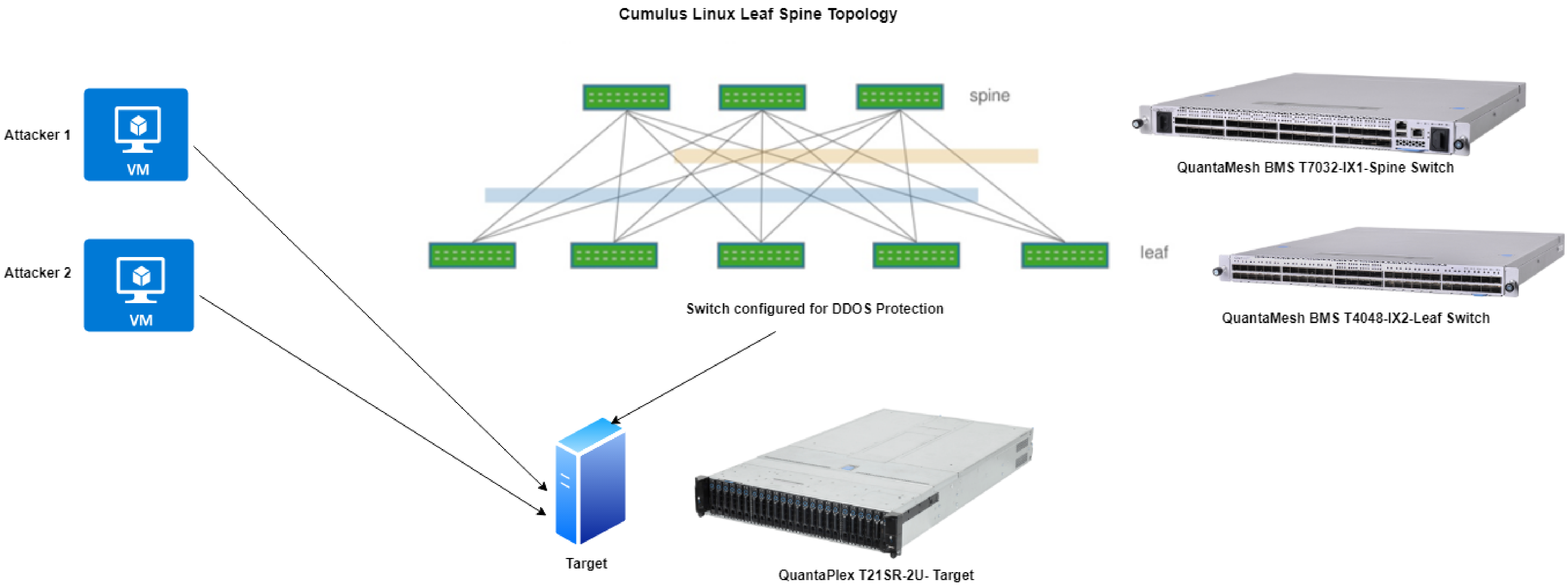
# DDOS mitigation with Cumulus Linux

A **distributed denial-of-service** (**DDoS**) is a large-scale DoS attack where the perpetrator uses more than one unique IP address, often thousands of them.[10] A distributed denial of service attack typically involves more than around 3–5 nodes on different networks; fewer nodes may qualify as a DoS attack but is not a DDoS attack.[11][12] Since the incoming traffic flooding the victim originates from different sources, it may be impossible to stop the attack simply by using ingress filtering. It also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin. As an alternative or augmentation of a DDoS, attacks may involve forging of IP sender addresses (IP address spoofing) further complicating identifying and defeating the attack.

**Date:**
**Created by:** Greg Androniko

This page was intentionally left blank.

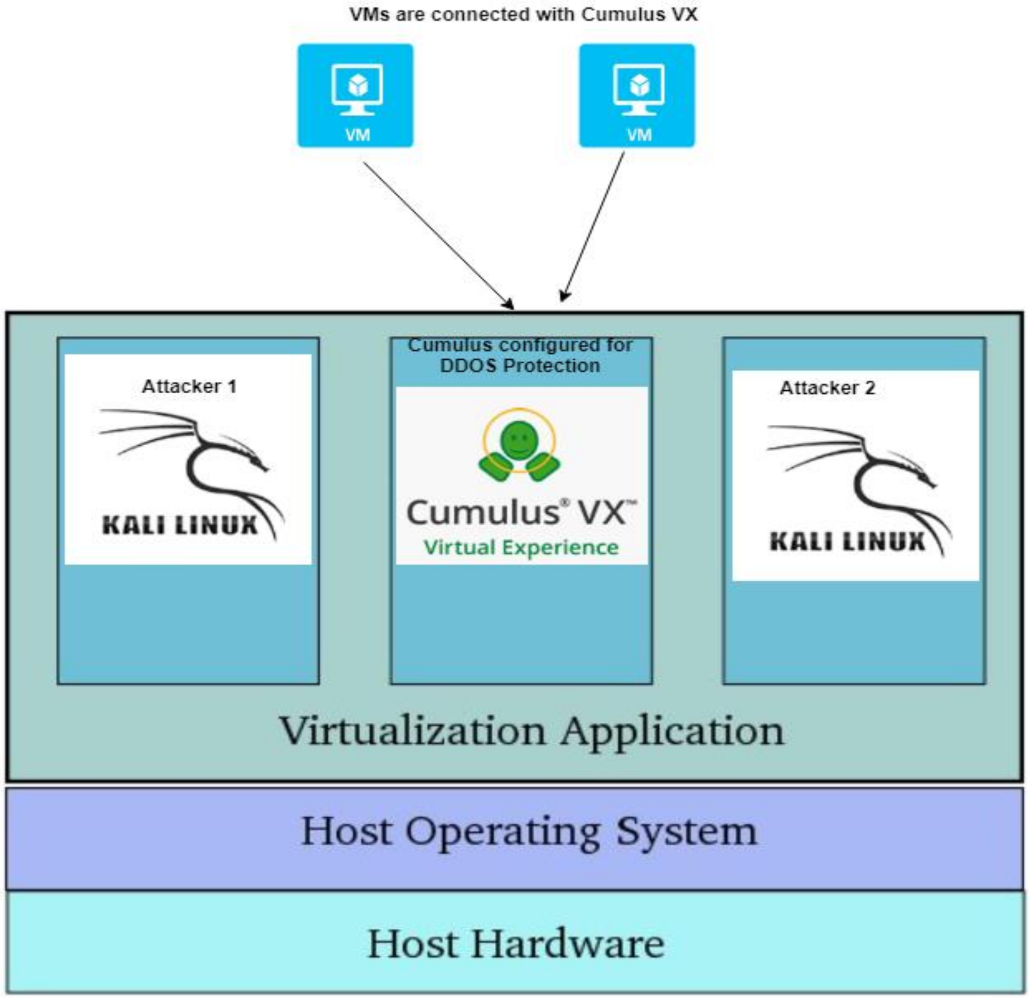
# 1- DDOS Protection with Cumulus Linux

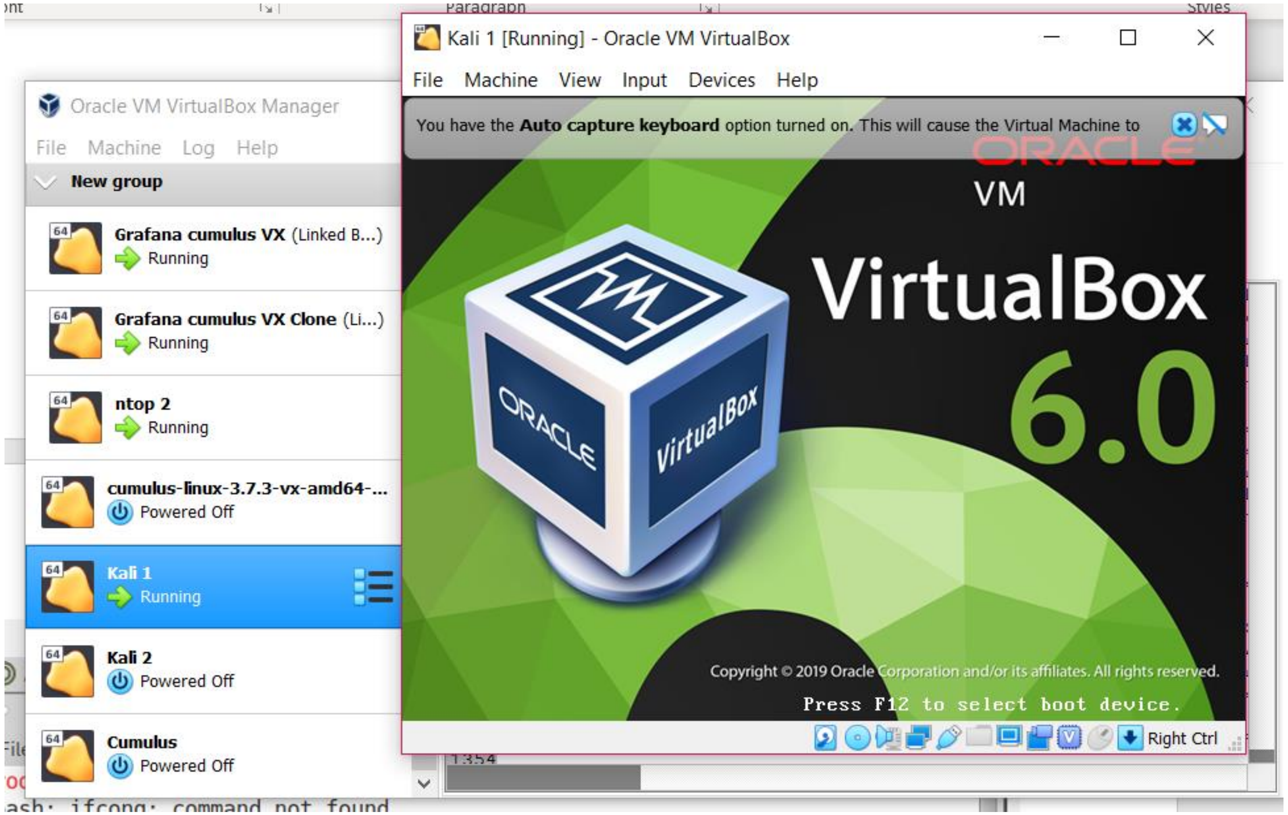


Cumulus Linux Leaf Spine Topology

Attacker 1
VM
Attacker 2
VM
spine
leaf
QuantaMesh BMS T7032-IX1-Spine Switch
QuantaMesh BMS T4048-IX2-Leaf Switch
Switch configured for DDOS Protection
Target
QuantaPlex T21SR-2U- Target

