LAB REPORT

Subject: Intrusion Detection and Prevention System

Session 02

Topic name: Snort Inline

1. GENERAL INFORMATION:

Num	Full name	Student ID	Email
1	Nguyen Dinh Kha	20520562	20520562@gm.uit.edu.vn
2	Le Sy Cuong	20521149	20521149@gm.uit.edu.vn

2. IMPLEMENTATION CONTENT

Num	Work	Component	Personal Responsible	Self-assessment Result
1				
2				

The section below of this report is the detailed documentation from the practical group.

DETAILED REPORT

Students undertake the practical exercise with the requirements below.

A.1 Explore and use Snort

Requirement 1: Students to answer the questions below.

1.1 a. What is Snort? In what modes can Snort operate?

Snort is an open-source Network Intrusion Detection System (IDS). It has the capability to monitor network traffic and detect intrusion activities, attacks, and other suspicious behaviors in the network. Snort can operate in the following modes:

Sniffer mode: This mode allows Snort to listen to and display network traffic from a specific network interface. It provides the capability to analyze network traffic and display packets on the screen. This mode is often used for monitoring and analyzing network-related issues.

Packet Logger mode: Snort can function as a tool for logging network packets into a file for later analysis. This mode allows Snort to store complete network packet data, including information on intrusion events detected by Snort.

Network Intrusion Detection mode: This is Snort's primary mode. It enables Snort to detect and alert on intrusion activities, attacks, and other suspicious behaviors in the network. Snort uses rules to match and detect known attack patterns.

Network Intrusion Prevention mode: This mode allows Snort to prevent intrusion activities and attacks by performing response actions on network traffic. This may include blocking intrusive packets, mitigating the impact of attacks, and protecting the network.

b. Describe the main features of Snort?

Snort has the following key features:

- **Intrusion detection:** Snort can detect intrusion activities and attacks in the network. It uses rules to match and detect known attack patterns. Snort also supports the detection of new attacks through dynamic analysis methods and the identification of abnormal behaviors.
- **Flexible rule management:** Snort allows users to create and customize rules to fit their specific requirements. Users can define attack patterns, protocols, IP addresses, and other attributes to create custom rules. This makes Snort flexible and capable of detecting unique attacks in the network.
- **Support for network protocols:** Snort supports many popular network protocols such as TCP, UDP, ICMP, and application protocols like HTTP, FTP, SMTP, and DNS. This enables Snort to monitor and detect intrusion activities across various layers and protocols in the network.
- **Flexible integration:** Snort can integrate with other tools and systems in the network environment. It can send alerts to Security Information and Event Management (SIEM) systems, log events to databases, or trigger response actions like blocking intrusive packets. Snort also supports communication protocols like Syslog and SNMP for interacting with other systems.

B.2 Install and configure Snort for network monitoring

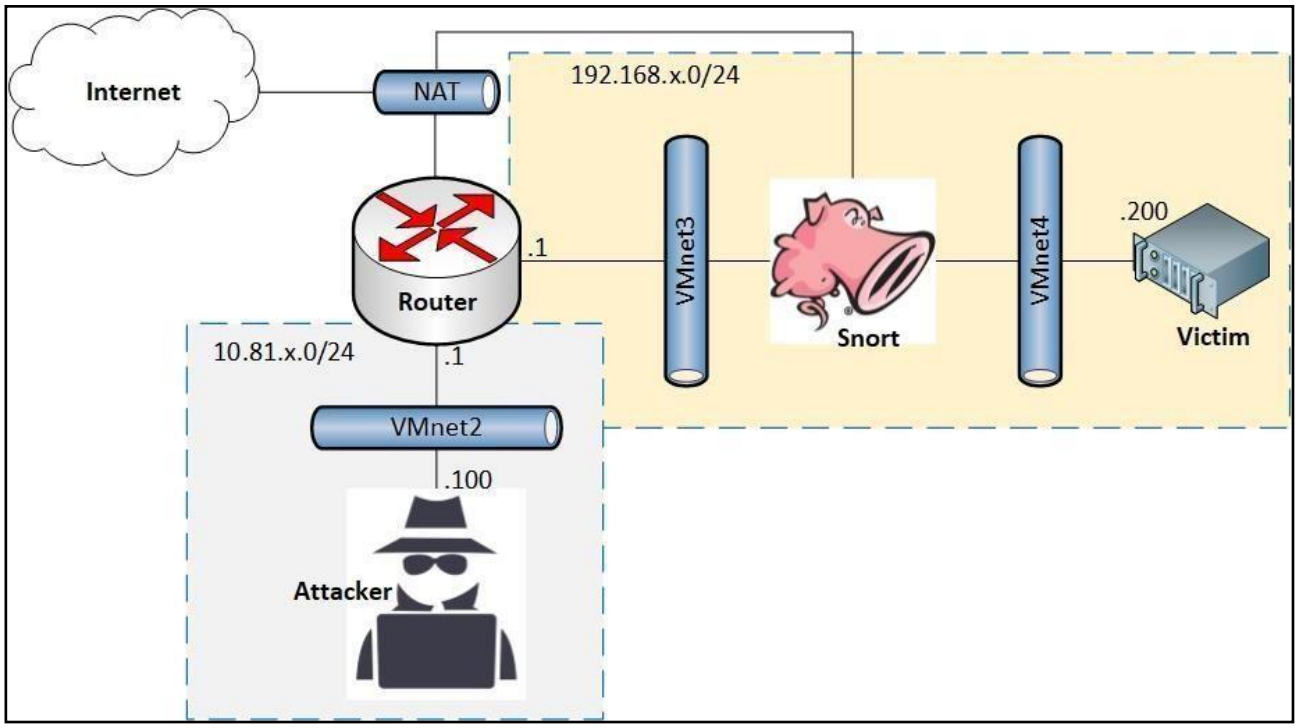


Figure 1. Snort Inline deployment model

Note: In the deployment model, x represents the last two digits of a team member's student ID number.

Yêu cầu 2: Sinh viên cài đặt và cấu hình Snort Inline theo các bước bên dưới. Chụplại các hình ảnh minh chứng (chụp full màn hình) cho từng bước làm.

2.1a. Network configuration for the devices according to the model

Students are to configure 04 virtual machines according to the model described in Figure 1.

Note: This guide is performed on VMware Workstation.

- Check that the VMnet8 (NAT) card exists and DHCP is enabled.

