

PRAKTIKUM KEAMANAN KOMPUTER

PERTEMUAN 4

SNORT



Disusun Oleh :

Nama : Febriyan Fathur RF
NIM : 1600631002

JURUSAN

MANAJEMEN INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2017

TUJUAN PEMBELAJARAN :

1. Mengenalkan pada mahasiswa tentang konsep dasar autentikasi Snort
2. Memahami konsep Run Snort

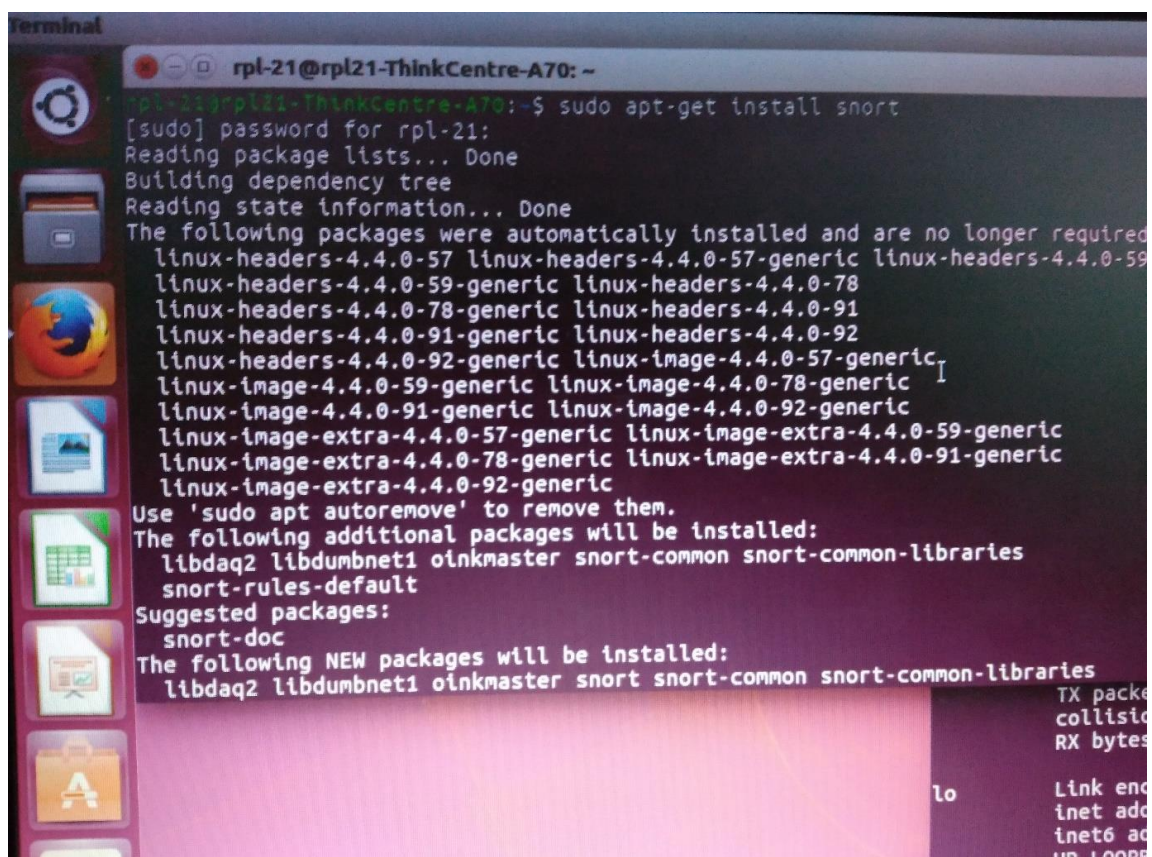
DASAR TEORI

Salah satu aplikasi Linux yang dapat dipakai untuk meningkatkan keamanan komputer adalah Snort. Secara garis besar, Snort adalah sebuah program yang memiliki tiga fungsi atau tiga modus operasi. Snort dapat dipakai dalam **packet sniffer mode** sehingga bekerja sebagai sniffer sama seperti Wireshark. Sama seperti Wireshark, Snort juga dapat menyimpan setiap packet yang di-capture ke dalam media penyimpan di modus **packet logger mode**. Akan tetapi berbeda dengan Wireshark, Snort dapat dipakai sebagai komponen NIDS dengan menjalankannya pada **Network Intrusion Detection System (NIDS) mode**. Pada modus yang terakhir ini, Snort akan menganalisa packet berdasarkan rule yang ada untuk mengenali adanya upaya serangan hacker.