## 2- Test Environment Setup





Kali 1 [Running] - Oracle VM VirtualBox

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to

Oracle VM VirtualBox Manager

New group

Grafana cumulus VX (Linked B...) Running

Grafana cumulus VX Clone (Li...) Running

ntop 2 Running

cumulus-linux-3.7.3-vx-amd64-... Powered Off

Kali 1 Running

Kali 2 Powered Off

Cumulus Powered Off

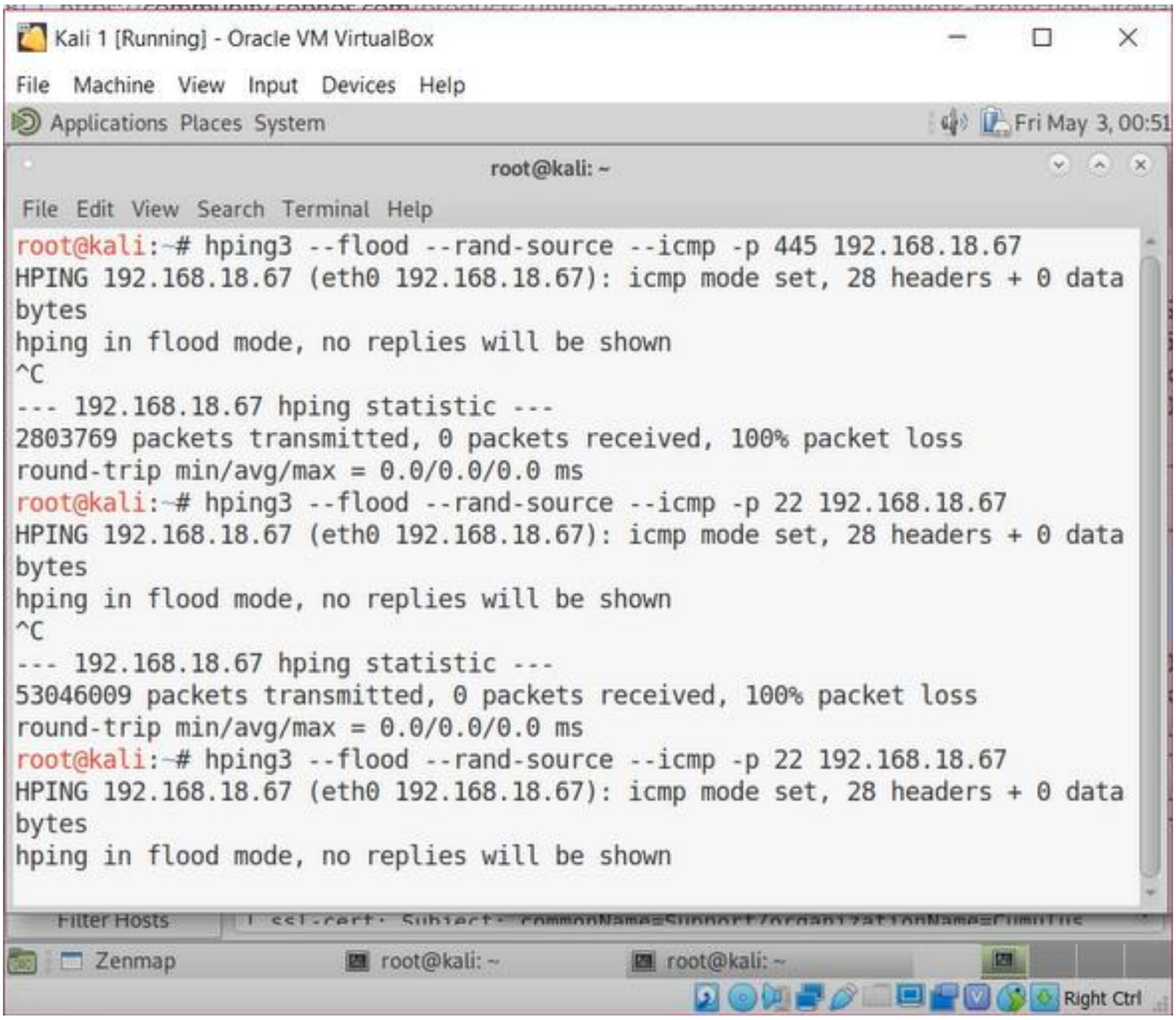
Copyright © 2019 Oracle Corporation and/or its affiliates. All rights reserved.

```
Press F12 to select boot device.
```

```
ash: ifconfig: command not found
```

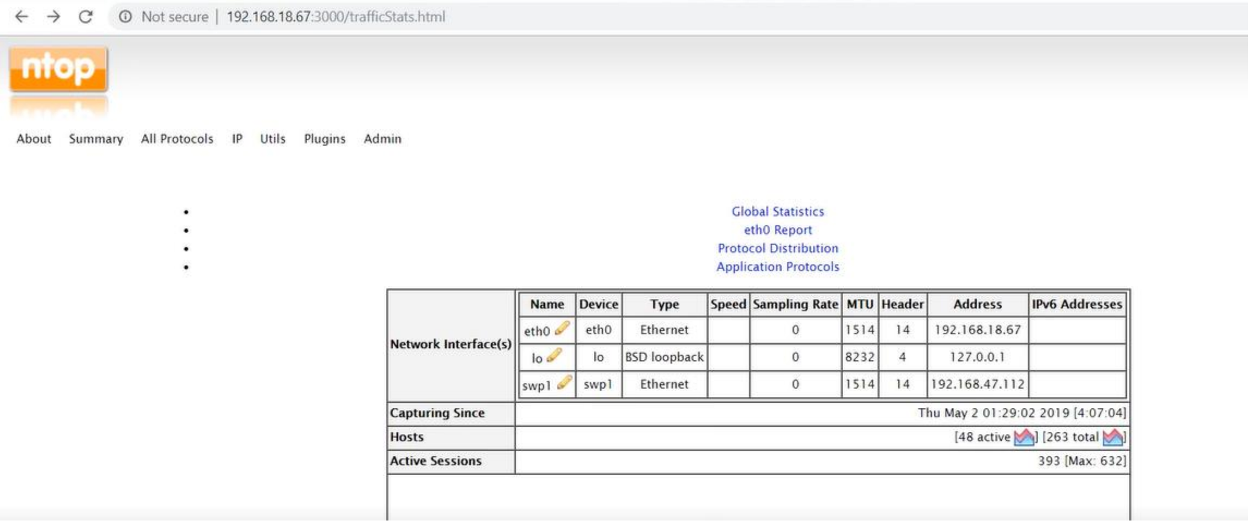
## 3- DDOS Simulation

1- Open Kali Linux and open terminal, write following command to start DDOS


Kali 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Fri May 3, 00:51
root@kali: ~
File Edit View Search Terminal Help
Filter Hosts
Zenmap
root@kali: ~
root@kali: ~
Right Ctrl

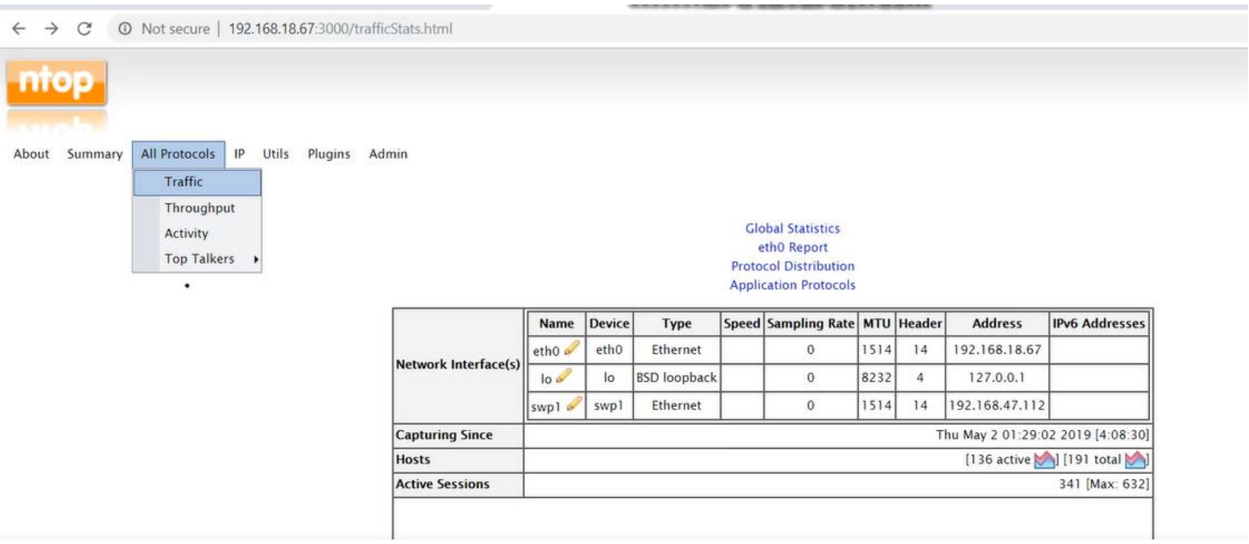
```
root@kali:~# hping3 --flood --rand-source --icmp -p 445 192.168.18.67
HPING 192.168.18.67 (eth0 192.168.18.67): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.67 hping statistic ---
2803769 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~# hping3 --flood --rand-source --icmp -p 22 192.168.18.67
HPING 192.168.18.67 (eth0 192.168.18.67): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.18.67 hping statistic ---
53046009 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~# hping3 --flood --rand-source --icmp -p 22 192.168.18.67
HPING 192.168.18.67 (eth0 192.168.18.67): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
```

2- On Ntop note active connections before DDOS Attack



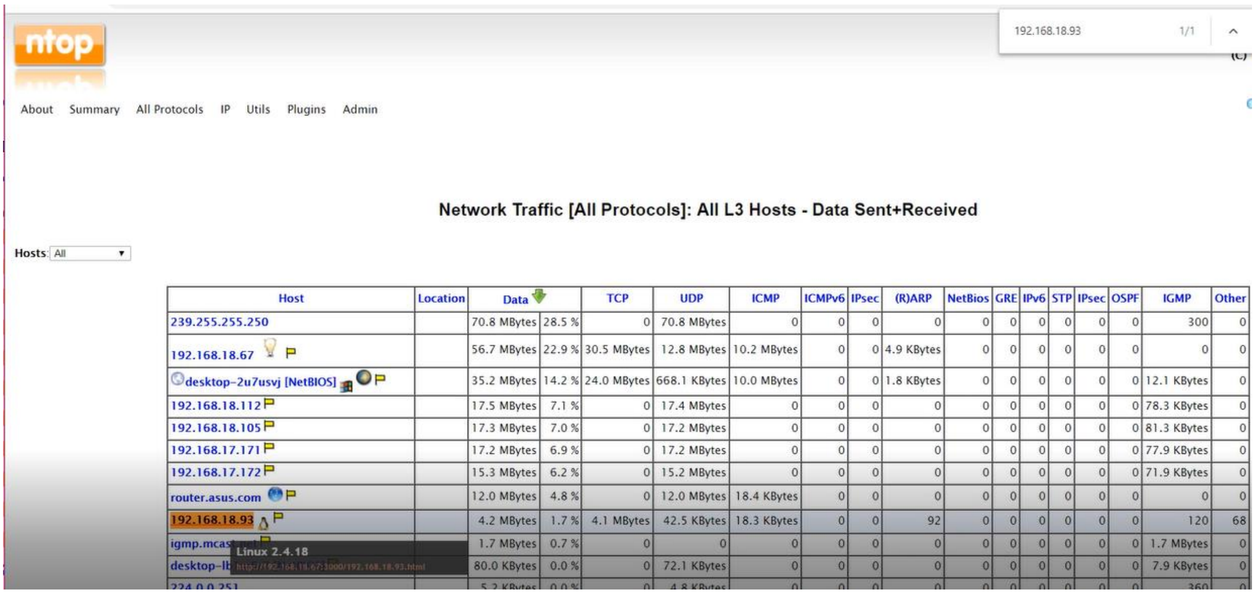
| | Name | Device | Type | Speed | Sampling Rate | MTU | Header | Address | IPv6 Addresses |
|---|---|---|---|---|---|---|---|---|---|
| Network Interface(s) | eth0 | eth0 | Ethernet | | 0 | 1514 | 14 | 192.168.18.67 | |
| | lo | lo | BSD loopback | | 0 | 8232 | 4 | 127.0.0.1 | |
| | swp1 | swp1 | Ethernet | | 0 | 1514 | 14 | 192.168.47.112 | |
| Capturing Since | Thu May 2 01:29:02 2019 [4:07:04] | | | | | | | | |
| Hosts | [48 active] [263 total] | | | | | | | | |
| Active Sessions | 393 [Max: 632] | | | | | | | | |

3- On Ntop note active connections after DDOS Attack



Global Statistics
eth0 Report
Protocol Distribution
Application Protocols

| | Name | Device | Type | Speed | Sampling Rate | MTU | Header | Address | IPv6 Addresses |
|---|---|---|---|---|---|---|---|---|---|
| Network Interface(s) | eth0 | eth0 | Ethernet | | 0 | 1514 | 14 | 192.168.18.67 | |
| | lo | lo | BSD loopback | | 0 | 8232 | 4 | 127.0.0.1 | |
| | swp1 | swp1 | Ethernet | | 0 | 1514 | 14 | 192.168.47.112 | |
| Capturing Since | Thu May 2 01:29:02 2019 [4:08:30] | | | | | | | | |
| Hosts | [136 active ] [191 total ] | | | | | | | | |
| Active Sessions | 341 [Max: 632] | | | | | | | | |



Network Traffic [All Protocols]: All L3 Hosts - Data Sent+Received

| Host | Location | Data | | TCP | UDP | ICMP | ICMPv6 | IPsec | (R)ARP | NetBios | GRE | IPv6 | STP | IPsec | OSPF | IGMP | Other |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 239.255.255.250 | | 70.8 MBytes | 28.5 % | 0 | 70.8 MBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 300 | 0 |
| 192.168.18.67 | | 56.7 MBytes | 22.9 % | 30.5 MBytes | 12.8 MBytes | 10.2 MBytes | 0 | 0 | 4.9 KBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| desktop-2u7usvj [NetBIOS] | | 35.2 MBytes | 14.2 % | 24.0 MBytes | 668.1 KBytes | 10.0 MBytes | 0 | 0 | 1.8 KBytes | 0 | 0 | 0 | 0 | 0 | 0 | 12.1 KBytes | 0 |
| 192.168.18.112 | | 17.5 MBytes | 7.1 % | 0 | 17.4 MBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 78.3 KBytes | 0 |
| 192.168.18.105 | | 17.3 MBytes | 7.0 % | 0 | 17.2 MBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 81.3 KBytes | 0 |
| 192.168.17.171 | | 17.2 MBytes | 6.9 % | 0 | 17.2 MBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 77.9 KBytes | 0 |
| 192.168.17.172 | | 15.3 MBytes | 6.2 % | 0 | 15.2 MBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 71.9 KBytes | 0 |
| router.asus.com | | 12.0 MBytes | 4.8 % | 0 | 12.0 MBytes | 18.4 KBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 192.168.18.93 | | 4.2 MBytes | 1.7 % | 4.1 MBytes | 42.5 KBytes | 18.3 KBytes | 0 | 0 | 92 | 0 | 0 | 0 | 0 | 0 | 0 | 120 | 68 |
| igmp.mcast | | 1.7 MBytes | 0.7 % | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.7 MBytes | 0 |
| desktop-lb | | 80.0 KBytes | 0.0 % | 0 | 72.1 KBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 7.9 KBytes | 0 |
| 224.0.0.251 | | 5.2 KBytes | 0.0 % | 0 | 4.8 KBytes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 360 | 0 |