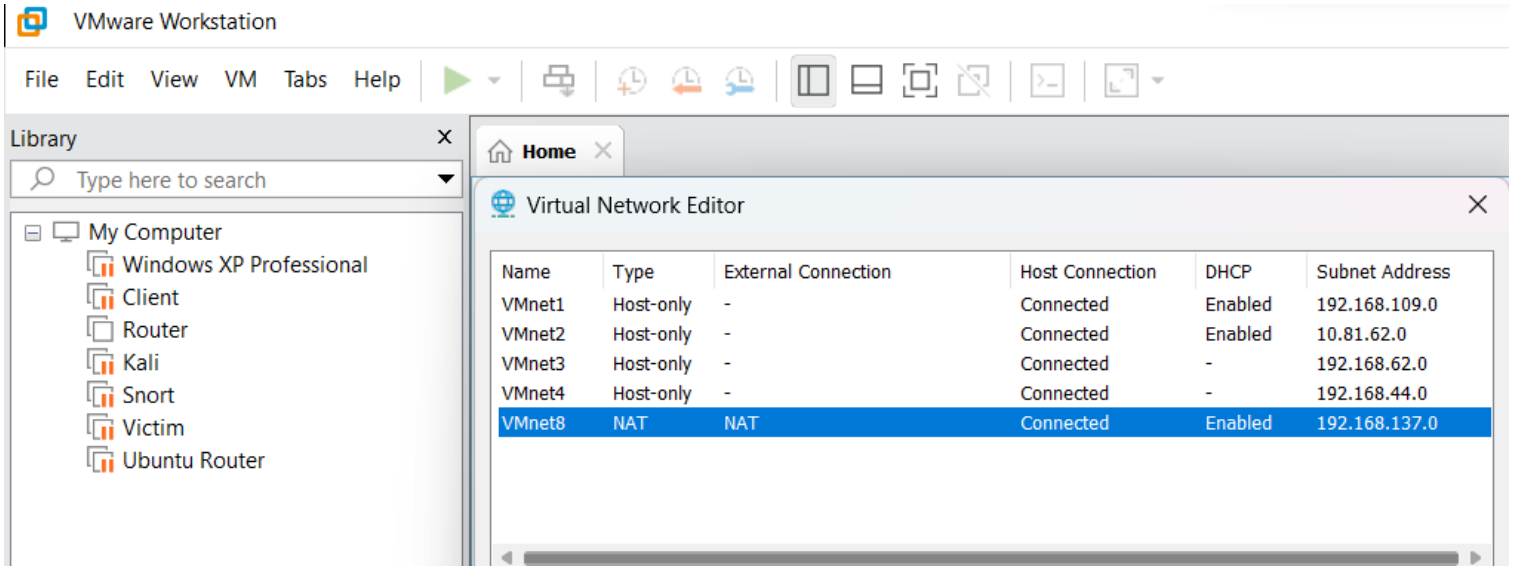


Figure 2. Checking the VMnet8 card

- Assign network cards to the **Router machine:**

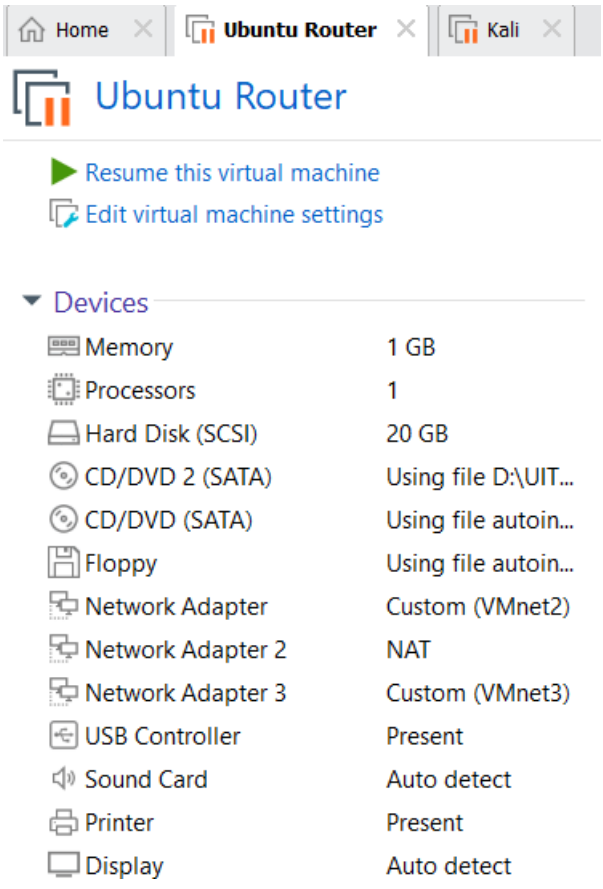


Figure 3. Settings of the Ubuntu Router machine

- Assign a network card to the **Kali machine:**

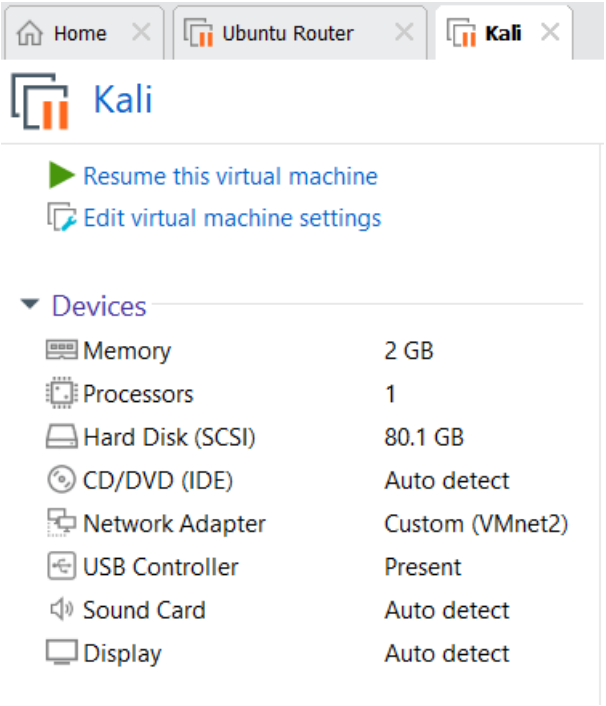


Figure 4. Settings of the Attacker (Kali) machine

- Assign a network card to the **Snort machine:**