Untuk memulai menggunakan Snort, download requirement serta source Snort, kemudian build & install. Bagi yang memakai distro Ubuntu, **libdnet** di distro tersebut adalah library yang berbeda dengan yang dibutuhkan Snort. Di Ubuntu, **libdnet** adalah **DECNet libraries**, sementara yang dibutuhkan oleh Snort diganti namanya menjadi **libdumpnet**. Sebaiknya download source dari Google Code, kemudian install ke lokasi **/usr**, bukan **/usr/local**. Caranya adalah dengan menambahkan argumen **-prefix=/usr** pada saat memanggil script **configure**.

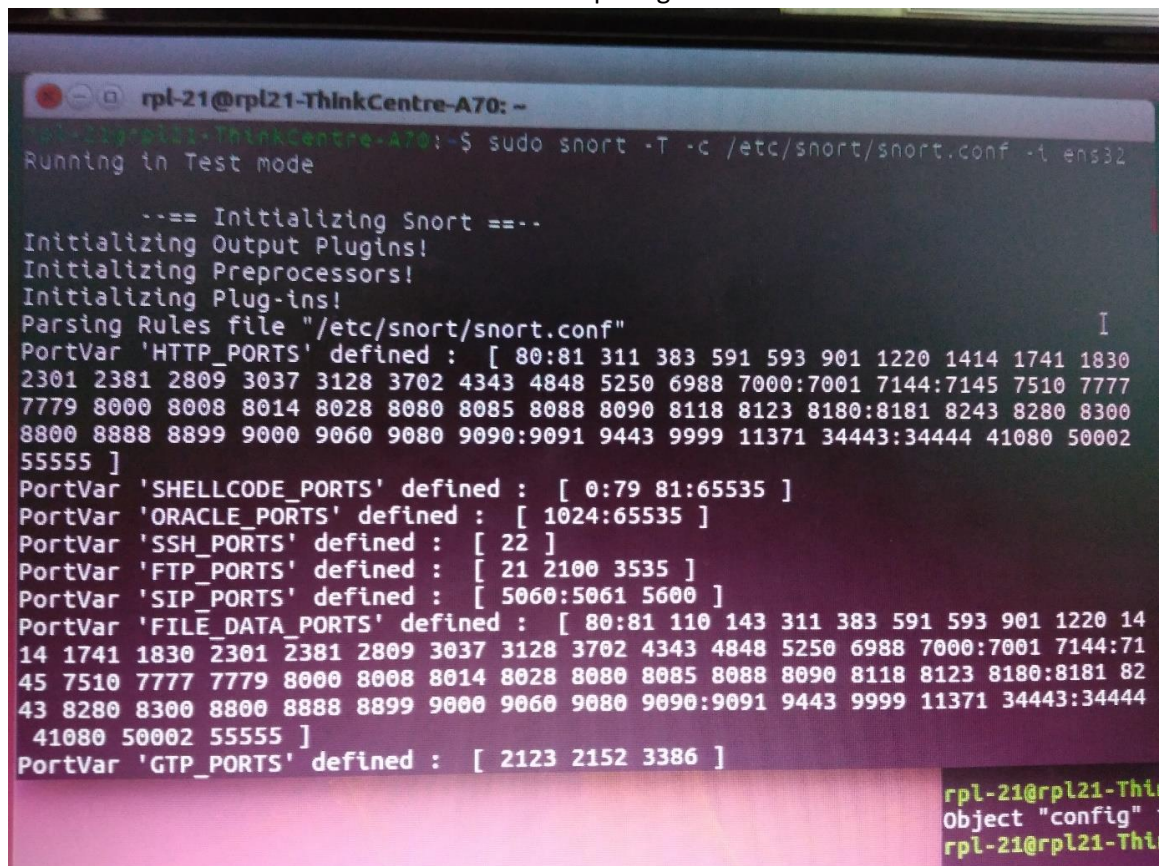
Langkah – Langkah Praktikum

1. Buka Terminal pada linux
2. Kemudian install snort terlebih dahulu.



```
Terminal
rpl-21@rpl21-ThinkCentre-A70: ~
rpl-21@rpl21-ThinkCentre-A70:~$ sudo apt-get install snort
[sudo] password for rpl-21:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-57 linux-headers-4.4.0-57-generic linux-headers-4.4.0-59
  linux-headers-4.4.0-59-generic linux-headers-4.4.0-78
  linux-headers-4.4.0-78-generic linux-headers-4.4.0-91
  linux-headers-4.4.0-91-generic linux-headers-4.4.0-92
  linux-headers-4.4.0-92-generic linux-image-4.4.0-57-generic
  linux-image-4.4.0-59-generic linux-image-4.4.0-78-generic