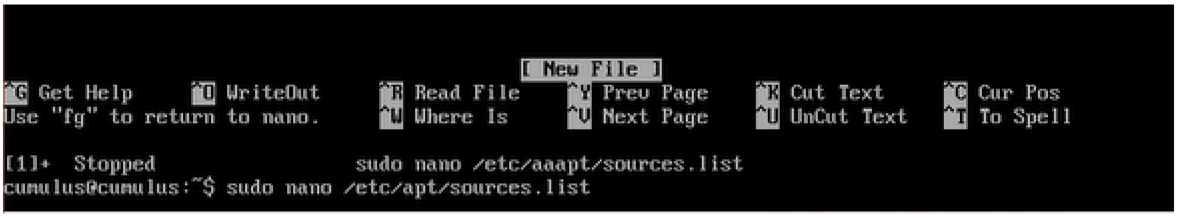
Linux 2.4.18
http://192.168.18.67:3000/192.168.18.93.html

## 4.0- Monitoring System Installation

We have installed Ntop, tshark, traffic monitoring on Cumulus

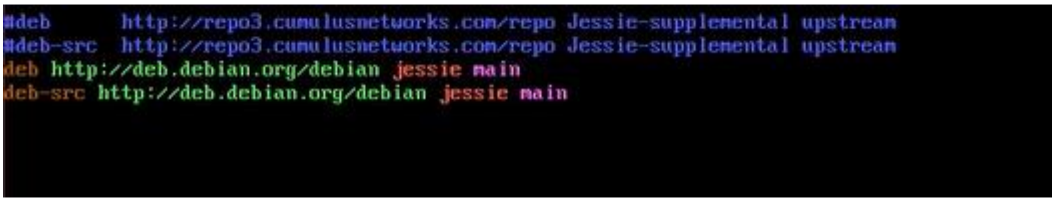
### 4.1- Ntop installation on Cumulus VX

1- Open Cumulus VX and login as a cumulus user and use password CumulusLinux!
open file /etc/apt/sources.list



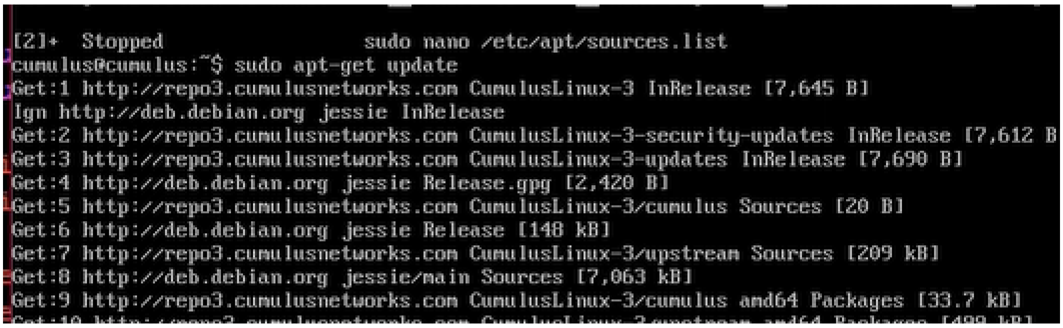
```
                                    [ New File ]
^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
Use "fg" to return to nano.     ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell

[1]+  Stopped                 sudo nano /etc/aaapt/sources.list
cumulus@cumulus:~$ sudo nano /etc/apt/sources.list
```

2- Add deb http://deb.debian.org/debian jessie main
deb-src http://deb.debian.org/debian jessie main
save file



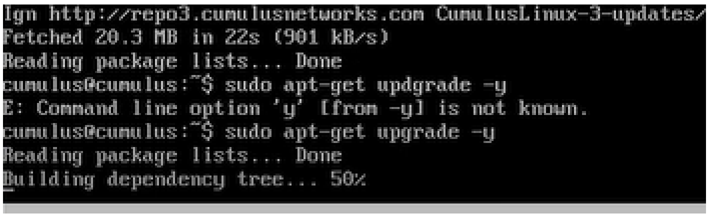
```
#deb      http://repo3.cumulusnetworks.com/repo Jessie-supplemental upstream
#deb-src  http://repo3.cumulusnetworks.com/repo Jessie-supplemental upstream
deb http://deb.debian.org/debian jessie main
deb-src http://deb.debian.org/debian jessie main
```

3- User sudo apt-get update to update



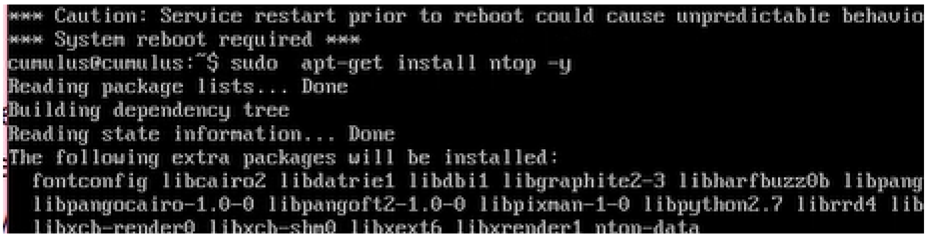
```
[2]+  Stopped                 sudo nano /etc/apt/sources.list
cumulus@cumulus:~$ sudo apt-get update
Get:1 http://repo3.cumulusnetworks.com CumulusLinux-3 InRelease [7,645 B]
Ign http://deb.debian.org jessie InRelease
Get:2 http://repo3.cumulusnetworks.com CumulusLinux-3-security-updates InRelease [7,612 B
Get:3 http://repo3.cumulusnetworks.com CumulusLinux-3-updates InRelease [7,690 B]
Get:4 http://deb.debian.org jessie Release.gpg [2,420 B]
Get:5 http://repo3.cumulusnetworks.com CumulusLinux-3/cumulus Sources [20 B]
Get:6 http://deb.debian.org jessie Release [148 kB]
Get:7 http://repo3.cumulusnetworks.com CumulusLinux-3/upstream Sources [209 kB]
Get:8 http://deb.debian.org jessie/main Sources [7,063 kB]
Get:9 http://repo3.cumulusnetworks.com CumulusLinux-3/cumulus amd64 Packages [33.7 kB]
Get:10 http://repo3.cumulusnetworks.com CumulusLinux-3/upstream amd64 Packages [499 kB]
```

4- User sudo apt-get upgrade -y for upgrade



```
Ign http://repo3.cumulusnetworks.com CumulusLinux-3-updates/
Fetched 20.3 MB in 22s (901 kB/s)
Reading package lists... Done
cumulus@cumulus:~$ sudo apt-get updgrade -y
E: Command line option 'y' [from -y] is not known.
cumulus@cumulus:~$ sudo apt-get upgrade -y
Reading package lists... Done
Building dependency tree... 50%
```

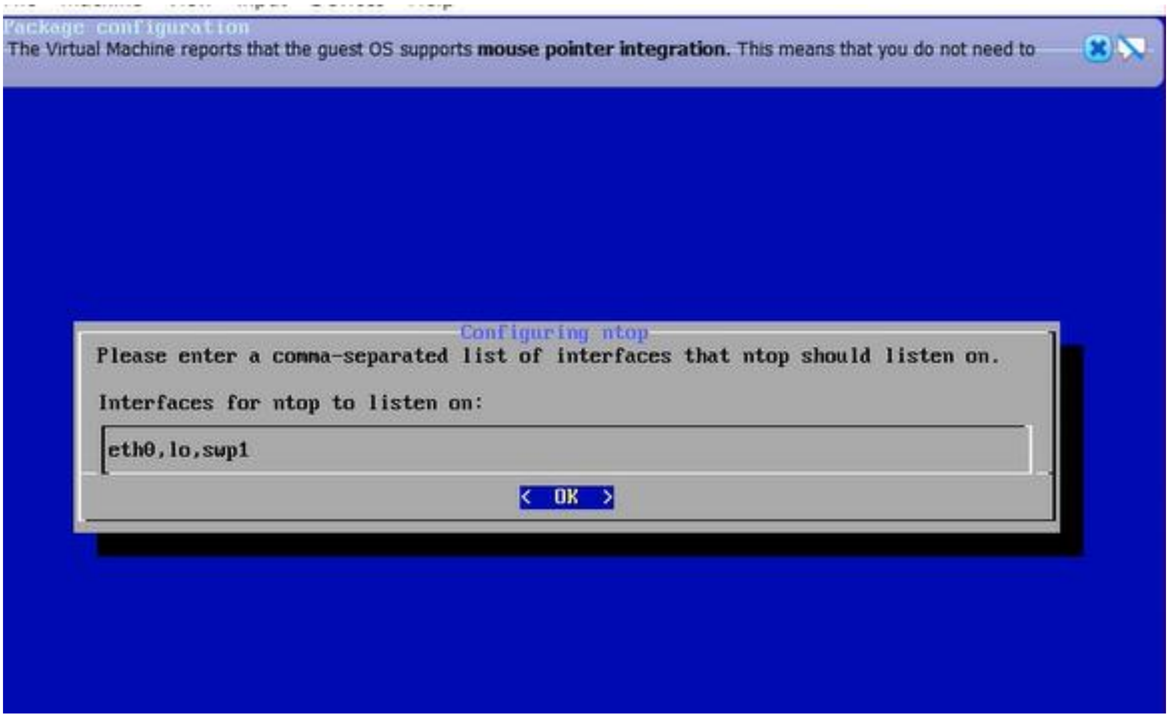
5- Type sudo apt-get install ntop -y to install ntop



```
*** Caution: Service restart prior to reboot could cause unpredictable behavio
*** System reboot required ***
cumulus@cumulus:~$ sudo  apt-get install ntop -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  fontconfig libcairo2 libdatrie1 libdbi1 libgraphite2-3 libharfbuzz0b libpang
  libpangocairo-1.0-0 libpangoft2-1.0-0 libpixman-1-0 libpython2.7 librrd4 lib
  libxcb-render0 libxcb-shm0 libxext6 libxrender1 ntop-data
```

6- You will be prompted for a list of interfaces that ntop will listen on. Enter each interface that you want to monitor separated by a comma if more than one interface is needed. For this example, I will just use the first interface eth0 (the first interface on your machine may be different, you can check this with the ifconfig command).