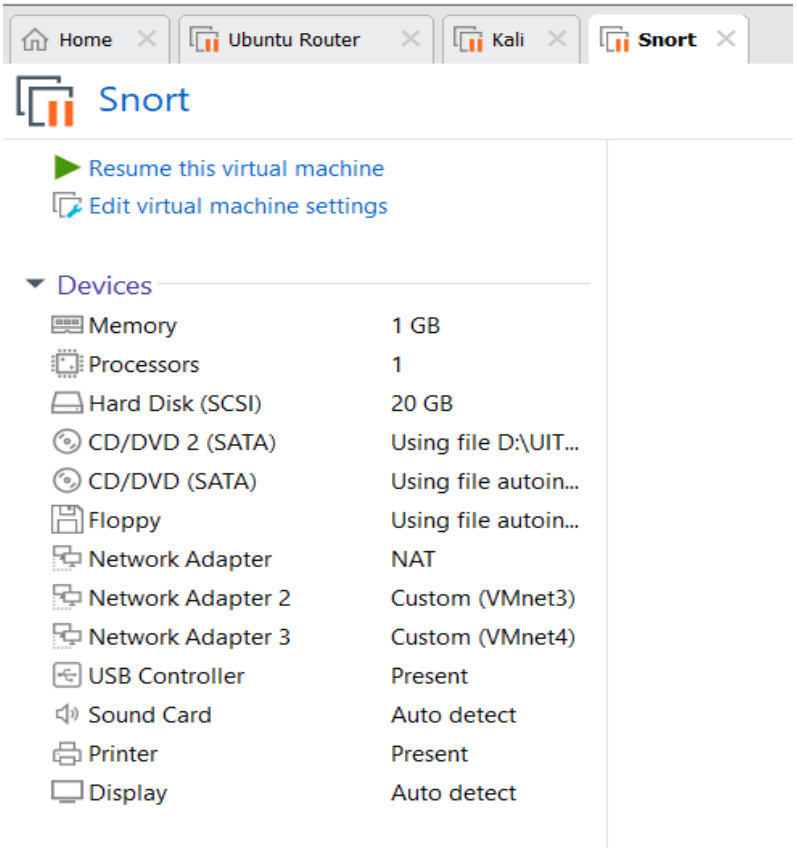


Figure 4. Settings of the IDS machine with Snort installed

- Assign a network card to the **Victim machine:**

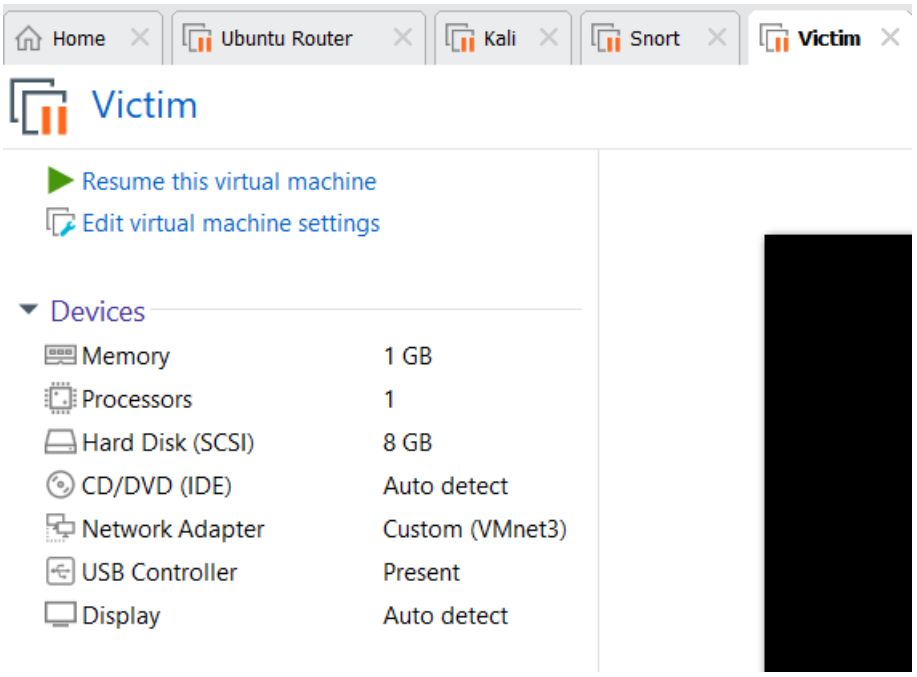


Figure 5. Settings of the Victim (Metasploitable) machine

2.1b. IP address configuration for the machines

- Router machine:

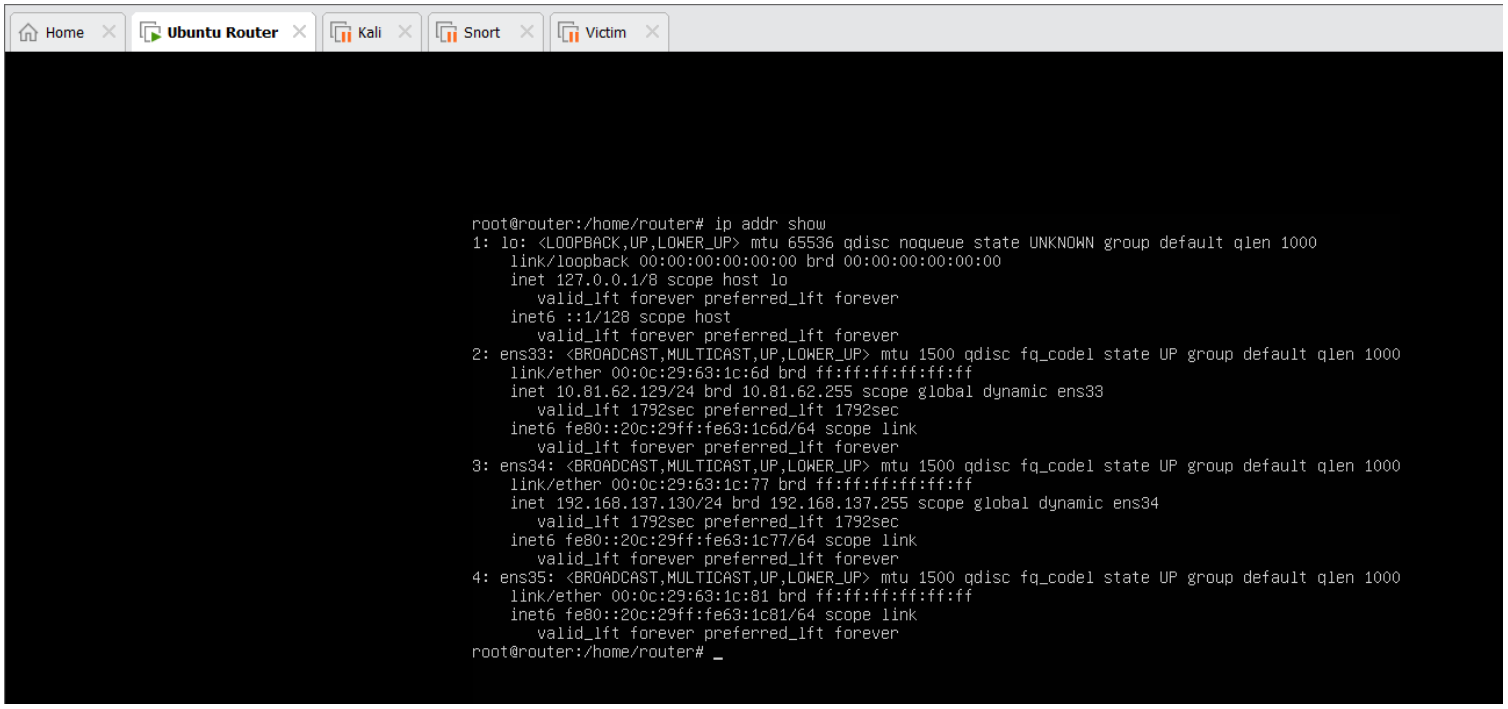


Figure 6. Ubuntu Router's IP show result after configuration

- Kali machine:

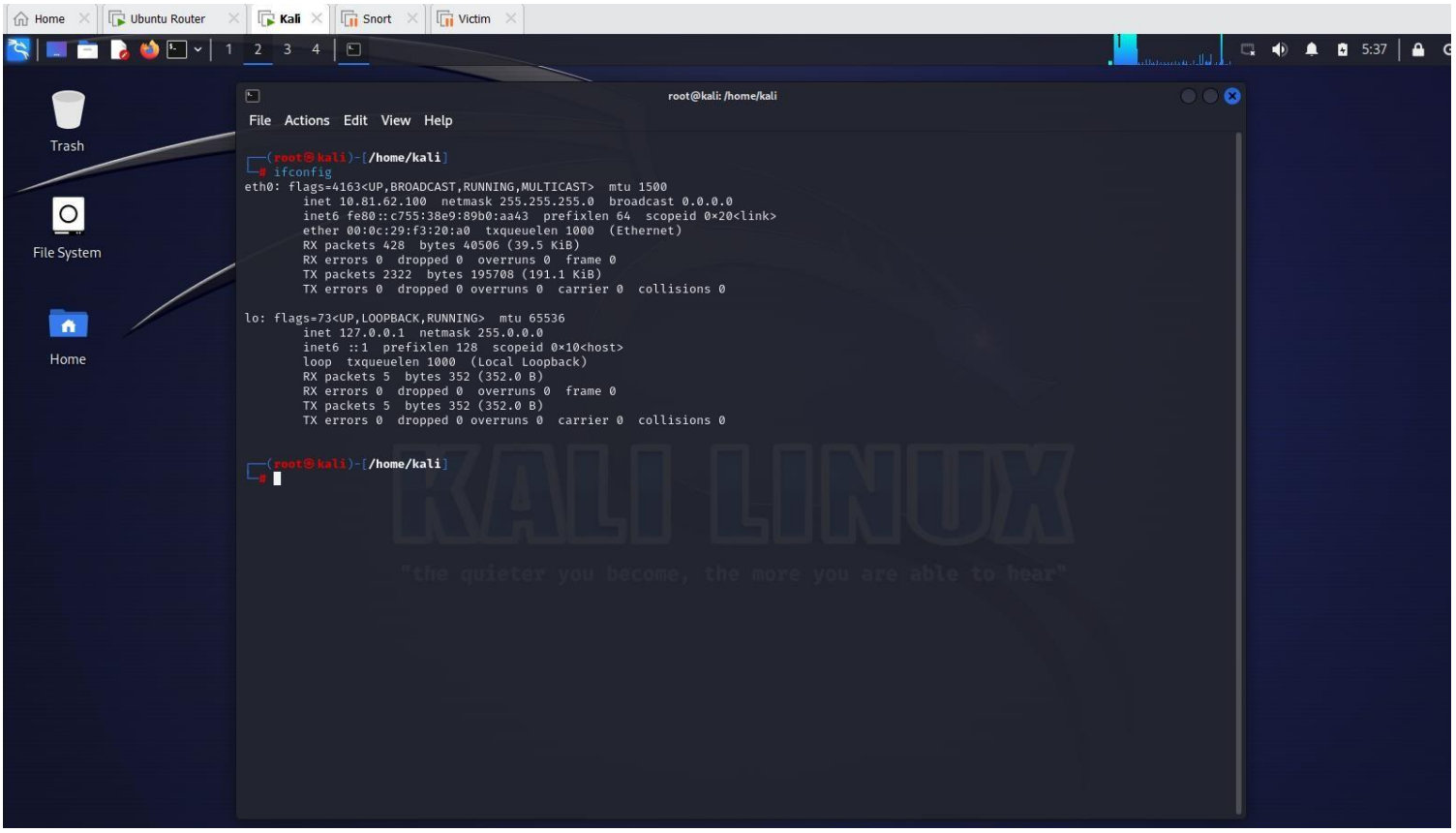


Figure 7. Attacker's IP show result after configuration

- Snort machine:

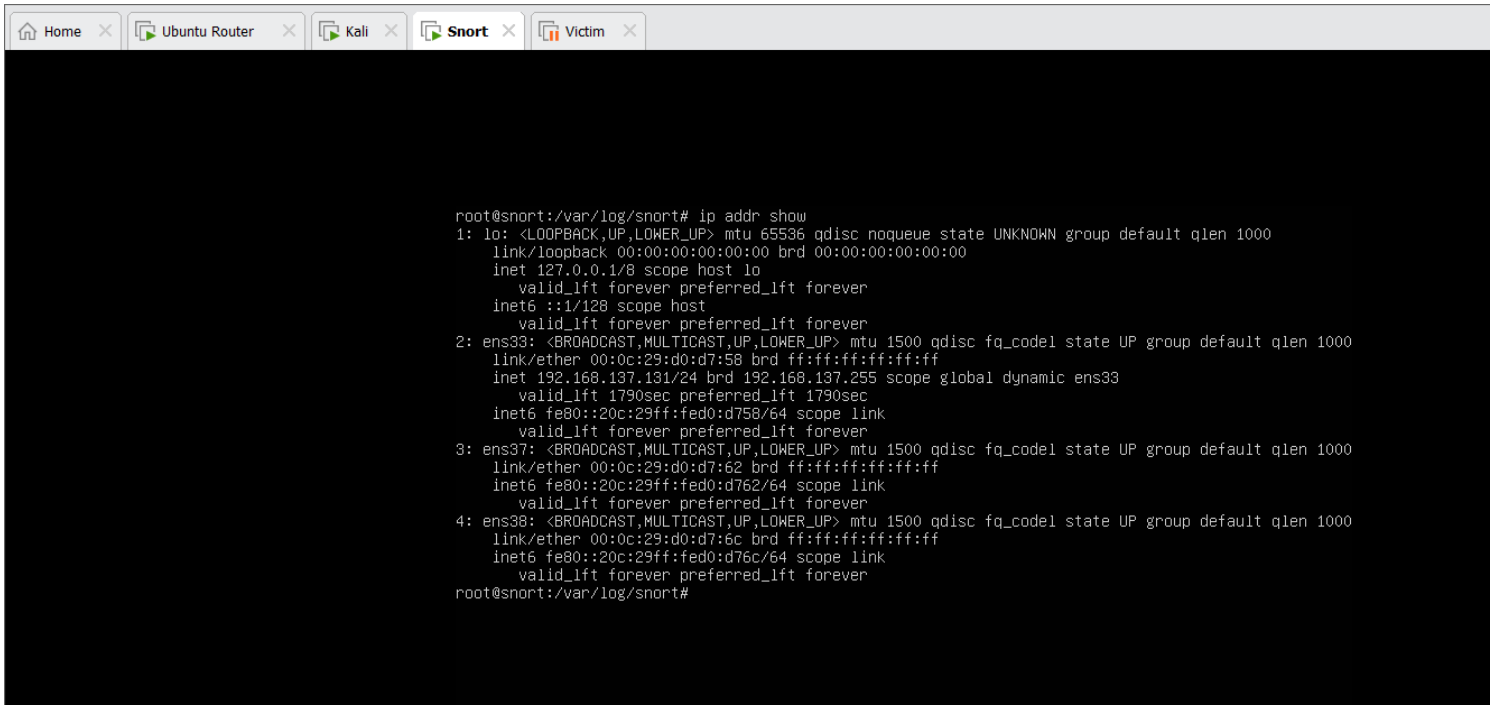


Figure 8. Snort machine's IP show result after configuration

- Victim machine:

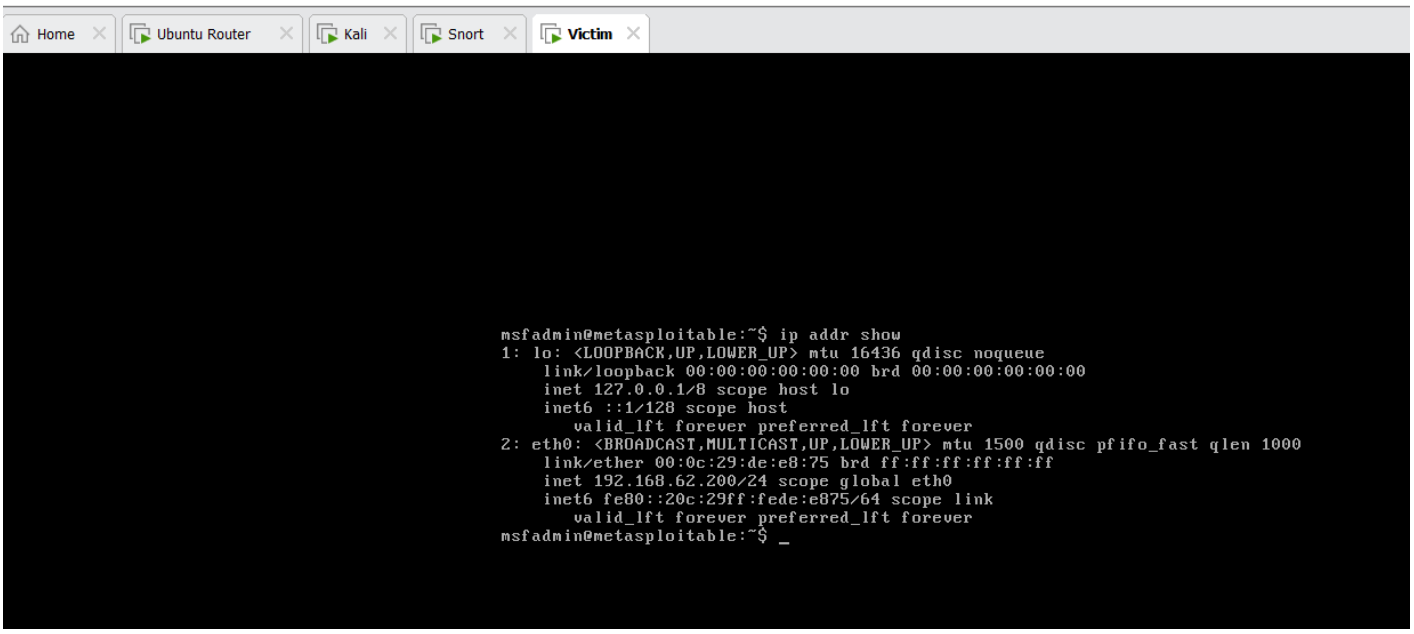
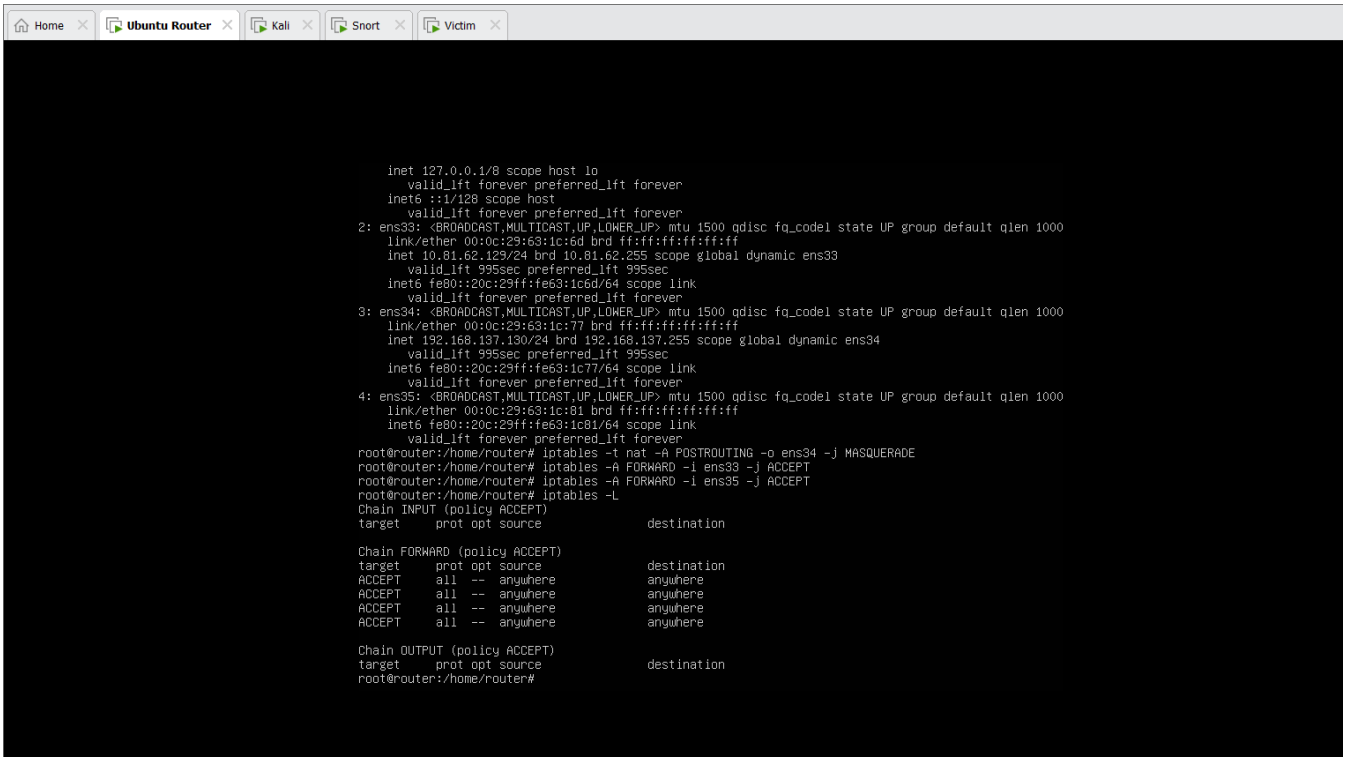
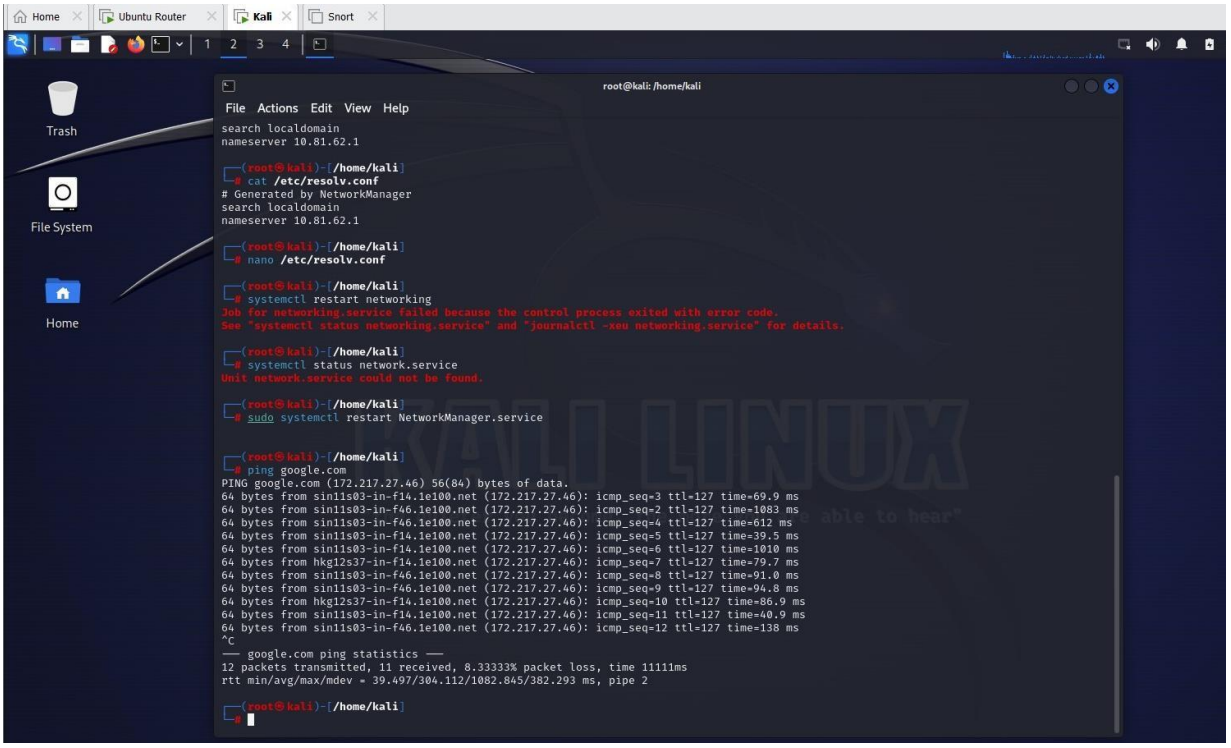