  linux-image-4.4.0-91-generic linux-image-4.4.0-92-generic
  linux-image-extra-4.4.0-57-generic linux-image-extra-4.4.0-59-generic
  linux-image-extra-4.4.0-78-generic linux-image-extra-4.4.0-91-generic
  linux-image-extra-4.4.0-92-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries
```


3. Jika Snort berhasil di install maka akan muncul seperti gambar dibawah

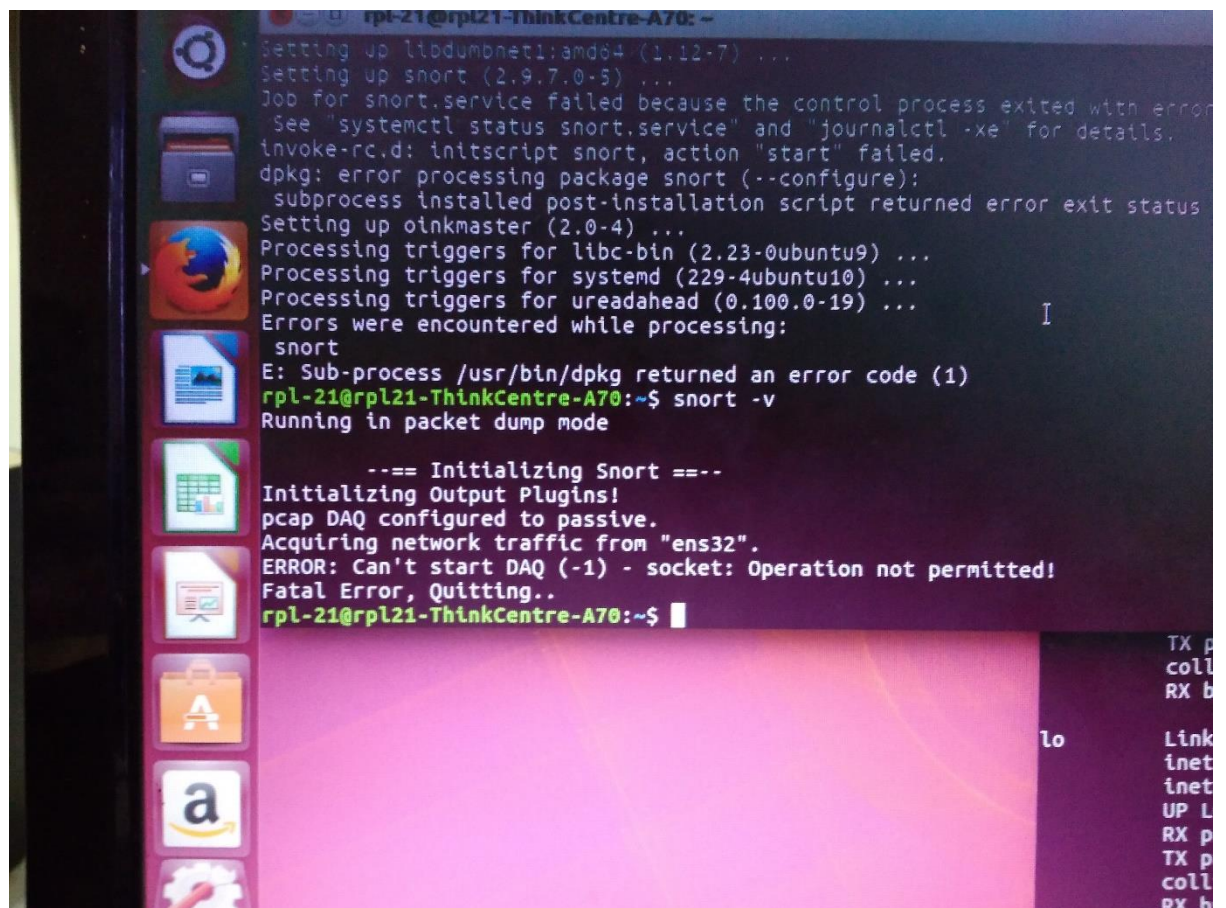
A terminal window on a Linux system (rpl-21@rpl21-ThinkCentre-A70) showing the output of the command 'sudo snort -T -c /etc/snort/snort.conf -t ens32'. The output indicates that Snort is running in test mode and lists various port ranges defined in the configuration file, such as HTTP_PORTS, ORACLE_PORTS, SSH_PORTS, FTP_PORTS, SIP_PORTS, FILE_DATA_PORTS, and GTP_PORTS. The terminal text is as follows:

```
rpl-21@rpl21-ThinkCentre-A70: ~$ sudo snort -T -c /etc/snort/snort.conf -t ens32
Running in Test mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830
2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777
7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 14
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]

rpl-21@rpl21-ThinkCentre-A70: ~$
```

