

Snort Installation on Kali linux:

Snort is an open source IDS/IPS system freely available for public use.

To know what an IDS/IPS system is, refer to the link to our youtube video:

[What is an IDS/IPS system?](#)

Open the terminal and type:

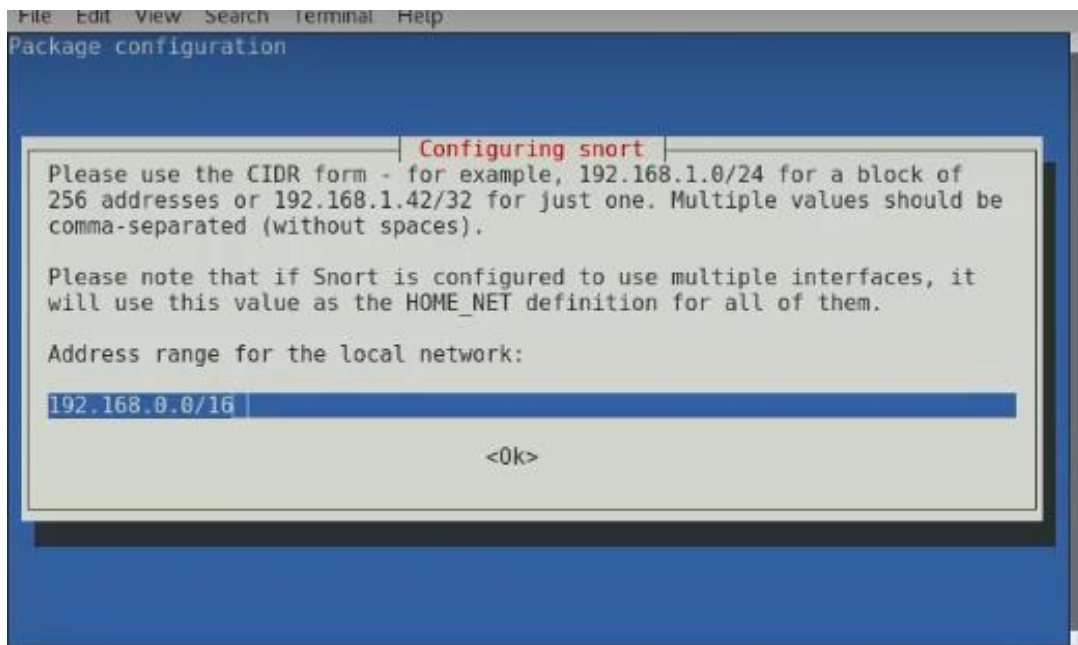
- apt-get update

This will download list of packages and will get newest versions of packages and their dependencies.

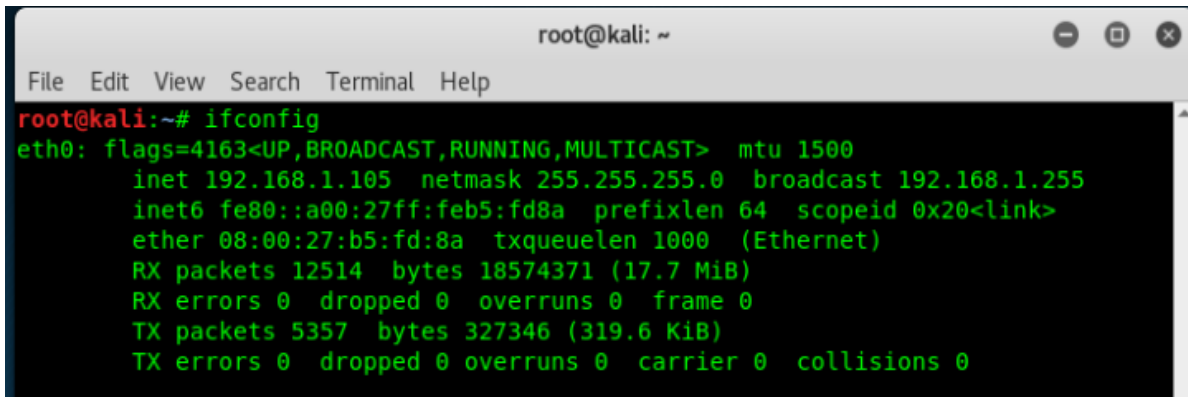
- apt-get install snort

This will start Snort download and installation on your machine.

➤ You will be prompted to enter your local network range:



You can check for yours by doing **ifconfig** and looking at your IP address:

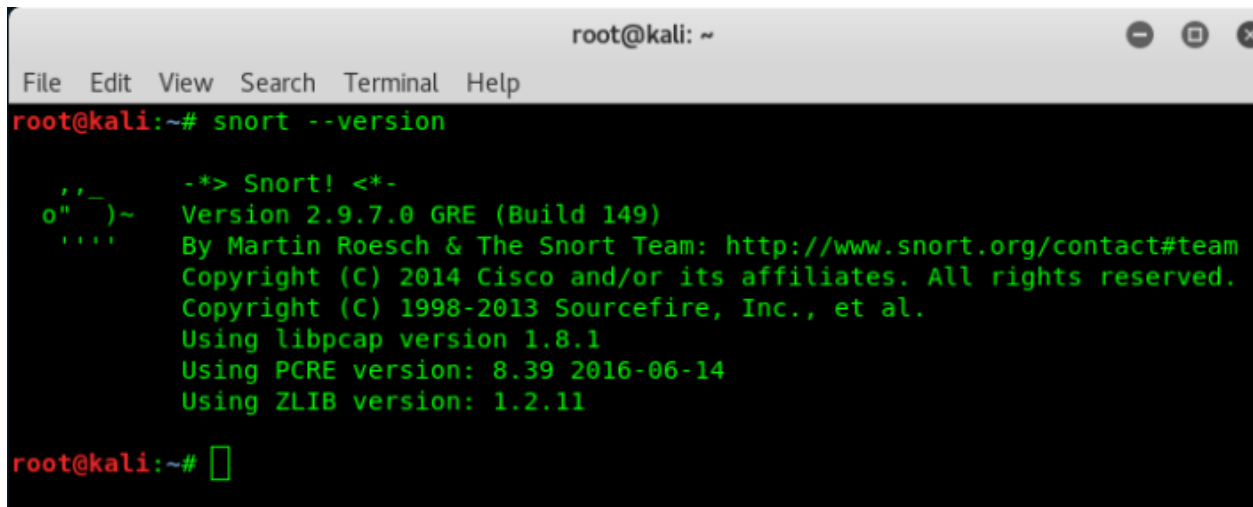
A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'ifconfig' has been executed, showing details for the 'eth0' interface. The output includes flags, MTU, IP address (192.168.1.105), netmask (255.255.255.0), broadcast address (192.168.1.255), MAC address (08:00:27:b5:fd:8a), and statistics for RX and TX packets, errors, and collisions.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feb5:fd8a  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b5:fd:8a  txqueuelen 1000  (Ethernet)
    RX packets 12514  bytes 18574371 (17.7 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 5357  bytes 327346 (319.6 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

After entering your network range press enter.

- `snort --version`

You can run the above command to see if the installation was successful and the version information.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'snort --version' has been executed, displaying the Snort version (2.9.7.0 GRE Build 149) and various dependencies like libpcap, PCRE, and ZLIB.

```
root@kali:~# 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 1.8.1
        Using PCRE version: 8.39 2016-06-14
        Using ZLIB version: 1.2.11

root@kali:~#
```

Done!