

KEAMANAN KOMPUTER

Instalasi snort



Disusun oleh:

Nama : Fani Firmansyah

NIM :1600631005

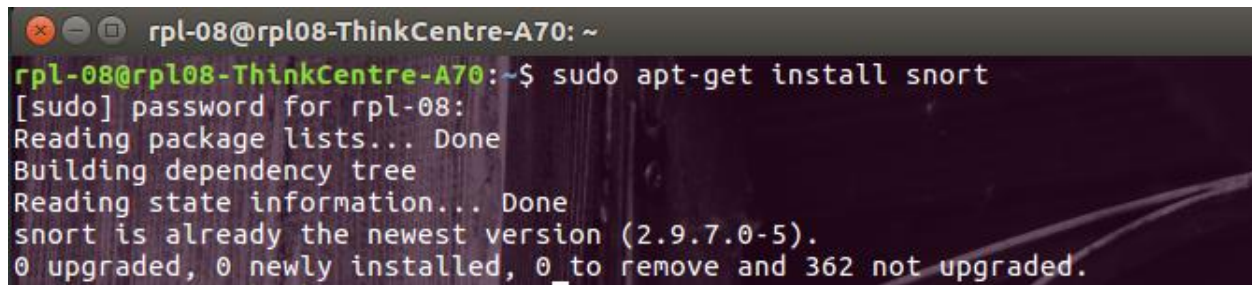
**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2017**

Praktikum :

Snort adalah aplikasi untuk mendeteksi adanya penyusupan, penyerangan, pemindaian dan dapat melakukan pencegahan.

Langkah langkah praktikum :

1. buka terminal terlebih dahulu, kemudian klik :

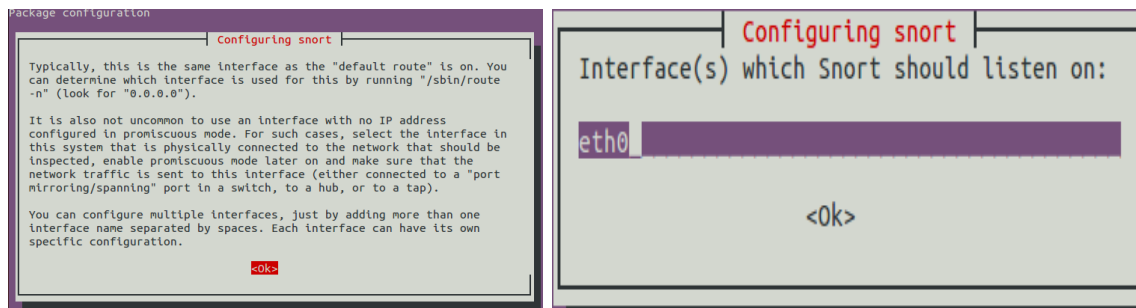


```
rpl-08@rpl08-ThinkCentre-A70: ~  
rpl-08@rpl08-ThinkCentre-A70:~$ sudo apt-get install snort  
[sudo] password for rpl-08:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
snort is already the newest version (2.9.7.0-5).  
0 upgraded, 0 newly installed, 0 to remove and 362 not upgraded.
```

Sudo apt-get install snort digunakan untuk menginstalasi snortnya

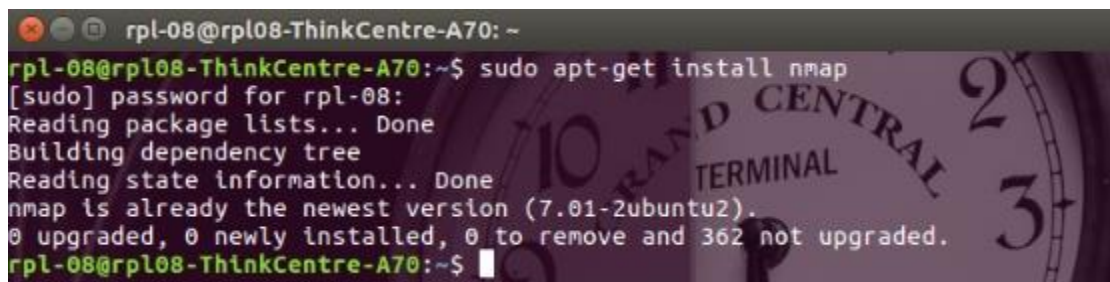
2. kemudian akan terjadi proses instalasi, tunggu sampai selesai.

3. pilih saja ok, untuk gambar ke-2 adalah interface yang akan dilindungi oleh snortnya



4. instalasi nmap pada ubuntu menggunakan perintah sudo apt-get install nmap

Buka pada terminal baru



```
rpl-08@rpl08-ThinkCentre-A70: ~  
rpl-08@rpl08-ThinkCentre-A70:~$ sudo apt-get install nmap  
[sudo] password for rpl-08:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
nmap is already the newest version (7.01-2ubuntu2).  
0 upgraded, 0 newly installed, 0 to remove and 362 not upgraded.  
rpl-08@rpl08-ThinkCentre-A70:~$
```

5. menjalankan nmap pada ubuntu dengan perintah seperti dibawah

```
rpl-08@rpl08-ThinkCentre-A70: ~
0 upgraded, 0 newly installed, 0 to remove and 362 not upgraded.
rpl-08@rpl08-ThinkCentre-A70:~$ sudo snort -T -c /etc/snort/snort.conf -i 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 ]
rpl-08@rpl08-ThinkCentre-A70:~$ sudo apt-get install
```

6. menjalankan nmap pada ubuntu dengan perintah seperti dibawah dengan ip computer teman

```
rpl-08@rpl08-ThinkCentre-A70:~$ nmap -sV -p 1-65535 192.168.34.11

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-30 09:12 WIB
Nmap scan report for 192.168.34.11
Host is up (0.000094s latency).
All 65535 scanned ports on 192.168.34.11 are closed
```

7. lakukan ping kepada ip computer teman untuk membuktikan apakah sudah dapat terhubung atau tidak

```
rpl-08@rpl08-ThinkCentre-A70: ~
rpl-08@rpl08-ThinkCentre-A70:~$ ping 192.168.34.11
PING 192.168.34.11 (192.168.34.11) 56(84) bytes of data:
64 bytes from 192.168.34.11: icmp_seq=1 ttl=64 time=0.153 ms
64 bytes from 192.168.34.11: icmp_seq=2 ttl=64 time=0.103 ms
64 bytes from 192.168.34.11: icmp_seq=3 ttl=64 time=0.130 ms
64 bytes from 192.168.34.11: icmp_seq=4 ttl=64 time=0.130 ms
64 bytes from 192.168.34.11: icmp_seq=5 ttl=64 time=0.130 ms
64 bytes from 192.168.34.11: icmp_seq=6 ttl=64 time=0.114 ms
64 bytes from 192.168.34.11: icmp_seq=7 ttl=64 time=0.159 ms
64 bytes from 192.168.34.11: icmp_seq=8 ttl=64 time=0.109 ms
64 bytes from 192.168.34.11: icmp_seq=9 ttl=64 time=0.121 ms
```

Gambar diatas menunjukkan bahwa perintah ping telah berjalan