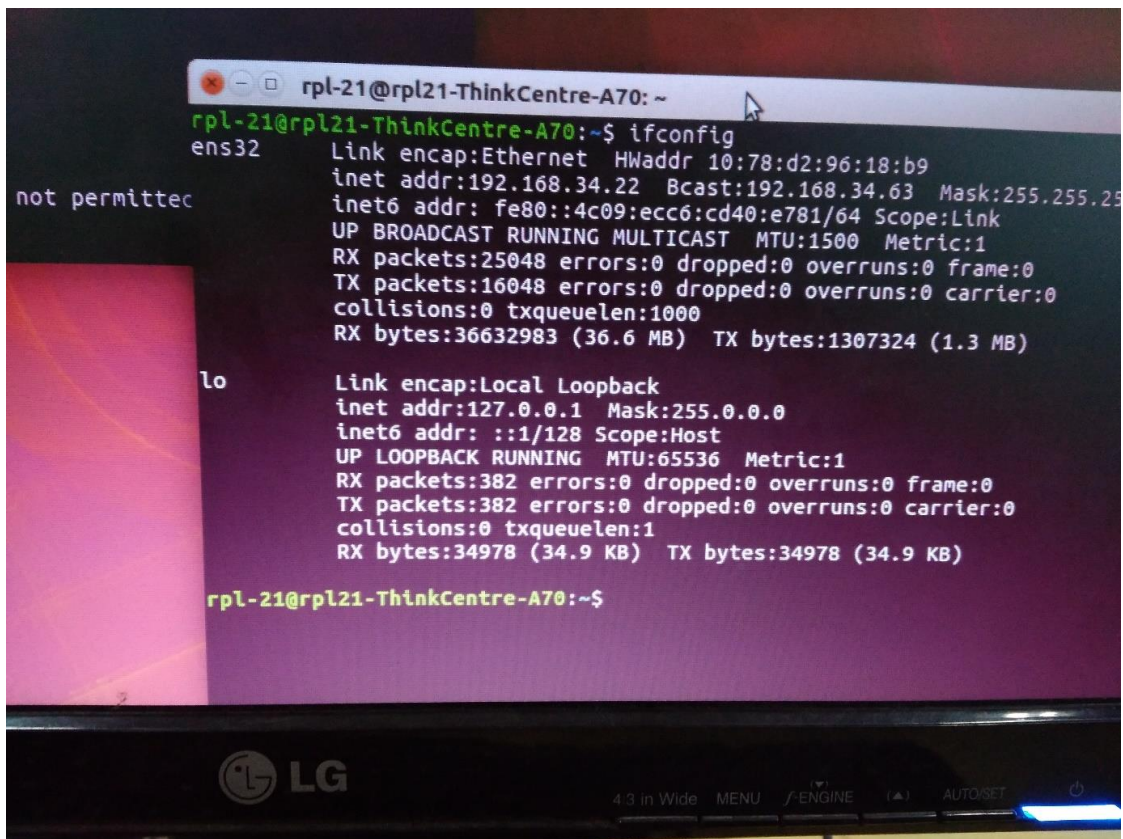
4. Setelah itu Running / jalankan snortnya