Type in interfaces which you want monitor

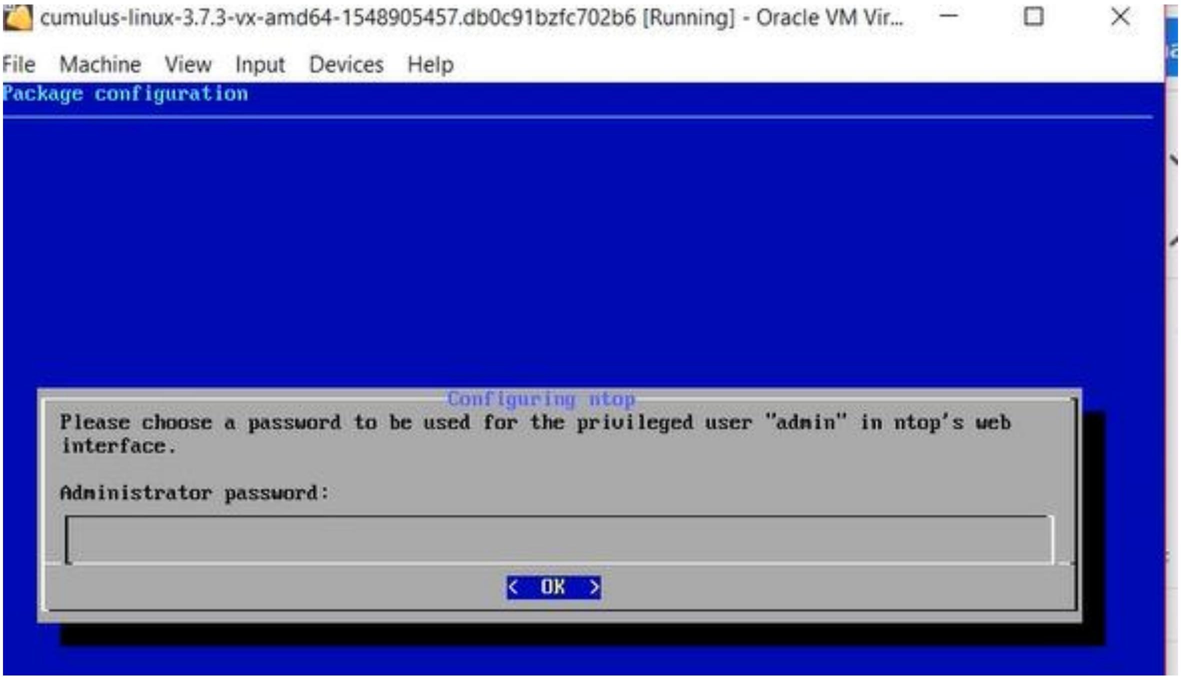


Package configuration

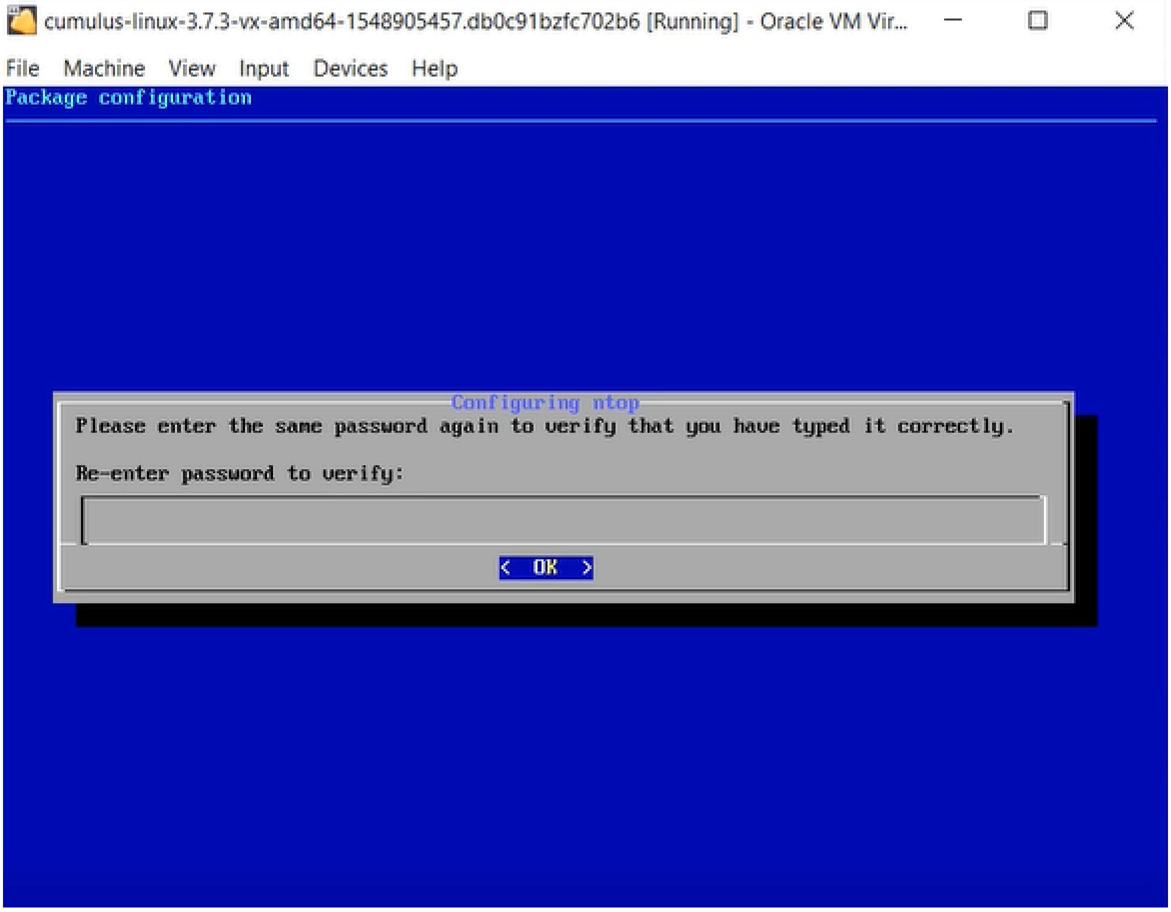
The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to

```
Configuring ntop
Please enter a comma-separated list of interfaces that ntop should listen on.

Interfaces for ntop to listen on:

eth0,lo,swp1

<  OK  >
```

7- You will then be prompted for an administrator's password. Type in a password and press enter to continue. You will need to confirm this password immediately after.

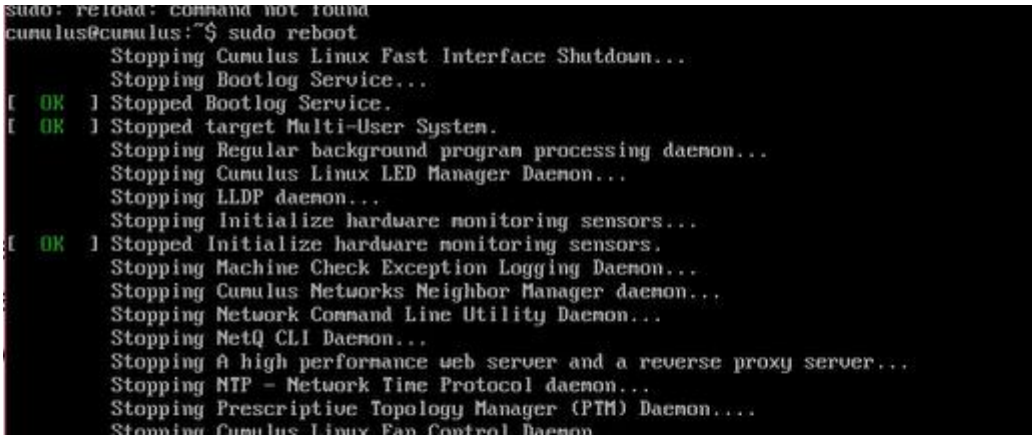

cumulus-linux-3.7.3-vx-amd64-1548905457.db0c91bzfc702b6 [Running] - Oracle VM Vir...
File Machine View Input Devices Help
< OK >

```
Package configuration

Configuring ntop
Please choose a password to be used for the privileged user "admin" in ntop's web
interface.

Administrator password:
```


cumulus-linux-3.7.3-vx-amd64-1548905457.db0c91bzfc702b6 [Running] - Oracle VM Vir...
File Machine View Input Devices Help
< OK >

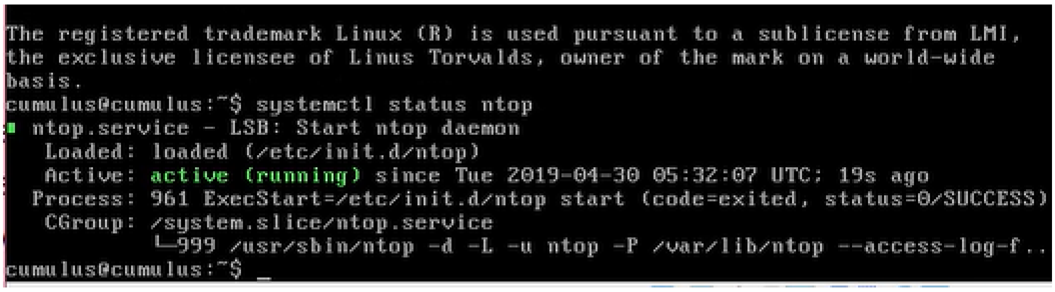
```
Package configuration

Configuring ntop
Please enter the same password again to verify that you have typed it correctly.

Re-enter password to verify:
```

8- Type sudo reboot and press enter to reboot system



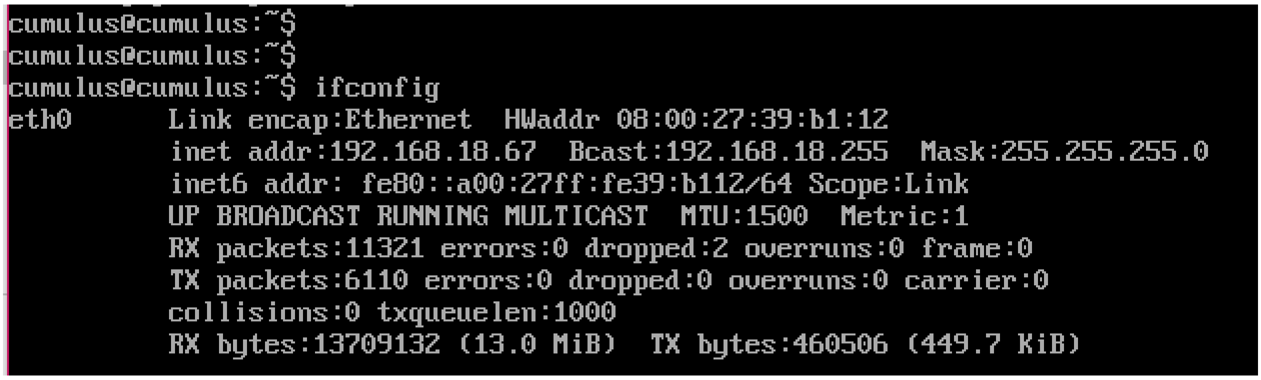
```
sudo: reload: command not found
cumulus@cumulus:~$ sudo reboot
             Stopping Cumulus Linux Fast Interface Shutdown...
             Stopping Bootlog Service...
[  OK  ] Stopped Bootlog Service.
[  OK  ] Stopped target Multi-User System.
             Stopping Regular background program processing daemon...
             Stopping Cumulus Linux LED Manager Daemon...
             Stopping LLDP daemon...
             Stopping Initialize hardware monitoring sensors...
[  OK  ] Stopped Initialize hardware monitoring sensors.
             Stopping Machine Check Exception Logging Daemon...
             Stopping Cumulus Networks Neighbor Manager daemon...
             Stopping Network Command Line Utility Daemon...
             Stopping NetQ CLI Daemon...
             Stopping A high performance web server and a reverse proxy server...
             Stopping NTP - Network Time Protocol daemon...
             Stopping Prescriptive Topology Manager (PTM) Daemon....
             Stopping Cumulus Linux Fan Control Daemon
```

9- To confirm ntop is running as expected. Use systemctl status ntop command



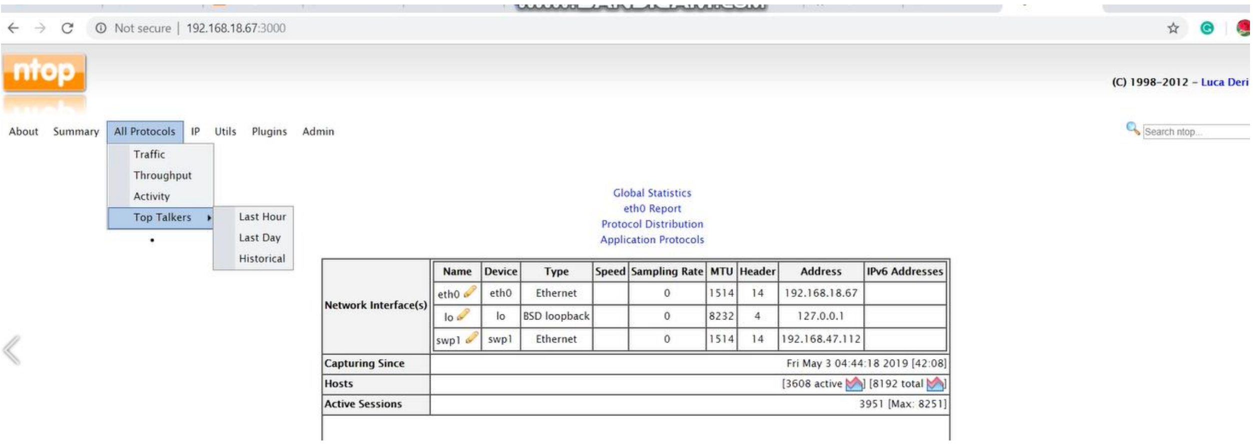
```
The registered trademark Linux (R) is used pursuant to a sublicense from LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide
basis.
cumulus@cumulus:~$ systemctl status ntop
● ntop.service - LSB: Start ntop daemon
   Loaded: loaded (/etc/init.d/ntop)
   Active: active (running) since Tue 2019-04-30 05:32:07 UTC; 19s ago
  Process: 961 ExecStart=/etc/init.d/ntop start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/ntop.service
           └─999 /usr/sbin/ntop -d -L -u ntop -P /var/lib/ntop --access-log-f..
cumulus@cumulus:~$ _
```

