rules                  policy.rules       web-frontpage.rules
community-inappropriate.rules   dns.rules                      pop2.rules         web-iis.rules
community-mail-client.rules     dos.rules                      pop3.rules         web-misc.rules
community-misc.rules            experimental.rules             porn.rules         web-php.rules
community-nntp.rules            exploit.rules                  rpc.rules          x11.rules
community-oracle.rules          finger.rules                   rservices.rules
lubuntu@lubuntu:~$ 
```

Test Snort:

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



```
|   DFA
|     1 byte states : 1.02
|     2 byte states : 13.96
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
lubuntu@lubuntu:~$
```

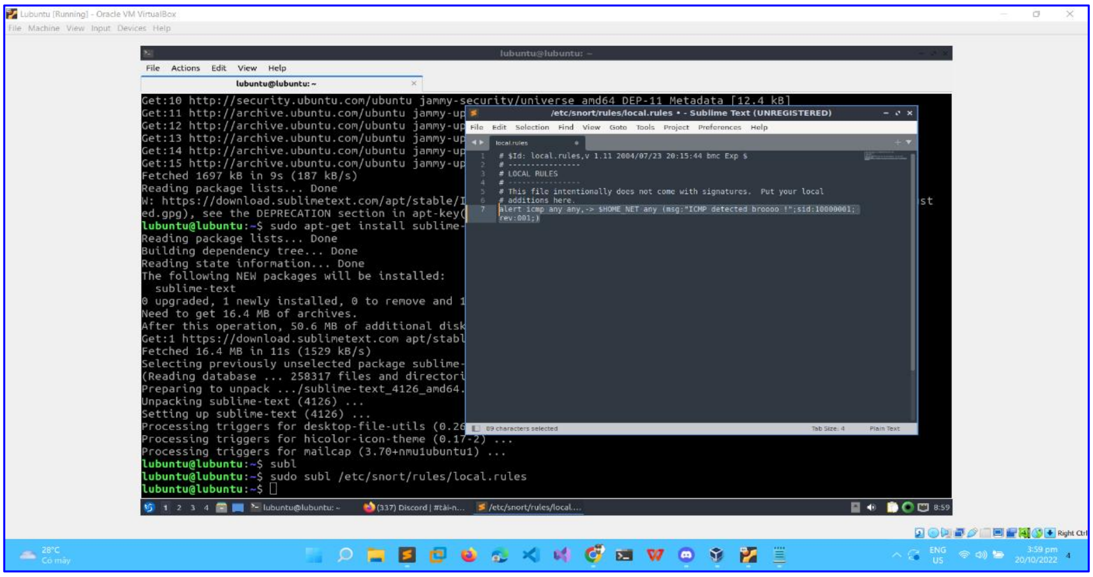
Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
1 2 3 4
(337) Discord | #tài-n...
/etc/snort/snort.conf ...
lubuntu@lubuntu: ~
10:08
Right Ctrl
29°C
Có mây
ENG
US
5:09 pm
20/10/2022

2.3 Configuration

Add this rule to file locals.local

```bash
sudo subl /etc/snort/rules/local.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"ICMP detected broooo !";sid:10000001; rev:001;)
```



