LAB :: SNORT (IDS)

> # super user command.
> $ normal user command.
> X replace with your group no.

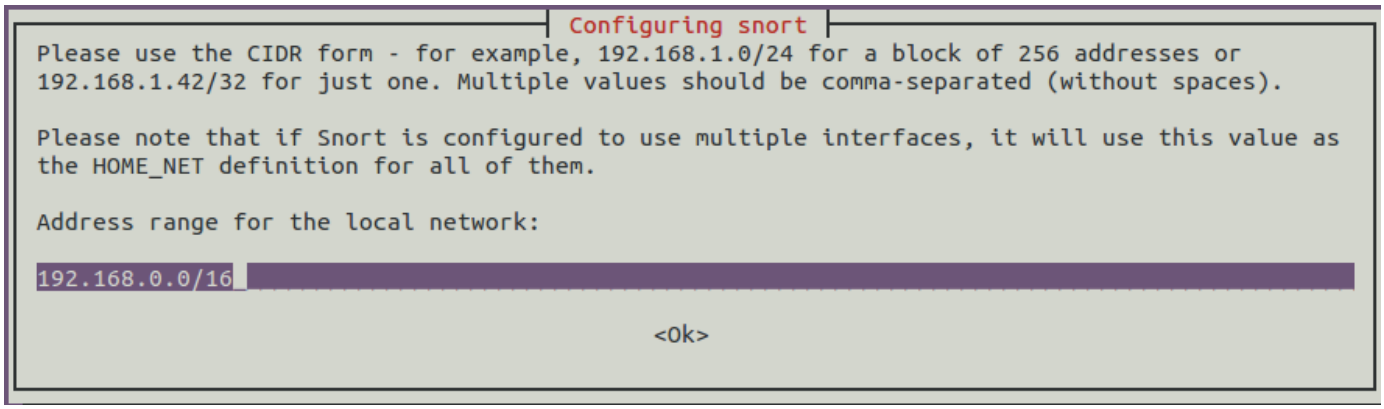
Topology

[group1.df-h.net] [192.168.1.11]
[group2.df-h.net] [192.168.1.12]
[group3.df-h.net] [192.168.1.13]
[group4.df-h.net] [192.168.1.14]
[group5.df-h.net] [192.168.1.15]
[group6.df-h.net] [192.168.1.16]
[group7.df-h.net] [192.168.1.17]
[group8.df-h.net] [192.168.1.18]
[group9.df-h.net] [192.168.1.19]
[group10.df-h.net] [192.168.1.20]
[group11.df-h.net] [192.168.1.21]
[group12.df-h.net] [192.168.1.22]
[group13.df-h.net] [192.168.1.23]
[group14.df-h.net] [192.168.1.24]
[group15.df-h.net] [192.168.1.25]
[group16.df-h.net] [192.168.1.26]
[group17.df-h.net] [192.168.1.27]
[group18.df-h.net] [192.168.1.28]
[group19.df-h.net] [192.168.1.29]
[group20.df-h.net] [192.168.1.30]

Install SNORT

```
$ sudo apt-get install snort
```

It will ask for your HOME_NET. For this lab define it as your host IP. For group1 it will `192.168.1.11/32`. If required we can change it from snort.conf file also.



After installation check the installation location of SNORT

```
$ whereis snort
```

Few important location

1. SNORT configuration : `/etc/snort/snort.conf`
2. SNORT debian configuration : `/etc/snort/snort.debian.conf`
3. SNORT rules : `/etc/snort/rules`
4. SNORT exuecuble : `/usr/sbin/snort`

Configure SNORT

Check HOME_NET and Interface related configuration from `/etc/snort/snort.debian.conf`. During installation process if you define your HOME_NET properly; no need to edit it. Or you can edit this file.

The main configuration file for SNORT is `/etc/snort/snort.conf` file.

```
$ sudo vi /etc/snort/snort.conf
```

This is a big configuration file; for lab purpose we will disable all predefined rules. Disable (put #) all the line having `include $RULE\_PATH` (in Step 7 of configuration file) except `include $RULE\_PATH/local.rules`. We will pur all our local rules in `include $RULE\_PATH/local.rules`

To enable alert log; comment (adding # before the line) the following line:

```
output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan
_event_types
```

Save and quit from `snort.conf` file `:wq`
Start SNORT `# /etc/init.d/snort start`
Check whether SNORT is running `# ps -ef|grep snort`

SNORT Rules

Snort rules are divided into two logical sections:

1. Rule Header : The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information.
2. Rule Options : The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

The First Bad Rule

Add the following rules in `/etc/snort/rules/local.rules`

```
alert ip any any -> any any (msg: "IP Packet detected"; sid: 10000;)
```

Save and exit. Restart `snort` service

```
$ sudo /etc/init.d/snort restart
```

This rules will generate alert for every packet. Try to ping any destination and check `alert` log file:

```
# tail -f /var/log/snort/alert
```

SNORT Exercise

Excercise 1 : Write a rules to check XMAS scan on your server from external network
Exercise 2 : Write a rules to check any external network access your webserver /admin pages
Exercise 3 : Write a rules to check SSH brute force attack and log IP trying to connect more than 3 times in 60 seconds