10- To access the ntop web interface, you will first need to find the IP address of the Cumulus Linux virtual machine. To find the IP address, use ifconfig command



```
cumulus@cumulus:~$
cumulus@cumulus:~$
cumulus@cumulus:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:b1:12
          inet addr:192.168.18.67  Bcast:192.168.18.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:b112/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11321 errors:0 dropped:2 overruns:0 frame:0
          TX packets:6110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13709132 (13.0 MiB)  TX bytes:460506 (449.7 KiB)
```

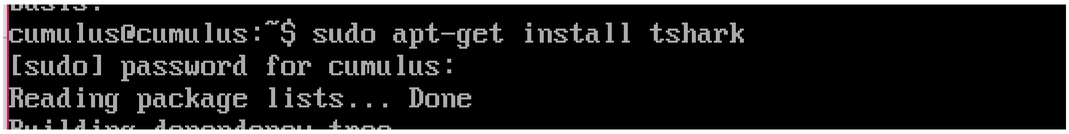
11- Type http://<IP Address>:3000/ in webrowser
Replace IP address by your Eth0 Ip address



| | Name | Device | Type | Speed | Sampling Rate | MTU | Header | Address | IPv6 Addresses |
|---|---|---|---|---|---|---|---|---|---|
| Network Interface(s) | eth0 | eth0 | Ethernet | | 0 | 1514 | 14 | 192.168.18.67 | |
| | lo | lo | BSD loopback | | 0 | 8232 | 4 | 127.0.0.1 | |
| | swp1 | swp1 | Ethernet | | 0 | 1514 | 14 | 192.168.47.112 | |
| Capturing Since | Fri May 3 04:44:18 2019 [42:08] | | | | | | | | |
| Hosts | [3608 active ] [8192 total ] | | | | | | | | |
| Active Sessions | 3951 [Max: 8251] | | | | | | | | |

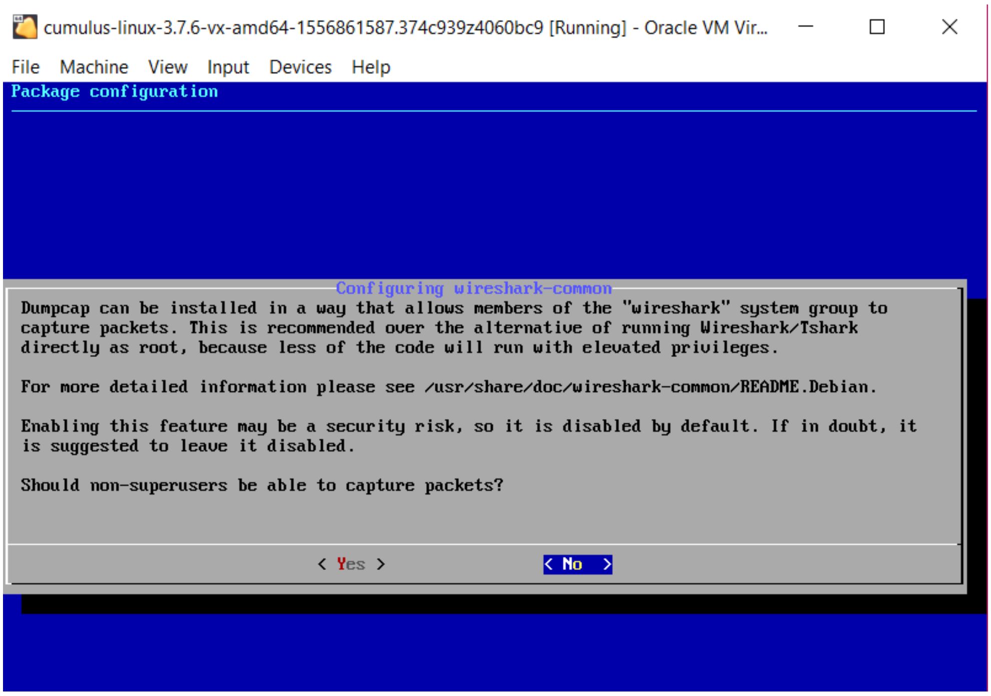
## 4.2 Tshark Installation (This is low level monitoring system)

1- Type sudo apt-get install tshark



```
cumulus@cumulus:~$ sudo apt-get install tshark
[sudo] password for cumulus:
Reading package lists... Done
```

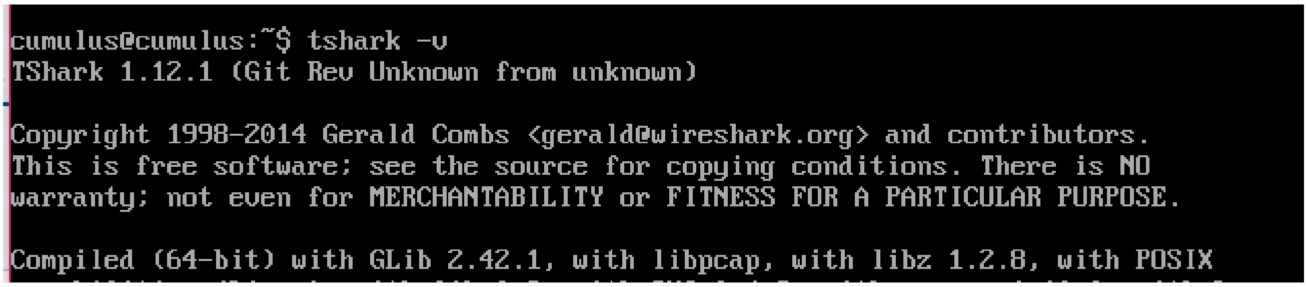
2- You will be prompted with screen, here you can define who can capture traffic



cumulus-linux-3.7.6-vx-amd64-1556861587.374c939z4060bc9 [Running] - Oracle VM Vir...
File
Machine
View
Input
Devices
Help

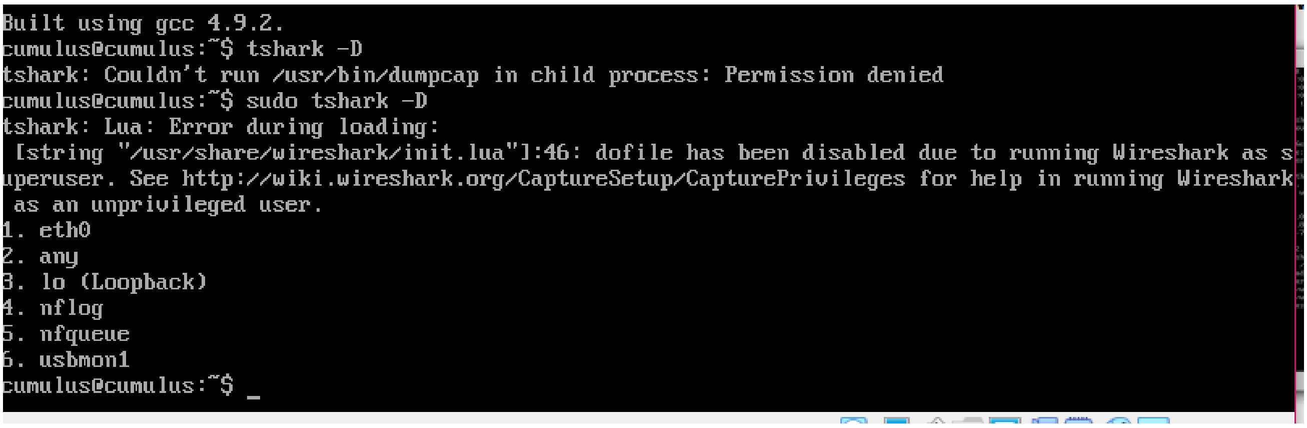
```
Package configuration

                     Configuring wireshark-common
 Dumpcap can be installed in a way that allows members of the "wireshark" system group to
 capture packets. This is recommended over the alternative of running Wireshark/Tshark
 directly as root, because less of the code will run with elevated privileges.

 For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.

 Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it
 is suggested to leave it disabled.

 Should non-superusers be able to capture packets?

                         < Yes >                    < No >
```

3- Verify version of tshark



```
cumulus@cumulus:~$ tshark -v
TShark 1.12.1 (Git Rev Unknown from unknown)

Copyright 1998-2014 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with GLib 2.42.1, with libpcap, with libz 1.2.8, with POSIX
```

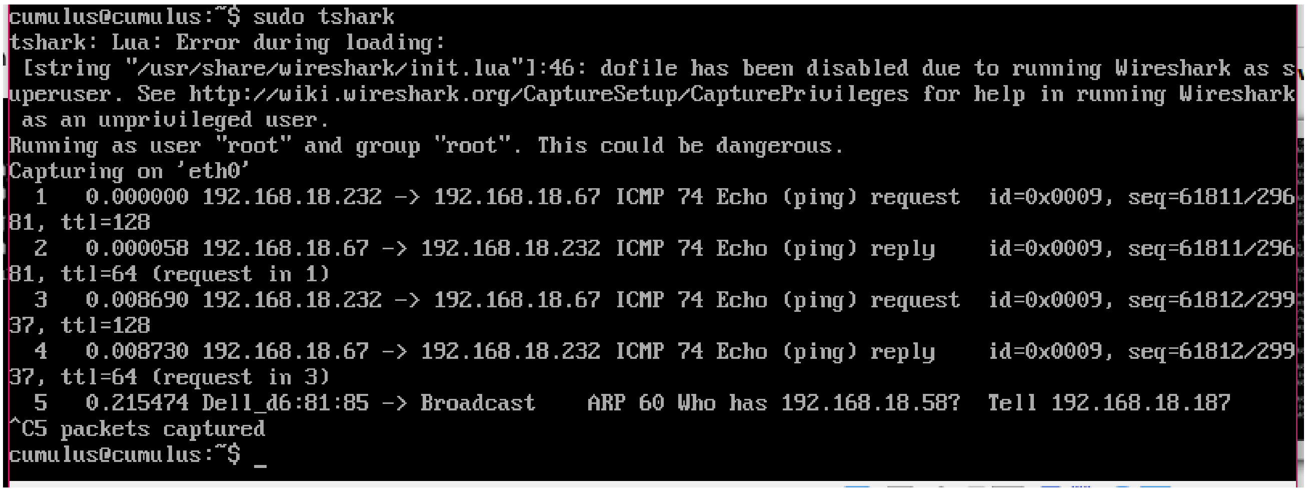
4- Use sudo tshark -D to get a list of the available network interfaces



```
Built using gcc 4.9.2.
cumulus@cumulus:~$ tshark -D
tshark: Couldn't run /usr/bin/dumpcap in child process: Permission denied
cumulus@cumulus:~$ sudo tshark -D
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as s
uperuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark
 as an unprivileged user.
1. eth0
2. any
3. lo (Loopback)
4. nflog
5. nfqueue
6. usbmon1
cumulus@cumulus:~$ _
```

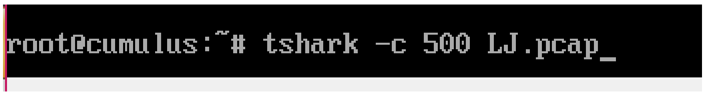
5- The simplest way of capturing data is by running tshark without any parameters, which will display all data on screen. You can stop data capturing by pressing Ctrl-C.

The output will scroll very fast on a busy network, so it won't be helpful at all.

