LAB :: SNORT (IDS)

- `#` super user command.
- `$` normal user command.
- Username `apnic` and password `training`.

VM Details

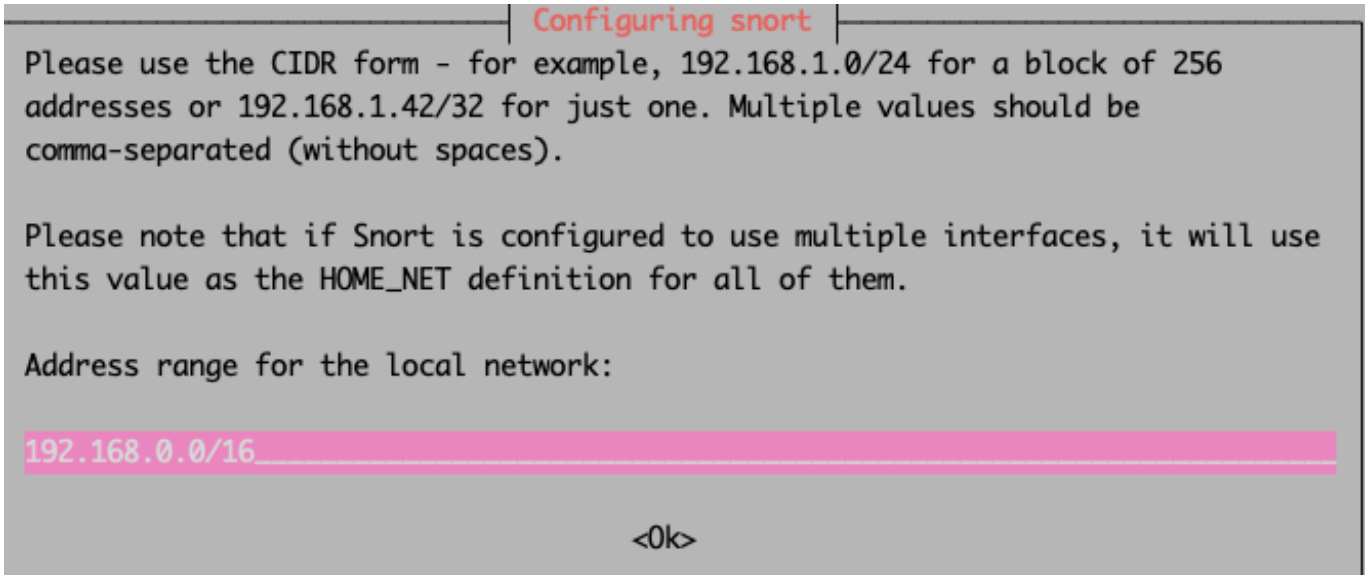
```
[group01.apnictraining.net] [192.168.30.1]
[group02.apnictraining.net] [192.168.30.2]
......
[group10.apnictraining.net] [192.168.30.10]
[group11.apnictraining.net] [192.168.30.11]
......
[group20.apnictraining.net] [192.168.30.20]
[group21.apnictraining.net] [192.168.30.21]
......
[group30.apnictraining.net] [192.168.30.30]
```

Install SNORT

1. Install SNORT:

   ```
   sudo apt update
   sudo apt install snort
   ```

2. It will ask for your `HOME_NET` address. For this lab define it as your host IP. Example, for `group 11` it will `192.168.30.11/32`. If required we can change it later from `snort.debian.conf` file also.



3. Check the installation location of SNORT

```
whereis snort
```

Few important location

- SNORT configuration : `/etc/snort/snort.conf`
- SNORT debian configuration : `/etc/snort/snort.debian.conf`
- SNORT rules : `/etc/snort/rules`
- SNORT exuecuble : `/usr/sbin/snort`

Configure SNORT

1. Check `HOME_NET` and Interface related configuration on `/etc/snort/snort.debian.conf` .
    - During installation process if you had defined your HOME_NET properly; no need to edit it. Else, you can edit this file.
2. 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 the purpose of this lab we will disable all predefined rules (ruleset).
    - Disable (comment out `#`) all the line having `include $RULE_PATH` (in Step 7 of configuration file) except `include $RULE_PATH/local.rules` .
    - We will put all our local rules in `include $RULE_PATH/local.rules`
    - To enable alert log; comment out (adding `#` before the line) the following line (Step 6 in the

configuration file):

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

- Save and quit from `snort.conf` file `:wq`
- Start SNORT:

```
sudo systemctl start snort
```

or

```
sudo /etc/init.d/snort start
```

- Check whether SNORT is running:

```
sudo systemctl status snort
```

or

```
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.

- Here is a good reference to learn about writing snort rules:

```
http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node28.html
```

The First Bad Rule

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

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

alert ip any any -> any any (msg: "IP Packet detected"; sid: 1000001;)
```

- Save and exit. Restart `snort` service

```
sudo systemctl restart snort
```

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

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

- **REMOVE** (or comment out) the bad rule from `local.rules` once you have seen the alert!

SNORT Exercise

Excercise 1 : Write a rule to check XMAS scan on your server from external network
Exercise 2 : Write a rule to check any external network access your webserver /admin pages
Exercise 3 : Write a rule to check SSH brute force attack and log IP trying to connect more than 3 times in 60 seconds (the threshold option may be deprecated*)

```
***END OF EXERCISE***
```