A terminal window on a Linux system (rpl-21@rpl21-ThinkCentre-A70) showing the output of the command 'snort -v'. The output indicates that Snort is running in packet dump mode and lists various port ranges defined in the configuration file. However, it also shows an error message: 'ERROR: Can't start DAQ (-1) - socket: Operation not permitted! Fatal Error, Quitting..'. The terminal text is as follows:

```
rpl-21@rpl21-ThinkCentre-A70: ~$ snort -v
Running in packet dump mode

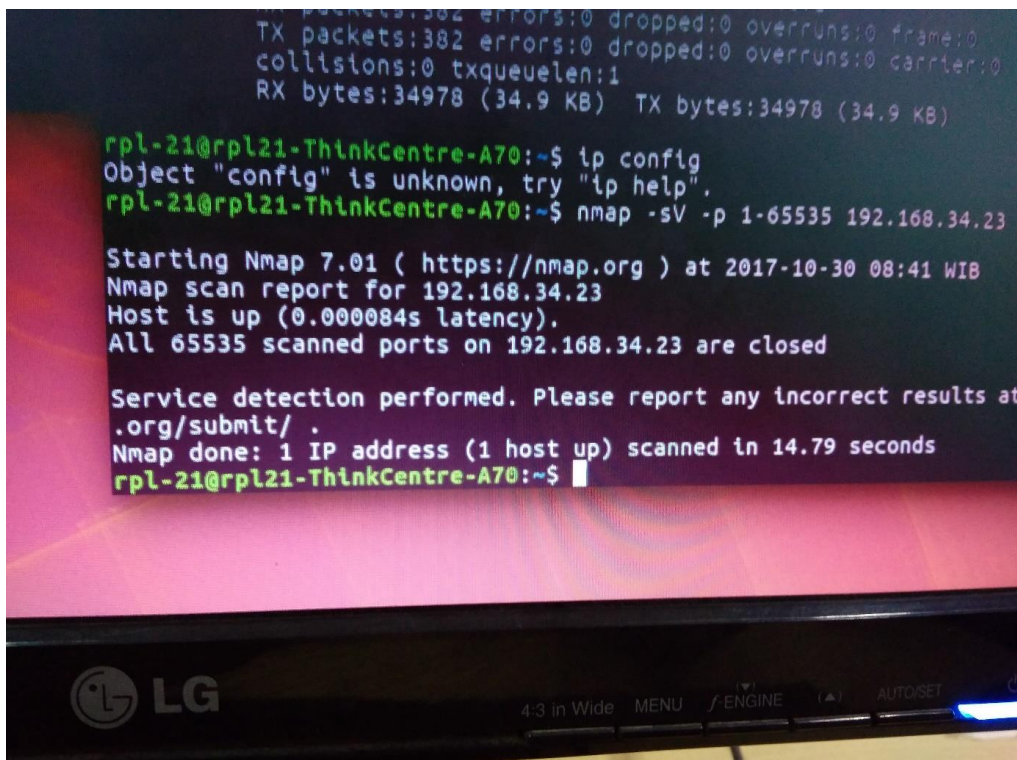
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens32".
ERROR: Can't start DAQ (-1) - socket: Operation not permitted!
Fatal Error, Quitting..
rpl-21@rpl21-ThinkCentre-A70: ~$
```