```
Get:10 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [12.4 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-up
Get:12 http://archive.ubuntu.com/ubuntu jammy-up
Get:13 http://archive.ubuntu.com/ubuntu jammy-up
Get:14 http://archive.ubuntu.com/ubuntu jammy-up
Get:15 http://archive.ubuntu.com/ubuntu jammy-up
Fetched 1697 kB in 9s (187 kB/s)
Reading package lists... Done
W: https://download.sublimetext.com/apt/stable/I
ed.gpg), see the DEPRECATION section in apt-key(
lubuntu@lubuntu:~$ sudo apt-get install sublime-
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sublime-text
0 upgraded, 1 newly installed, 0 to remove and 1
Need to get 16.4 MB of archives.
After this operation, 50.6 MB of additional disk
Get:1 https://download.sublimetext.com apt/stabl
Fetched 16.4 MB in 11s (1529 kB/s)
Selecting previously unselected package sublime-
(Reading database ... 258317 files and directori
Preparing to unpack .../sublime-text_4126_amd64.
Unpacking sublime-text (4126) ...
Setting up sublime-text (4126) ...
Processing triggers for desktop-file-utils (0.26
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
lubuntu@lubuntu:~$ subl
lubuntu@lubuntu:~$ sudo subl /etc/snort/rules/local.rules
lubuntu@lubuntu:~$ 
```

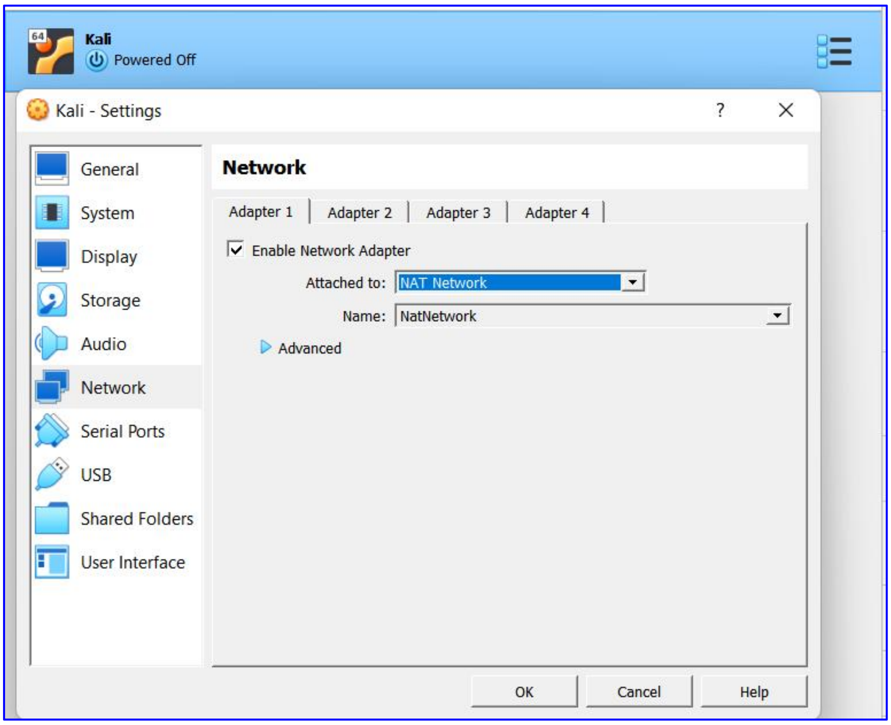
/etc/snort/rules/local.rules • - Sublime Text (UNREGISTERED)

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any,-> $HOME_NET any (msg:"ICMP detected broooo !";sid:10000001;
rev:001;)
```

89 characters selected

Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
File Edit Selection Find View Goto Tools Project Preferences Help
local.rules
Tab Size: 4
Plain Text
lubuntu@lubuntu: ~
(337) Discord | #tài-n...
/etc/snort/rules/local...
8:59
28°C
Có mây
ENG
US
3:59 pm
20/10/2022

Now use a VM kali ping to VM Ubuntu. Make sure that Use NAT network both machine.