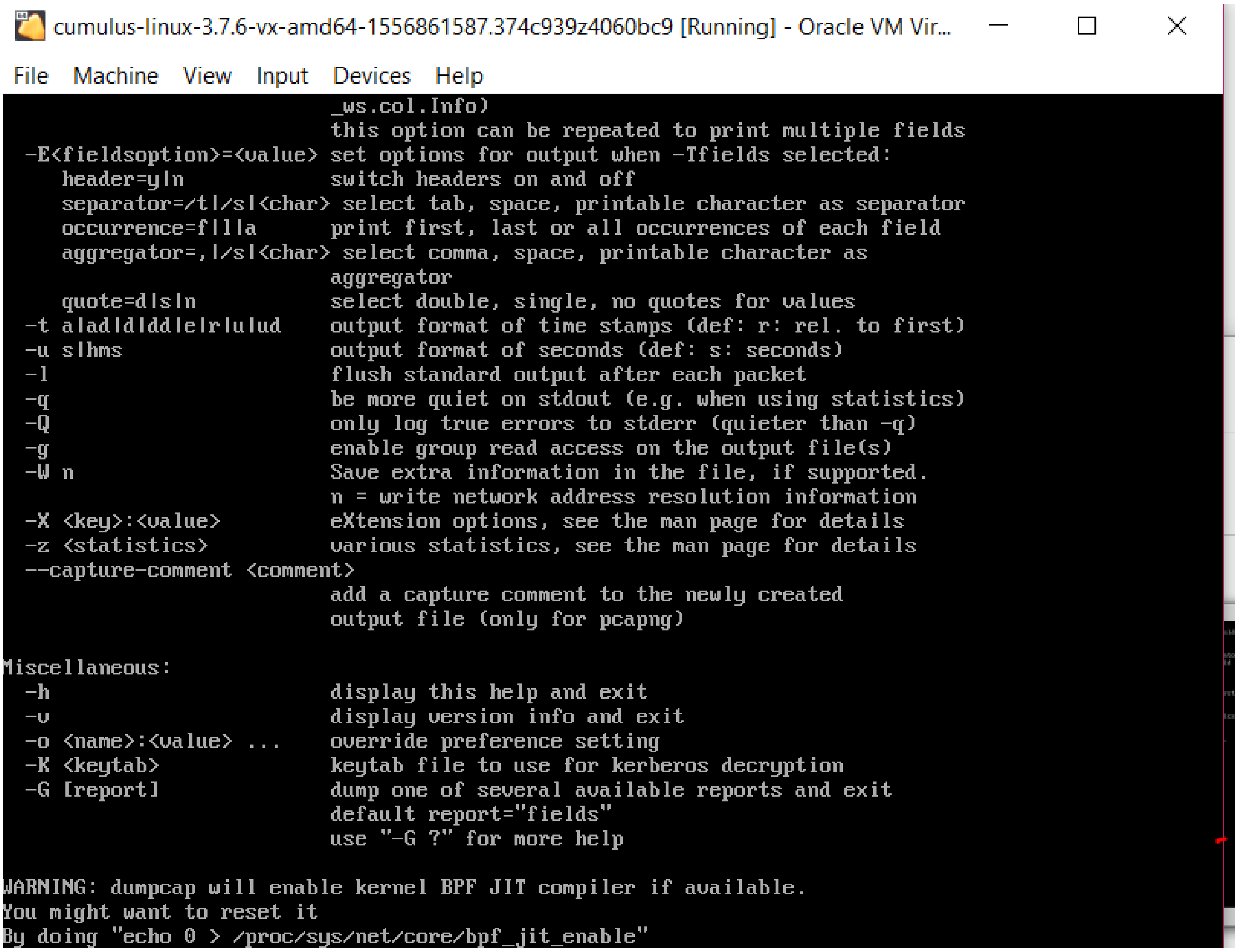


```
cumulus@cumulus:~$ sudo tshark
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as s
uperuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark
 as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
  1   0.000000 192.168.18.232 -> 192.168.18.67 ICMP 74 Echo (ping) request  id=0x0009, seq=61811/296
81, ttl=128
  2   0.000058 192.168.18.67 -> 192.168.18.232 ICMP 74 Echo (ping) reply    id=0x0009, seq=61811/296
81, ttl=64 (request in 1)
  3   0.008690 192.168.18.232 -> 192.168.18.67 ICMP 74 Echo (ping) request  id=0x0009, seq=61812/299
37, ttl=128
  4   0.008730 192.168.18.67 -> 192.168.18.232 ICMP 74 Echo (ping) reply    id=0x0009, seq=61812/299
37, ttl=64 (request in 3)
  5   0.215474 Dell_d6:81:85 -> Broadcast    ARP 60 Who has 192.168.18.58?  Tell 192.168.18.187
^C5 packets captured
cumulus@cumulus:~$ _
```

6- As a root user tshark -c 500 -w LJ.pcap command captures 500 network packets (-c 500) and saves them into a file called LJ.pcap (-w LJ.pcap)



```
root@cumulus:~# tshark -c 500 LJ.pcap_
```



cumulus-linux-3.7.6-vx-amd64-1556861587.374c939z4060bc9 [Running] - Oracle VM Vir...
File
Machine
View
Input
Devices
Help

```
                           _ws.col.Info)
                           this option can be repeated to print multiple fields
  -E<fieldsoption>=<value> set options for output when -Tfields selected:
     header=y|n            switch headers on and off
     separator=/t|/s|<char> select tab, space, printable character as separator
     occurrence=f|l|a      print first, last or all occurrences of each field
     aggregator=,|/s|<char> select comma, space, printable character as
                           aggregator
     quote=d|s|n           select double, single, no quotes for values
  -t a|ad|d|dd|e|r|u|ud    output format of time stamps (def: r: rel. to first)
  -u s|hms                 output format of seconds (def: s: seconds)
  -l                       flush standard output after each packet
  -q                       be more quiet on stdout (e.g. when using statistics)
  -Q                       only log true errors to stderr (quieter than -q)
  -g                       enable group read access on the output file(s)
  -W n                     Save extra information in the file, if supported.
                           n = write network address resolution information
  -X <key>:<value>         eXtension options, see the man page for details
  -z <statistics>          various statistics, see the man page for details
  --capture-comment <comment>
                           add a capture comment to the newly created
                           output file (only for pcapng)

Miscellaneous:
  -h                       display this help and exit
  -v                       display version info and exit
  -o <name>:<value> ...    override preference setting
  -K <keytab>              keytab file to use for kerberos decryption
  -G [report]              dump one of several available reports and exit
                           default report="fields"
                           use "-G ?" for more help

WARNING: dumpcap will enable kernel BPF JIT compiler if available.
You might want to reset it
By doing "echo 0 > /proc/sys/net/core/bpf_jit_enable"
```

The second-most useful parameter is -r. When followed by a valid filename, it allows you to read and process a previously captured file with network data

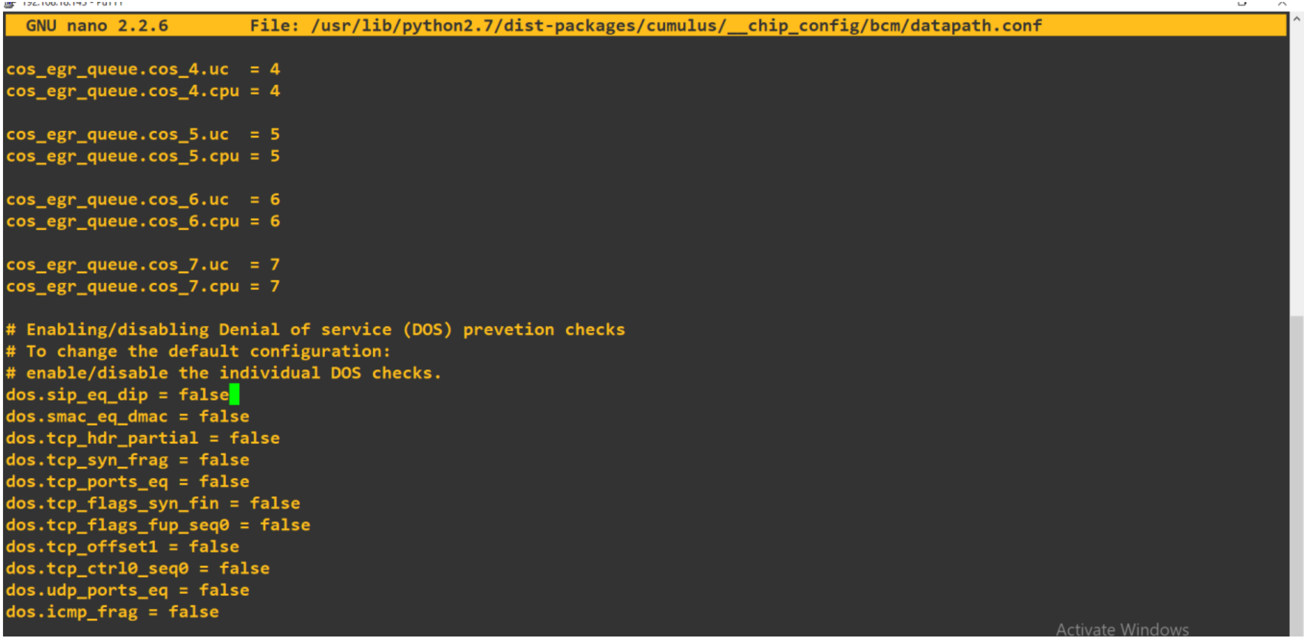
# 5.0- DDOS Mitigation

## 5.1 Hardware-enabled DDOS Protection

1- Open /etc/cumulus/datapath/traffic.conf file in a text editor. Enable DOS prevention checks by changing the following value to true, and save the file

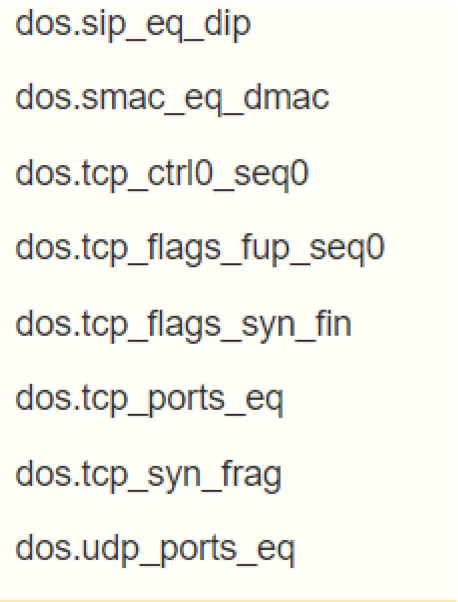
```
# To turn on/off Denial of Service (DOS) prevention checks
dos_enable = true
```

2- Open the /usr/lib/python2.7/dist-packages/cumulus/__chip_config/bcm/datapath.conf file in a text editor and set the following checks to true, and save the file



```
  GNU nano 2.2.6         File: /usr/lib/python2.7/dist-packages/cumulus/__chip_config/bcm/datapath.conf

cos_egr_queue.cos_4.uc  = 4
cos_egr_queue.cos_4.cpu = 4

cos_egr_queue.cos_5.uc  = 5
cos_egr_queue.cos_5.cpu = 5

cos_egr_queue.cos_6.uc  = 6
cos_egr_queue.cos_6.cpu = 6

cos_egr_queue.cos_7.uc  = 7
cos_egr_queue.cos_7.cpu = 7

# Enabling/disabling Denial of service (DOS) prevetion checks
# To change the default configuration:
# enable/disable the individual DOS checks.
dos.sip_eq_dip = false
dos.smac_eq_dmac = false
dos.tcp_hdr_partial = false
dos.tcp_syn_frag = false
dos.tcp_ports_eq = false
dos.tcp_flags_syn_fin = false
dos.tcp_flags_fup_seq0 = false
dos.tcp_offset1 = false
dos.tcp_ctrl0_seq0 = false
dos.udp_ports_eq = false
dos.icmp_frag = false
```

3- Configuring any of the following settings affects the BFD echo function. For example, if you enable dos.udp_ports_eq, all the BFD packets will get dropped because the BFD protocol uses the same source and destination UDP ports.



dos.sip_eq_dip

dos.smac_eq_dmac

dos.tcp_ctrl0_seq0

dos.tcp_flags_fup_seq0

dos.tcp_flags_syn_fin

dos.tcp_ports_eq

dos.tcp_syn_frag

dos.udp_ports_eq

4- Restart Switchd to enable DDOS protection

Sudo systemctl restart switchd.service

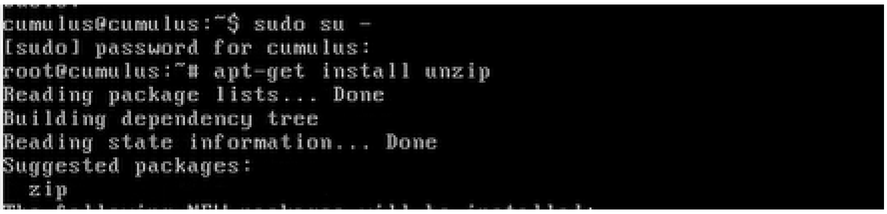
### 5.2 Installation of DDOS-Deflate

(D)DoS Deflate is a lightweight bash shell script designed to assist in the process of blocking a denial of service attack. It utilizes the command below to create a list of IP addresses connected to the server, along with their total number of connections. It is one of the simplest and easiest to install solutions at the software level. IP addresses with over a pre-configured number of connections are automatically blocked in the server's firewall, which can be direct ipfw, iptables, or Advanced Policy Firewall (APF).

1- Installing unzip package .