5. Lakukan perintah if config untuk mengetahui IP komputer anda dan komputer teman anda.



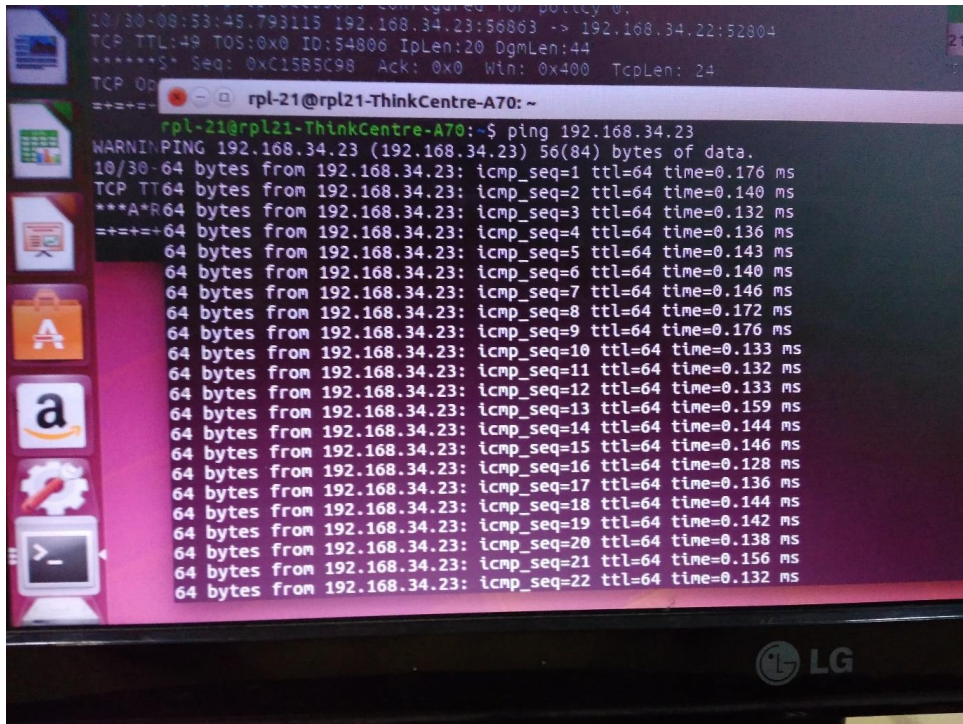
```
rpl-21@rpl21-ThinkCentre-A70: ~  
rpl-21@rpl21-ThinkCentre-A70:~$ ifconfig  
ens32      Link encap:Ethernet  HWaddr 10:78:d2:96:18:b9  
            inet addr:192.168.34.22  Bcast:192.168.34.63  Mask:255.255.255  
            inet6 addr: fe80::4c09:ecc6:cd40:e781/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:25048 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:16048 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:36632983 (36.6 MB)  TX bytes:1307324 (1.3 MB)  
  
lo         Link encap:Local Loopback  
            inet addr:127.0.0.1  Mask:255.0.0.0  
            inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:65536  Metric:1  
            RX packets:382 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:382 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1  
            RX bytes:34978 (34.9 KB)  TX bytes:34978 (34.9 KB)  
  
rpl-21@rpl21-ThinkCentre-A70:~$
```