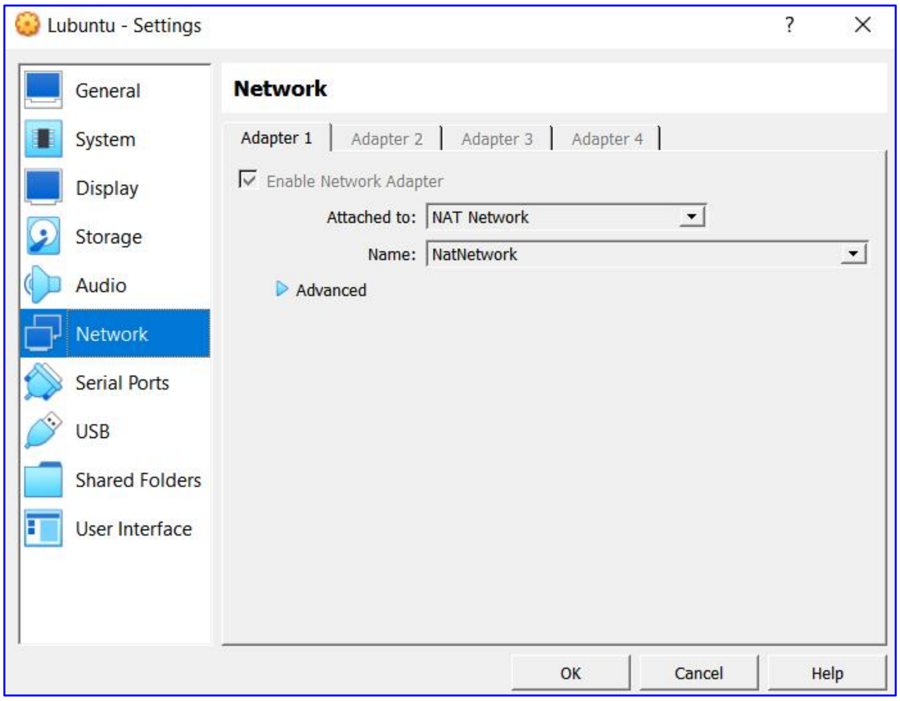
Kali - Settings

Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork



Lubuntu - Settings

Network

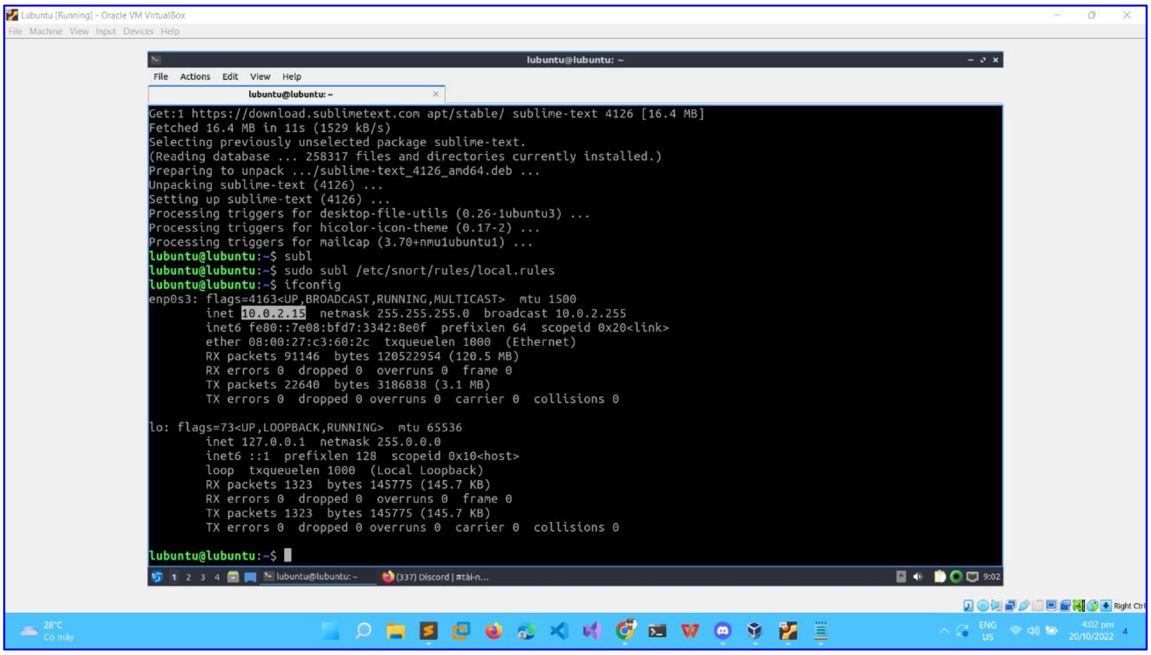
☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

Use ifconfig to know the IP:

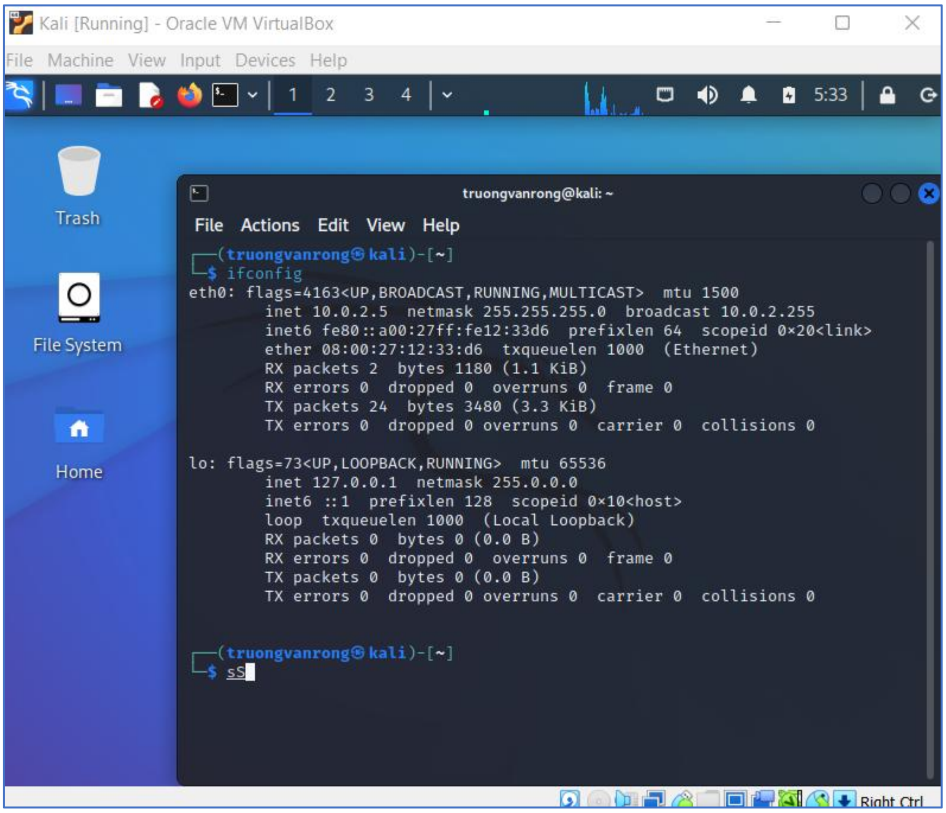
Lubuntu machine → 10.0.2.15



Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
1 2 3 4
lubuntu@lubuntu: ~
(337) Discord | #tải-n...
9:02
Right Ctrl
28°C
Có mây
ENG
US
4:02 pm
20/10/2022

```
Get:1 https://download.sublimetext.com apt/stable/ sublime-text 4126 [16.4 MB]
Fetched 16.4 MB in 11s (1529 kB/s)
Selecting previously unselected package sublime-text.
(Reading database ... 258317 files and directories currently installed.)
Preparing to unpack .../sublime-text_4126_amd64.deb ...
Unpacking sublime-text (4126) ...
Setting up sublime-text (4126) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
lubuntu@lubuntu:~$ subl
lubuntu@lubuntu:~$ sudo subl /etc/snort/rules/local.rules
lubuntu@lubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::7e08:bfd7:3342:8e0f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c3:60:2c  txqueuelen 1000  (Ethernet)
        RX packets 91146  bytes 120522954 (120.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22640  bytes 3186838 (3.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1323  bytes 145775 (145.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1323  bytes 145775 (145.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lubuntu@lubuntu:~$ 
```