Figure 9. Victim's IP show result after configuration

2.1c. Configure outbound NAT for the router machine

- Configuring outbound NAT allows devices within the network to access the Internet. After successfully configuring NAT, the Kali machine can connect to the Internet.

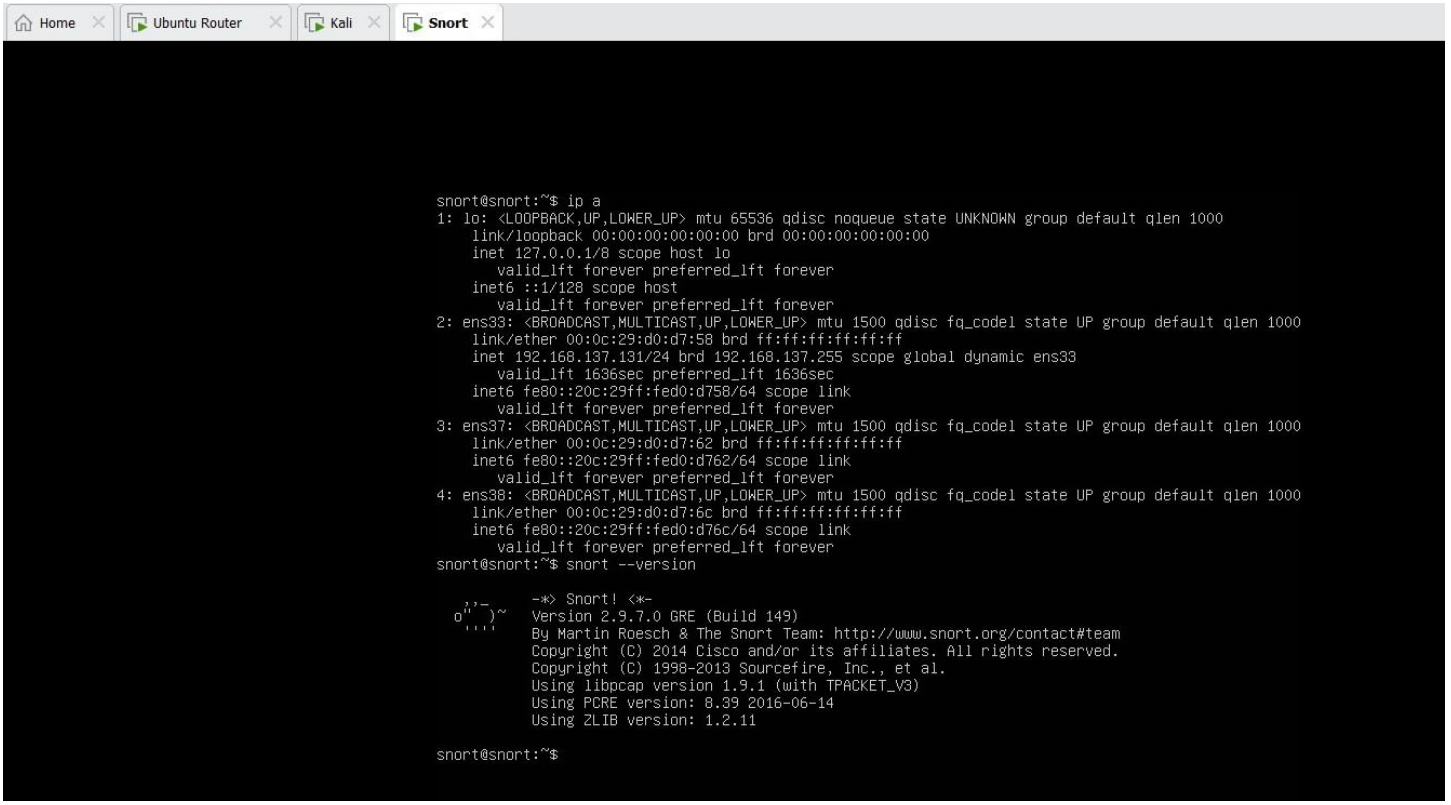




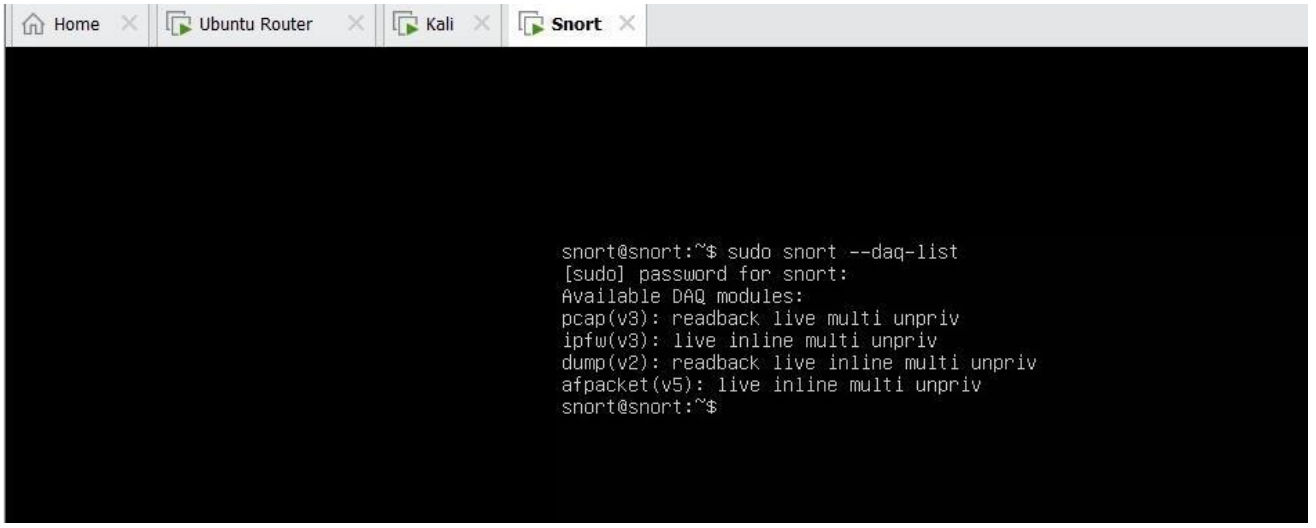
2.1d. Installation and configuration of Snort

Note: This guide is for installing Snort on Ubuntu Server.

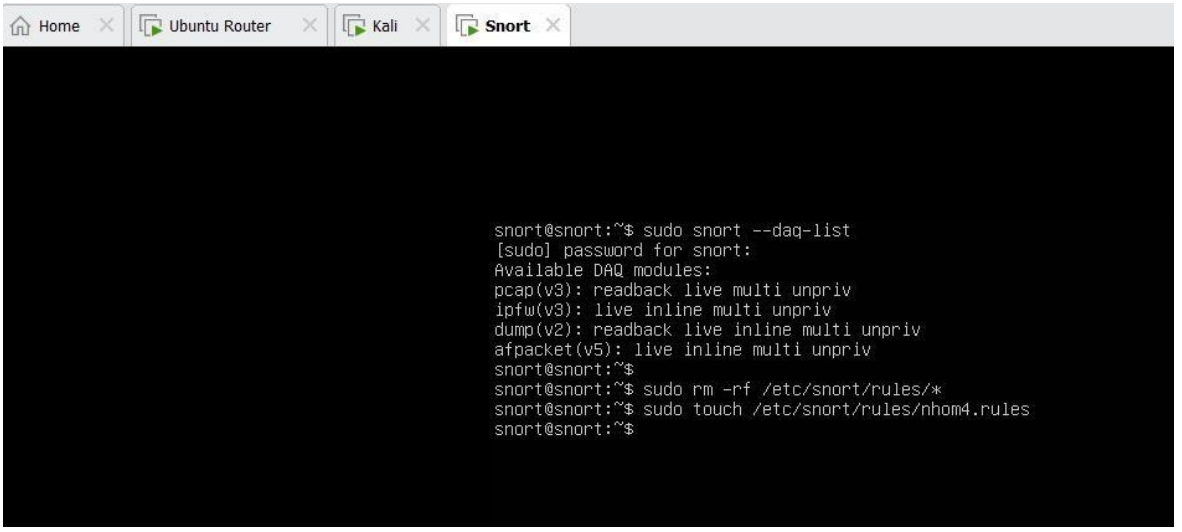
- Install Snort using the APT tool. After successful installation, check the Snort version.



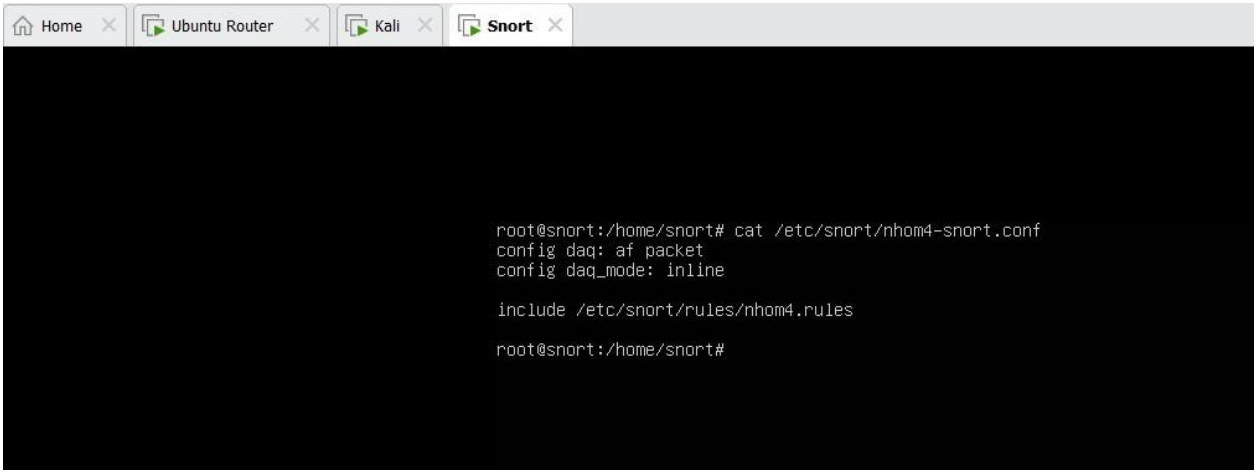
- Ensure the afpacket DAQ is installed to use inline mode.



