Network Security - Assignment 6

In this assignment, you will be installing and configuring Snort for your Ubuntu Virtual Machine. This is only scratching the surface of how you can utilize snort. Play around and check out the configuration files! Take screenshots of your work and answer the questions as you go. Add your lab to your Home Lab GitHub repo. Your submission must be the link to your repo.

Step 1: Update the System

Ensure your system is up to date before installing Snort:

```
sudo apt update
sudo apt upgrade -y
```

Step 2: Install Snort

You can install Snort directly using `apt`:

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

During installation, you will be prompted to enter the network interface and the HOME_NET IP range that Snort will monitor.

1. **Network Interface**: Enter the interface you want Snort to monitor (e.g., `eth0`, `enX0`, `ens33`, etc.).
2. **HOME_NET**: Define your home network (e.g., `192.168.1.0/24`, for a private network or `any` to monitor all networks).

After installation, Snort will be installed to `/etc/snort/` with the default configuration and rules.

To find your network interface, you can run the command:

```
ip a
```

As an example, in my output in my VM on AWS, I get the following:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000

    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

    inet 127.0.0.1/8 scope host lo

       valid_lft forever preferred_lft forever

    inet6 ::1/128 scope host noprefixroute

       valid_lft forever preferred_lft forever

2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP
group default qlen 1000

    link/ether 12:cc:c1:e1:14:7d brd ff:ff:ff:ff:ff:ff

    inet 172.31.85.58/20 metric 100 brd 172.31.95.255 scope global dynamic
enX0

       valid_lft 2859sec preferred_lft 2859sec

    inet6 fe80::10cc:c1ff:fee1:147d/64 scope link

       valid_lft forever preferred_lft forever
```

With this information, I will set my **Network Interface** to `172.31.85.58/20`, and I will set my **HOME_NET** to `enX0`.

Step 3: Configure Snort

If you want to customize the Snort configuration, open the main configuration file:

```
sudo nano /etc/snort/snort.conf
```

Key sections to check in `snort.conf`:

- **HOME_NET**: Ensure it matches your network setup. You can adjust the `ipvar HOME_NET` if needed:

  ```
  ipvar HOME_NET 192.168.1.0/24  # Or whatever network range is appropriate
  ```

Check out the various files in the /etc/snort directory.

Step 4: Update and Manage Snort Rules

By default, Snort comes with community rules, but you can download and add additional rules for better threat detection.

If needed only, to download community rules:

```
sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz
sudo tar -xvzf community-rules.tar.gz
sudo cp community-rules/* /etc/snort/rules/
```

If you want to add your own rules, you can manually edit the local rule file:

```
sudo nano /etc/snort/rules/local.rules
```

Then, add custom rules if needed. For example:

```
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;)
```

Check out the various rule files file in the rules directory. Which rules stick out to you? What is the purpose of rules in general?

Step 5: Test Snort Configuration

After configuring, test that Snort is working properly by running a configuration test:

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

If the configuration is correct, you'll see a message like:

```
Snort successfully validated the configuration!
```

Step 6: Running Snort in IDS Mode

Now that Snort is installed and configured, you can run it in IDS mode to monitor traffic. Specify the interface to monitor (e.g., `eth0`, `enX0`, etc.):

```
sudo snort -c /etc/snort/snort.conf -i eth0
```

Snort will now monitor network traffic and log alerts. To exit, hit `ctrl+c`.

Step 7: Viewing Snort Logs

Snort logs alerts in the `/var/log/snort/` directory. Go to this directory. What files did you find here? Do any of them contain any content? Why or why not?

Step 8: Running Snort as a Daemon

To run Snort in the background as a daemon, use the following. Specify the interface to monitor (e.g., `eth0`, `enX0`, etc.):

```
sudo snort -D -c /etc/snort/snort.conf -i eth0
```

This will keep Snort running in the background, continuously monitoring the specified network interface.

To see to the different processes running in your system, use the command `top`. If you wait a few seconds, you should see Snort running. If you wanted to stop the Snort process from running, what is the command to terminate it?