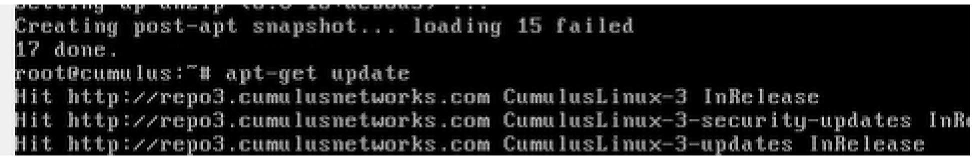
Use su – and enter password CumulusLinux! (or you can log in as a root user)

Use apt-get install unzip and press enter



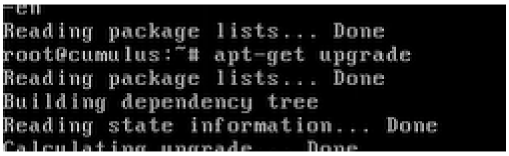
```
cumulus@cumulus:~$ sudo su -
[sudo] password for cumulus:
root@cumulus:~# apt-get install unzip
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  zip
```

2- Use apt-get update command to update



```
Creating post-apt snapshot... loading 15 failed
17 done.
root@cumulus:~# apt-get update
Hit http://repo3.cumulusnetworks.com CumulusLinux-3 InRelease
Hit http://repo3.cumulusnetworks.com CumulusLinux-3-security-updates InR
Hit http://repo3.cumulusnetworks.com CumulusLinux-3-updates InRelease
```

3- Use apt-get upgrade for upgrade

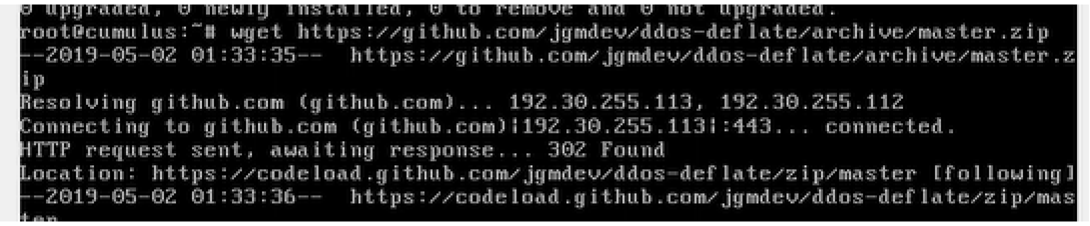


```
Reading package lists... Done
root@cumulus:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

4- As root user execute the following commands:

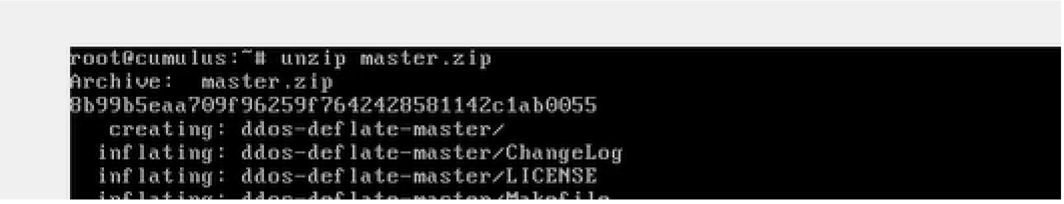
wget https://github.com/jgmdev/ddos-deflate/archive/master.zip
unzip master.zip

cd ddos-deflate-master
./install.sh



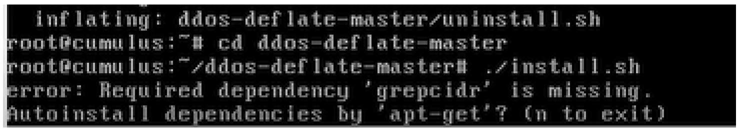
```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@cumulus:~# wget https://github.com/jgmdev/ddos-deflate/archive/master.zip
--2019-05-02 01:33:35--  https://github.com/jgmdev/ddos-deflate/archive/master.z
ip
Resolving github.com (github.com)... 192.30.255.113, 192.30.255.112
Connecting to github.com (github.com)|192.30.255.113|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/jgmdev/ddos-deflate/zip/master [following]
--2019-05-02 01:33:36--  https://codeload.github.com/jgmdev/ddos-deflate/zip/mas
ter
```

Unzipping  master.zip

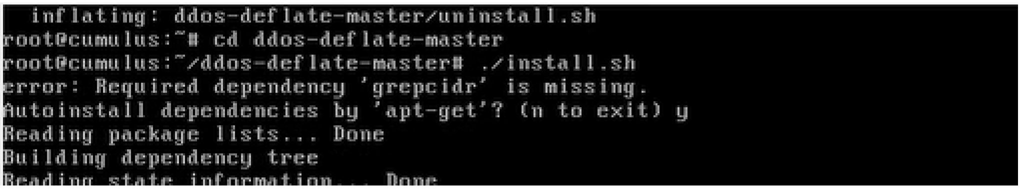


```
root@cumulus:~# unzip master.zip
Archive:  master.zip
8b99b5eaa709f96259f7642428581142c1ab0055
   creating: ddos-deflate-master/
  inflating: ddos-deflate-master/ChangeLog
  inflating: ddos-deflate-master/LICENSE
  inflating: ddos-deflate-master/Makefile
```

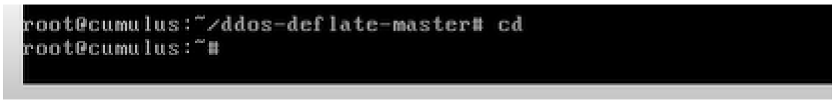
Installing .sh



```
  inflating: ddos-deflate-master/uninstall.sh
root@cumulus:~# cd ddos-deflate-master
root@cumulus:~/ddos-deflate-master# ./install.sh
error: Required dependency 'grepcidr' is missing.
Autoinstall dependencies by 'apt-get'? (n to exit)
```



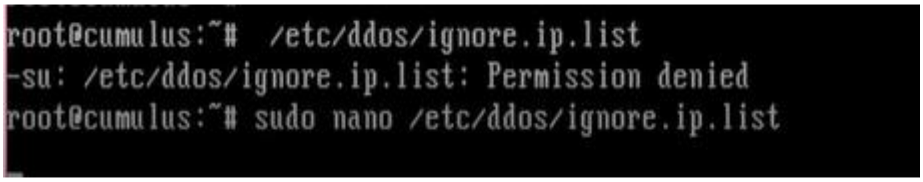
```
  inflating: ddos-deflate-master/uninstall.sh
root@cumulus:~# cd ddos-deflate-master
root@cumulus:~/ddos-deflate-master# ./install.sh
error: Required dependency 'grepcidr' is missing.
Autoinstall dependencies by 'apt-get'? (n to exit) y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```



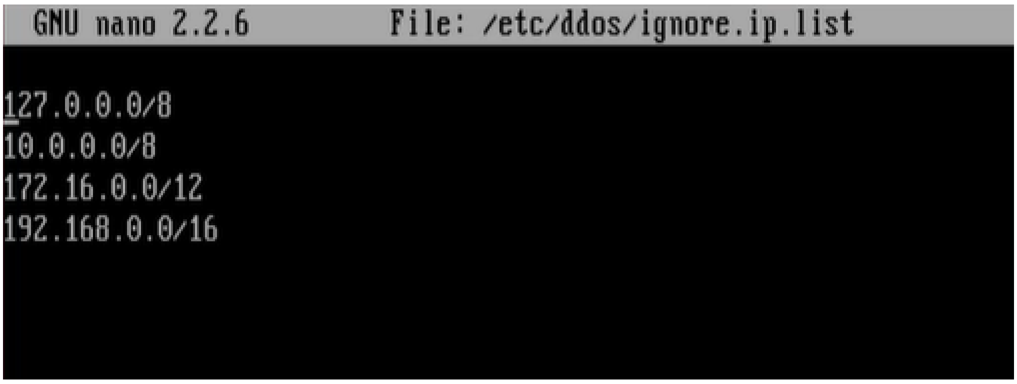
```
root@cumulus:~/ddos-deflate-master# cd
root@cumulus:~#
```

5- Open /etc/ddos/ignore.ip.list

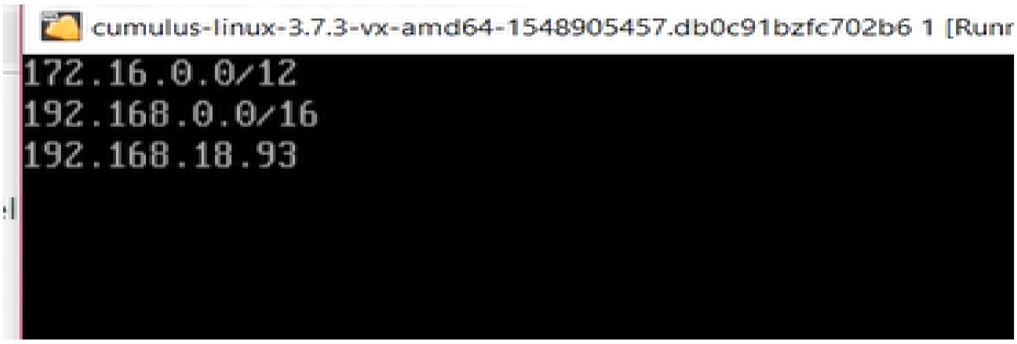
On this file you can add a list of ip addresses and subnets to be whitelisted



```
root@cumulus:~#  /etc/ddos/ignore.ip.list
-su: /etc/ddos/ignore.ip.list: Permission denied
root@cumulus:~# sudo nano /etc/ddos/ignore.ip.list
```

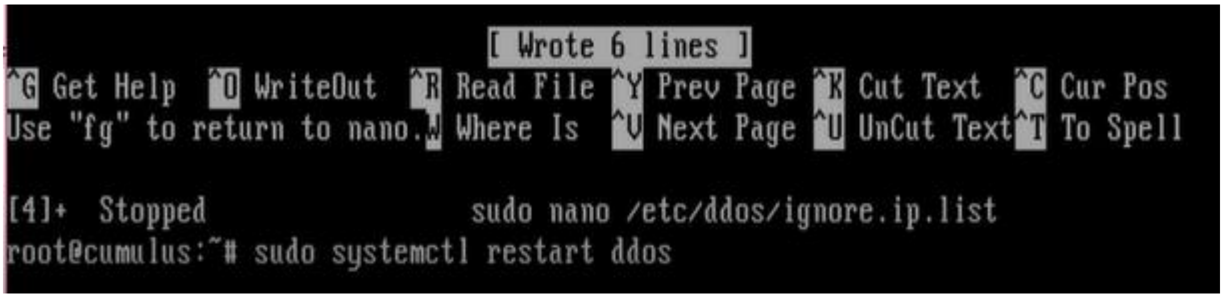


```
GNU nano 2.2.6            File: /etc/ddos/ignore.ip.list

127.0.0.0/8
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
```



```
cumulus-linux-3.7.3-vx-amd64-1548905457.db0c91bzfc702b6 1 [Runr
172.16.0.0/12
192.168.0.0/16
192.168.18.93
```

6- After editing DDOS configuration type sudo systemctl restart ddos



```
                              [ Wrote 6 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
Use "fg" to return to nano.W Where Is  ^V Next Page ^U UnCut Text^T To Spell

[4]+  Stopped                 sudo nano /etc/ddos/ignore.ip.list
root@cumulus:~# sudo systemctl restart ddos
```

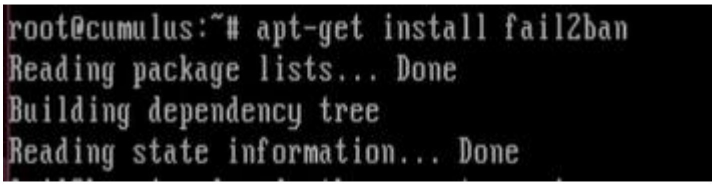
## 5.3 Fail2ban installation

Fail2ban works in a similar way to DDoS Deflate, as it also bans traffic based on malicious IP address profiling. It's a good performer and some of the main features are as follows:

- ✓ Easy to configure with some automation features included.
- ✓ Compatible with existing firewalls, e.g. iptables.
- ✓ Customizable blacklisting and whitelisting features.
- ✓ Ability to block automated brute force attacks.
- ✓ Time-based IP blocking.

- ✓ Fail2Ban is good option for any web server that has SSH and few other services.