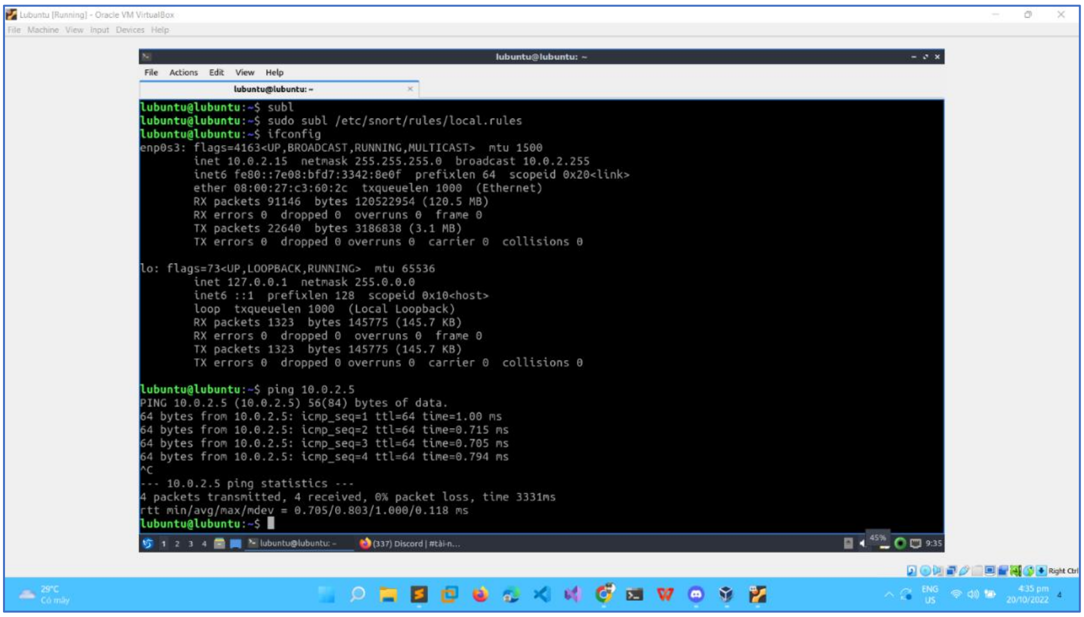
Kali → 10.0.2.5



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:33
Trash
File System
Home
truongvanrong@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(truongvanrong㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe12:33d6  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:12:33:d6  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 1180 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3480 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(truongvanrong㉿kali)-[~]
└─$ ss
```

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

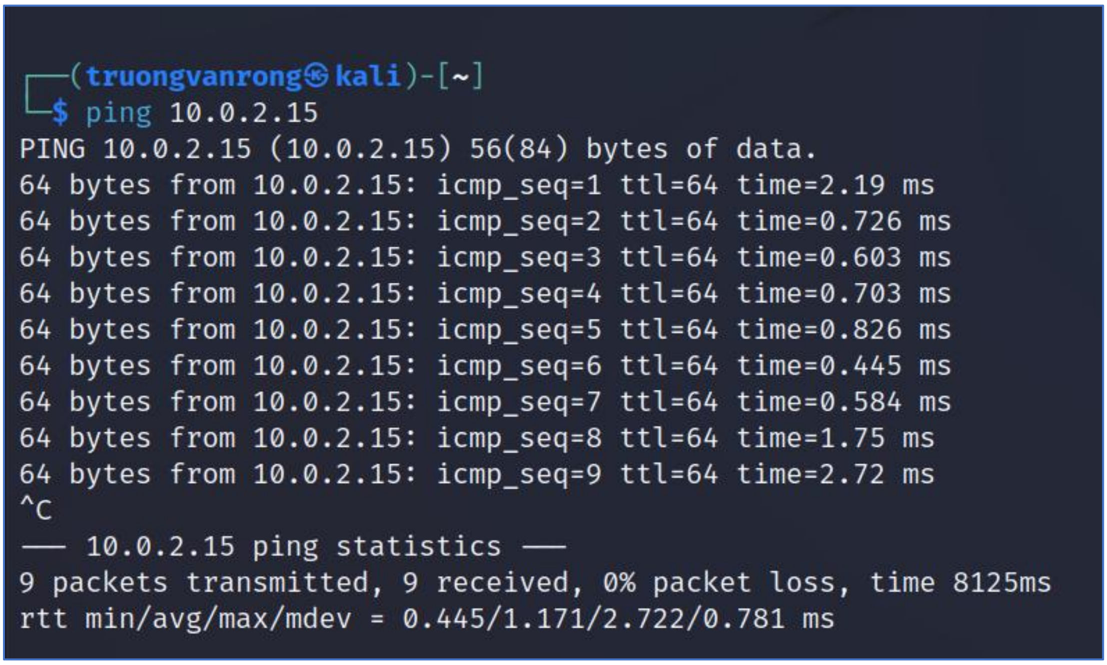

Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
lubuntu@lubuntu: ~
(337) Discord | #tài-n...