6. Setelah Melakukan Perintah diatas, masukan IP komputer teman anda kedalam snort tersebut.



```
rpl-21@rpl21-ThinkCentre-A70:~$ ip config  
Object "config" is unknown, try "ip help".  
rpl-21@rpl21-ThinkCentre-A70:~$ nmap -sV -p 1-65535 192.168.34.23  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-30 08:41 WIB  
Nmap scan report for 192.168.34.23  
Host is up (0.000084s latency).  
All 65535 scanned ports on 192.168.34.23 are closed  
  
Service detection performed. Please report any incorrect results at  
.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 14.79 seconds  
rpl-21@rpl21-ThinkCentre-A70:~$
```

7. Langkah Akhir lakukan perintah Ping untuk mengetahui proses snort berhasil atau tidak. Jika proses berhasil maka akan muncul seperti gambar dibawah

A photograph of a computer monitor displaying a terminal window. The terminal shows a network configuration for a policy, followed by a ping command being executed from a host named 'rpl-21@rpl21-ThinkCentre-A70'. The output of the ping command shows 22 successful responses, each 64 bytes in size, with varying round-trip times between 0.128 ms and 0.176 ms. The terminal window has a dark background with light-colored text. On the left side of the monitor, a vertical dock contains several application icons, including a file manager, a web browser, and a terminal. The LG logo is visible at the bottom center of the monitor frame.

```
10/30-08:53:45.793113 192.168.34.23:56863 -> 192.168.34.22:52804
TCP TTL:49 TOS:0x0 ID:54806 IpLen:20 DgmLen:44
*****S* Seq: 0xC15B5C98 Ack: 0x0 Win: 0x400 TcpLen: 24
TCP Op
=====
rpl-21@rpl21-ThinkCentre-A70: ~
rpl-21@rpl21-ThinkCentre-A70:~$ ping 192.168.34.23
WARNING:PING 192.168.34.23 (192.168.34.23) 56(84) bytes of data.
10/30-64 bytes from 192.168.34.23: icmp_seq=1 ttl=64 time=0.176 ms
TCP TT64 bytes from 192.168.34.23: icmp_seq=2 ttl=64 time=0.140 ms
***A*R64 bytes from 192.168.34.23: icmp_seq=3 ttl=64 time=0.132 ms
==+=+=64 bytes from 192.168.34.23: icmp_seq=4 ttl=64 time=0.136 ms
64 bytes from 192.168.34.23: icmp_seq=5 ttl=64 time=0.143 ms
64 bytes from 192.168.34.23: icmp_seq=6 ttl=64 time=0.140 ms
64 bytes from 192.168.34.23: icmp_seq=7 ttl=64 time=0.146 ms
64 bytes from 192.168.34.23: icmp_seq=8 ttl=64 time=0.172 ms
64 bytes from 192.168.34.23: icmp_seq=9 ttl=64 time=0.176 ms
64 bytes from 192.168.34.23: icmp_seq=10 ttl=64 time=0.133 ms
64 bytes from 192.168.34.23: icmp_seq=11 ttl=64 time=0.132 ms
64 bytes from 192.168.34.23: icmp_seq=12 ttl=64 time=0.133 ms
64 bytes from 192.168.34.23: icmp_seq=13 ttl=64 time=0.159 ms
64 bytes from 192.168.34.23: icmp_seq=14 ttl=64 time=0.144 ms
64 bytes from 192.168.34.23: icmp_seq=15 ttl=64 time=0.146 ms
64 bytes from 192.168.34.23: icmp_seq=16 ttl=64 time=0.128 ms
64 bytes from 192.168.34.23: icmp_seq=17 ttl=64 time=0.136 ms
64 bytes from 192.168.34.23: icmp_seq=18 ttl=64 time=0.144 ms
64 bytes from 192.168.34.23: icmp_seq=19 ttl=64 time=0.142 ms
64 bytes from 192.168.34.23: icmp_seq=20 ttl=64 time=0.138 ms
64 bytes from 192.168.34.23: icmp_seq=21 ttl=64 time=0.156 ms
64 bytes from 192.168.34.23: icmp_seq=22 ttl=64 time=0.132 ms
```