1 – As a root user type apt-get install fail2ban and press enter

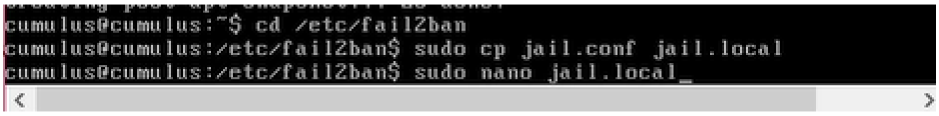


```
root@cumulus:~# apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

2- The fail2ban configuration is kept in the /etc/fail2ban directory. The configuration file that specifies the default banning rules is called jail.conf. Because of the way that fail2ban updates its configuration files when the program has a new version, we should not edit the default configuration file. Instead, we should copy it to a new location and edit it there:

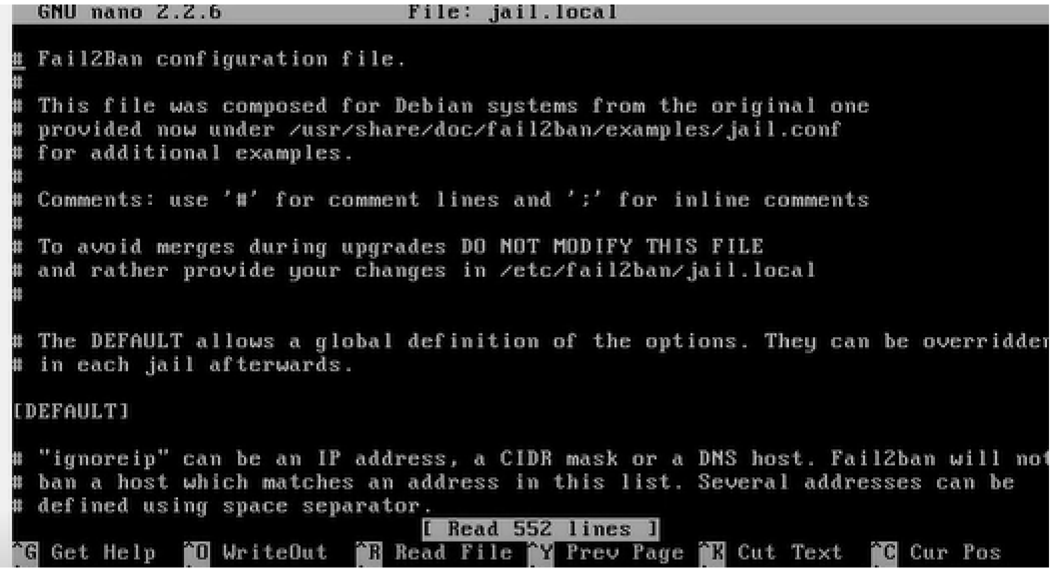
Use following commands on Cumulus VX

cd /etc/fail2ban
sudo cp jail.conf jail.local
sudo nano jail.local



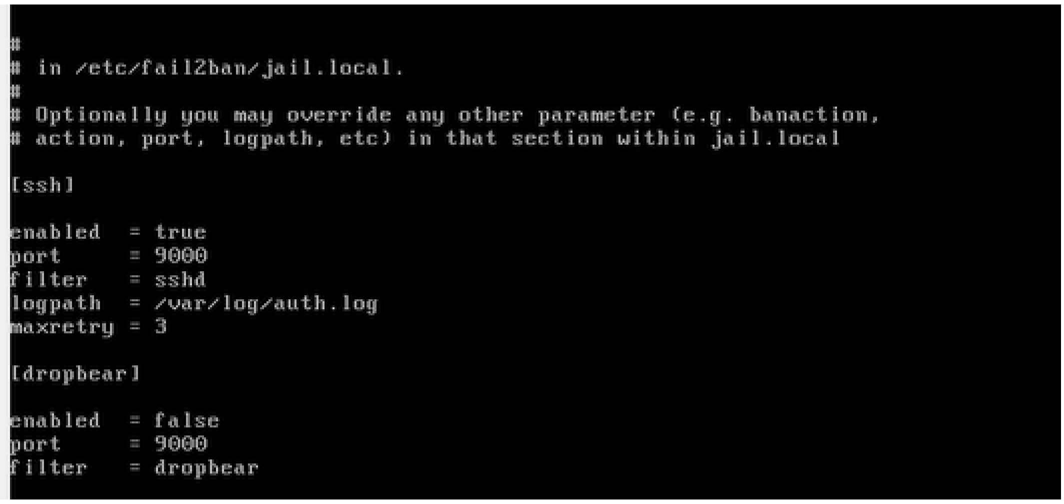
```
cumulus@cumulus:~$ cd /etc/fail2ban
cumulus@cumulus:/etc/fail2ban$ sudo cp jail.conf jail.local
cumulus@cumulus:/etc/fail2ban$ sudo nano jail.local_
```

3- Verify the configuration you can edit



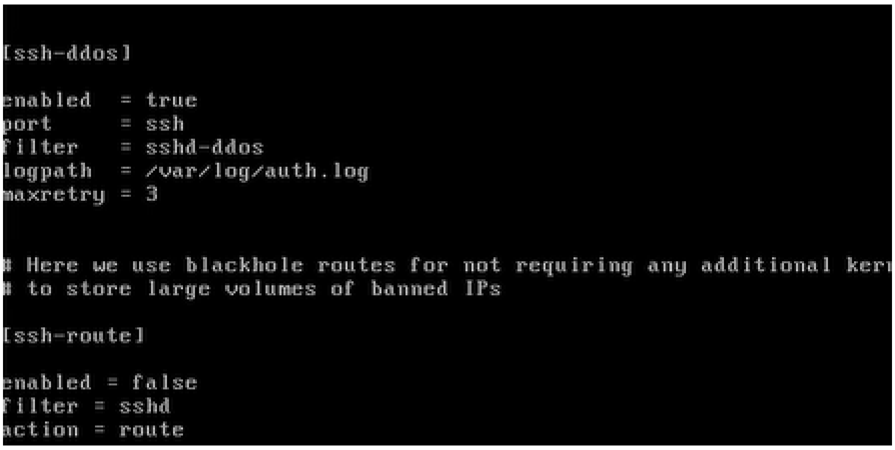
```
  GNU nano 2.2.6              File: jail.local

# Fail2Ban configuration file.
#
# This file was composed for Debian systems from the original one
# provided now under /usr/share/doc/fail2ban/examples/jail.conf
# for additional examples.
#
# Comments: use '#' for comment lines and ';' for inline comments
#
# To avoid merges during upgrades DO NOT MODIFY THIS FILE
# and rather provide your changes in /etc/fail2ban/jail.local
#

# The DEFAULT allows a global definition of the options. They can be overridde
# in each jail afterwards.

[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will no
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
                               [ Read 552 lines ]
^G Get Help   ^O WriteOut   ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
```

5- Change normal ssh port and retry option



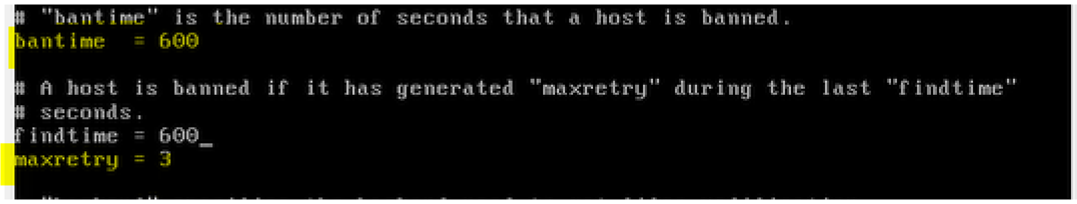
```
#
# in /etc/fail2ban/jail.local.
#
# Optionally you may override any other parameter (e.g. banaction,
# action, port, logpath, etc) in that section within jail.local

[ssh]

enabled  = true
port     = 9000
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3

[dropbear]

enabled  = false
port     = 9000
filter   = dropbear
```

6- Enabling SSH DDOS



```
[ssh-ddos]

enabled  = true
port     = ssh
filter   = sshd-ddos
logpath  = /var/log/auth.log
maxretry = 3


# Here we use blackhole routes for not requiring any additional ker
# to store large volumes of banned IPs

[ssh-route]

enabled = false
filter = sshd
action = route
```

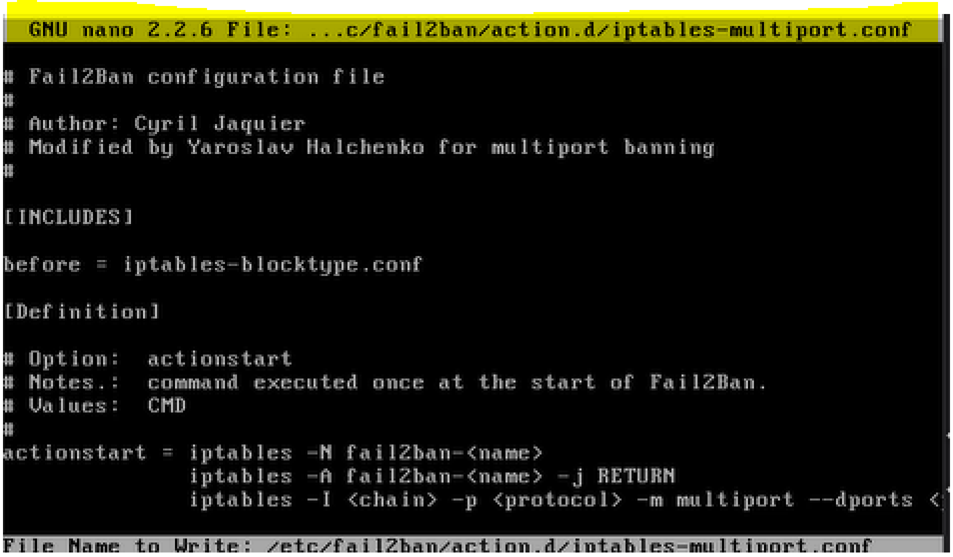
7- Defining bantime , maxretry limits



```
# "bantime" is the number of seconds that a host is banned.
bantime  = 600

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 600_
maxretry = 3
```

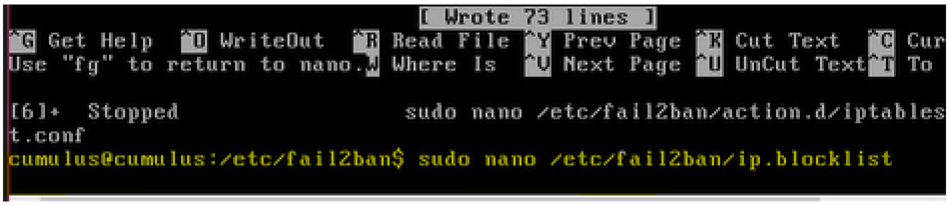
8- For our purposes, amend the actionstart command in the [Definition] section. This command (or commands) executes when the jail starts. To override the default action, create a corresponding. local file and add the amended actionstart command:

sudo nano /etc/fail2ban/action.d/iptables-multiport.local

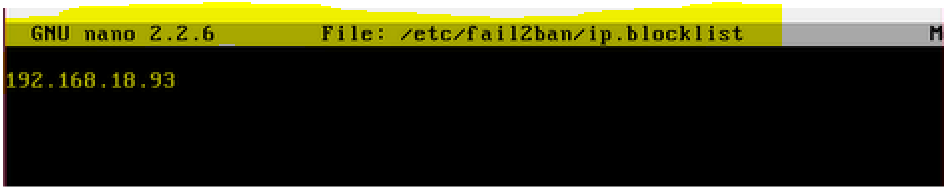


```
 GNU nano 2.2.6 File: ...c/fail2ban/action.d/iptables-multiport.conf

# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-blocktype.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I <chain> -p <protocol> -m multiport --dports <

File Name to Write: /etc/fail2ban/action.d/iptables-multiport.conf
```

9- Open file /etc/fail2ban/ip.blocklist and enter IP addresses to ban - one per line

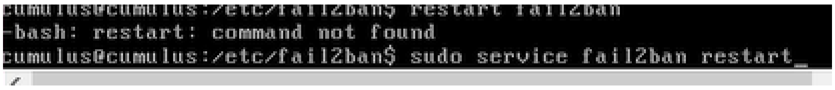


```
                                [ Wrote 73 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur
Use "fg" to return to nano.^W Where Is ^V Next Page ^U UnCut Text^T To

[6]+  Stopped                 sudo nano /etc/fail2ban/action.d/iptables
t.conf
cumulus@cumulus:/etc/fail2ban$ sudo nano /etc/fail2ban/ip.blocklist
```



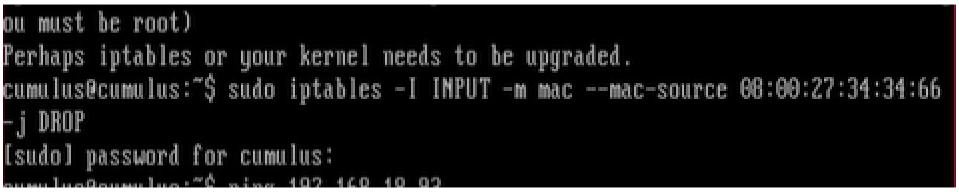
```
 GNU nano 2.2.6          File: /etc/fail2ban/ip.blocklist                M

192.168.18.93
```

10- Restart Fail2Ban for the changes to be applied. If you run sudo iptables -S now, you should see rules



```
cumulus@cumulus:/etc/fail2ban$ restart fail2ban
-bash: restart: command not found
cumulus@cumulus:/etc/fail2ban$ sudo service fail2ban restart_
```

11- Alternatively, IP address, mac address and other filter rules can be applied directly via Iptables as well. Example of Blocking Mac address via Ip tables



```
ou must be root)
Perhaps iptables or your kernel needs to be upgraded.
cumulus@cumulus:~$ sudo iptables -I INPUT -m mac --mac-source 08:00:27:34:34:66
-j DROP
[sudo] password for cumulus:
cumulus@cumulus:~$ ping 192.168.18.93
```