```
lubuntu@lubuntu:~$ subl
lubuntu@lubuntu:~$ sudo subl /etc/snort/rules/local.rules
lubuntu@lubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::7e08:bfd7:3342:8e0f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c3:60:2c  txqueuelen 1000  (Ethernet)
        RX packets 91146  bytes 120522954 (120.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22640  bytes 3186838 (3.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1323  bytes 145775 (145.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1323  bytes 145775 (145.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lubuntu@lubuntu:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.715 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.705 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.794 ms
^C
--- 10.0.2.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3331ms
rtt min/avg/max/mdev = 0.705/0.803/1.000/0.118 ms
lubuntu@lubuntu:~$
```

III.Result

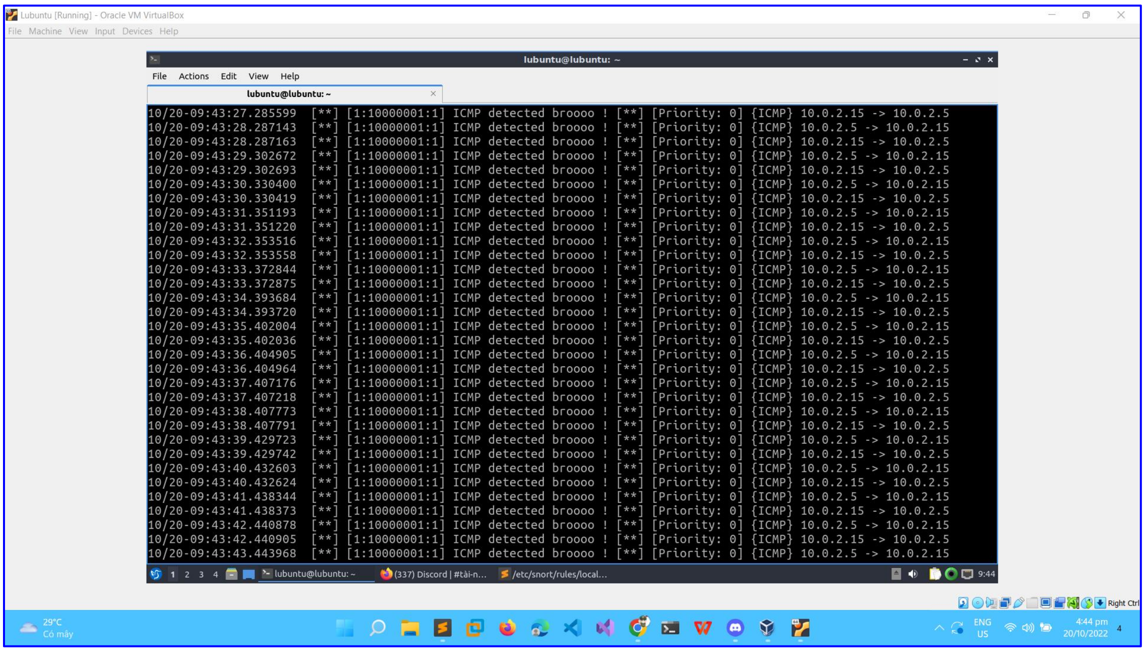
❖ Basic result:

Kali VM:



```
┌──(truongvanrong㉿kali)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=2.19 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.726 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.603 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.703 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.826 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.445 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.584 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=1.75 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=2.72 ms
^C
── 10.0.2.15 ping statistics ──
9 packets transmitted, 9 received, 0% packet loss, time 8125ms
rtt min/avg/max/mdev = 0.445/1.171/2.722/0.781 ms
```

Lubuntu VM:



```
10/20-09:43:27.285599  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:28.287143  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:28.287163  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:29.302672  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:29.302693  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:30.330400  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:30.330419  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:31.351193  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:31.351220  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:32.353516  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:32.353558  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:33.372844  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:33.372875  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:34.393684  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:34.393720  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:35.402004  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:35.402036  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:36.404905  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:36.404964  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:37.407176  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:37.407218  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:38.407773  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:38.407791  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:39.429723  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:39.429742  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:40.432603  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:40.432624  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:41.438344  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:41.438373  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:42.440878  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
10/20-09:43:42.440905  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.15 -> 10.0.2.5
10/20-09:43:43.443968  [**] [1:10000001:1] ICMP detected broooo ! [**] [Priority: 0] {ICMP} 10.0.2.5 -> 10.0.2.15
```

Lubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lubuntu@lubuntu: ~
File Actions Edit View Help
lubuntu@lubuntu: ~
1 2 3 4
lubuntu@lubuntu: ~
(337) Discord | #tài-n...
/etc/snort/rules/local...
9:44
Right Ctrl
29°C
Có mây
ENG
US
4:44 pm
20/10/2022

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

---

END