- Delete all default Snort rule files.
- Create a rule file defined by the team.

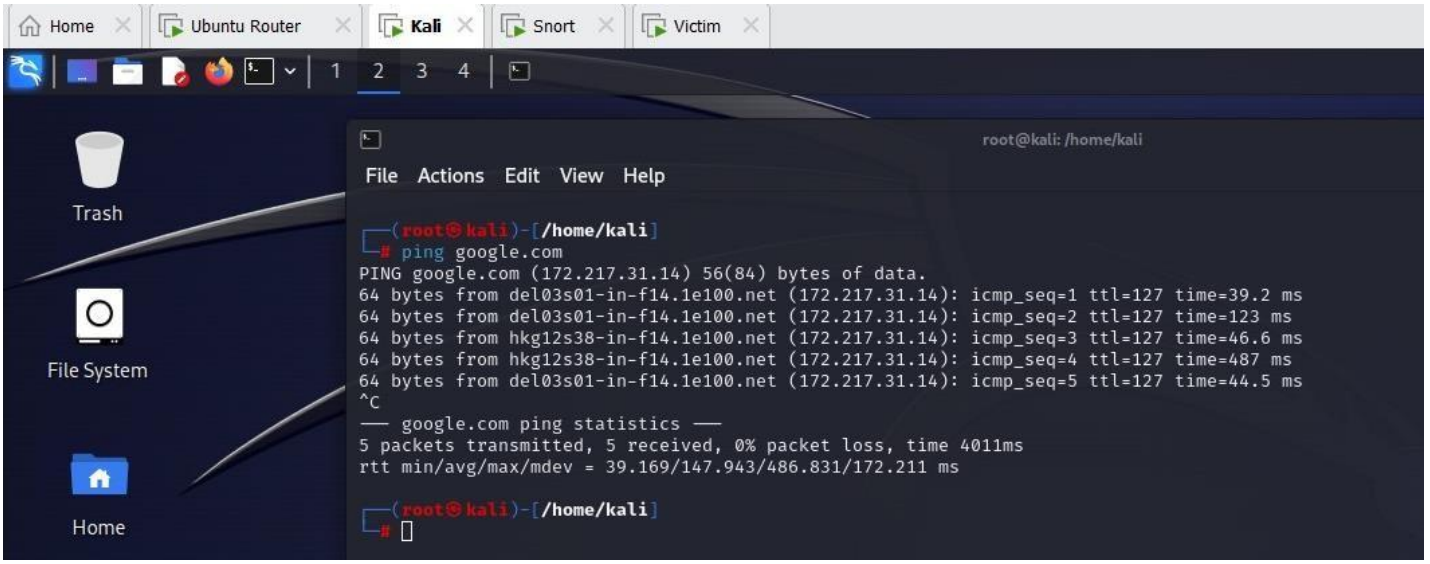


- Create the team's Snort configuration file at /etc/snort/nhom4-snort.conf with the content below to enable inline mode.

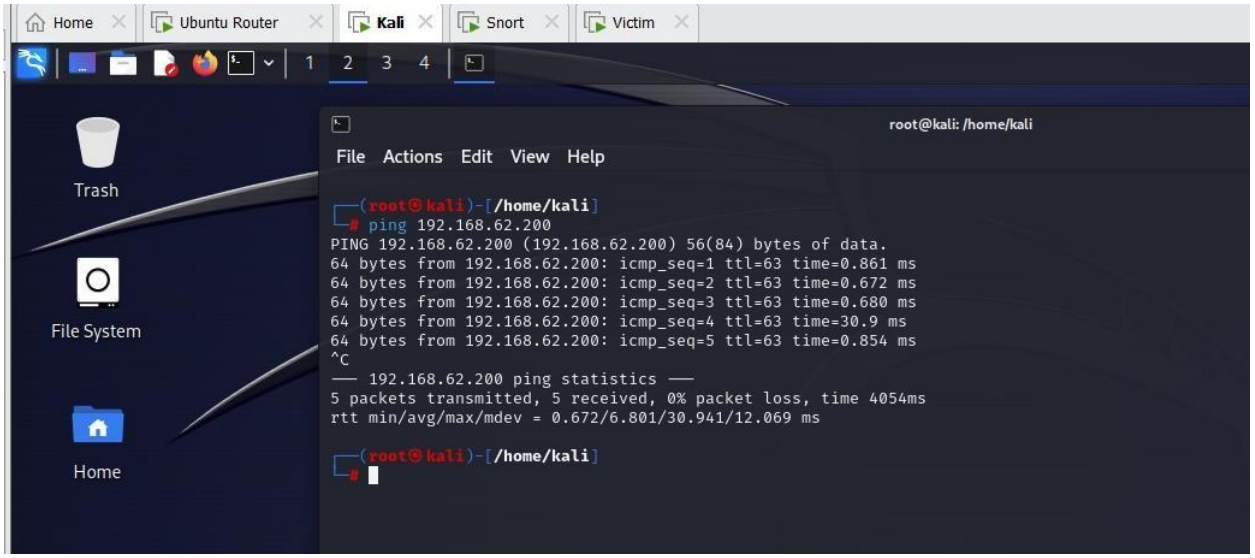


Lab 2: Deploying Snort Inline

- After running successfully, check the connectivity of the machines.
  - **Kali machine** ping google.com



  - **Kali machine** ping **Victim machine**



  - **Victim machine** ping google.com

Home | Ubuntu Router | Kali | Snort | Victim

```
    inet6 fe80::20c:29ff:fede:e875/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.24.238

msfadmin@metasploitable:~$ ping google.com
PING google.com (216.58.203.78) 56(84) bytes of data.
64 bytes from hkg07s48-in-f14.1e100.net (216.58.203.78): icmp_seq=1 ttl=127 time
=34.9 ms
64 bytes from kul09s03-in-f14.1e100.net (216.58.203.78): icmp_seq=2 ttl=127 time
=54.7 ms
64 bytes from kul09s03-in-f14.1e100.net (216.58.203.78): icmp_seq=3 ttl=127 time
=86.3 ms
64 bytes from hkg07s48-in-f14.1e100.net (216.58.203.78): icmp_seq=4 ttl=127 time
=61.1 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 15331ms
rtt min/avg/max/mdev = 34.962/59.336/86.393/18.374 ms
msfadmin@metasploitable:~$
```

2.1e. Writing rules for Snort

Write a rule to detect ICMP packets sent to the network layer 192.168.x.0/24 in the file

/etc/snort/rules/nhomX.rules

Check Snort's log on the console and **/var/log/snort/alert**.