PRAKTIKUM KEAMANAN KOMPUTER

LAPORAN 5

PORTSENTRY

Disusun Oleh :

Nama : Febriyan Fathur RF
NIM : 1600631002

JURUSAN

MANAJEMEN INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2017

TUJUAN PEMBELAJARAN :

1. Mengenalkanpadamahasiswatentangkonsepdasarautentikasilinux
2. MemahamikonsepPortsentry
3. Memahami cara menjalankan portsentry dalam linux

Praktikum 5

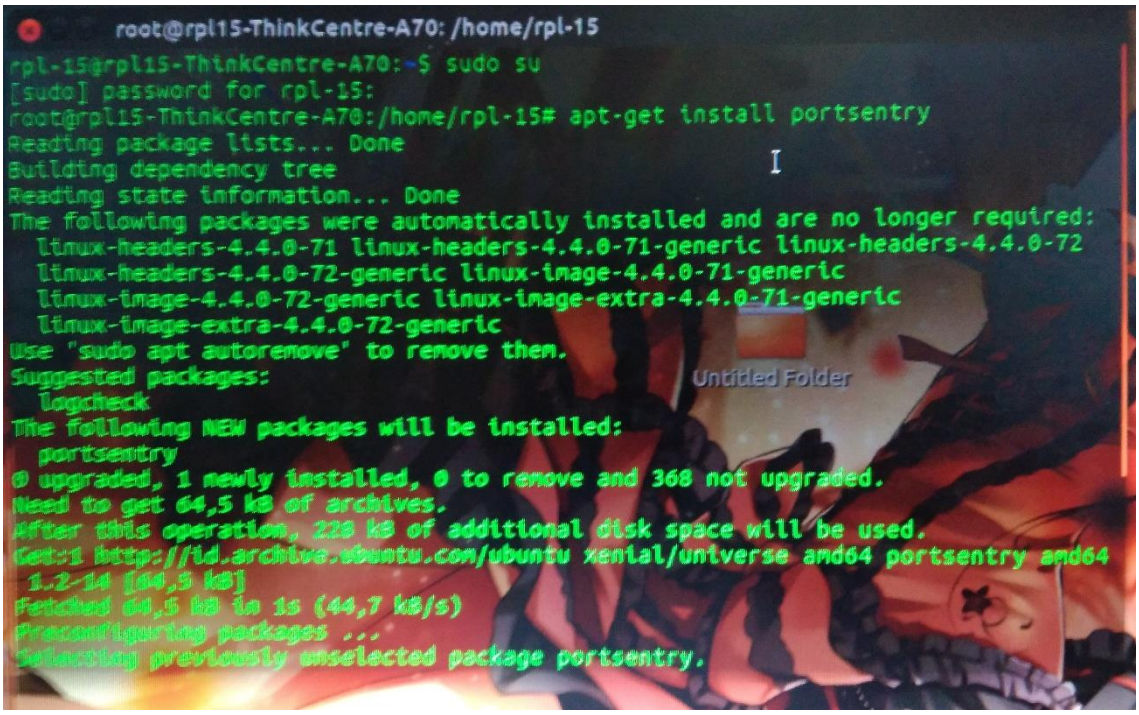
- Install Portsentry
  buka terminal
  ketiksudosu :
  install dengancara : apt-get install portsentry
- melihatkonfigurasiportsentry :
  ls -l /etc/portsentry
  ada 3 filekonfigurasiportsentryyaitu :
- nanoportsentry.conf
  1. nanoportsentry.ignore : alamatipkomputersebelahnya
     ifconfig –a
  2. nanoportsentry.ignore.static
     untukmelihatpesan yang dibuatportsentry
  3. grepportsentry /var/log/syslog
     kodeuntukmenjalankanportsentrybaik manual maupunotomatis
     ls -l /etc/init.d/portsentry
- untukmencariidentitas id portsentry
  find /etc/rc*.d/* -print | xargs ls -l | grepportsentry
  runlevel
  N
  0 = system halt
  1 = single user
  2 = full multi user mode (default)
  3-5 = samaseperti 2
  6 = system reboot
- menjalankandanmenghentikanportsentrysecara manual
  cd /etc/init.d
  ./portsentrystop
- ngecekportsentrysedangjalanapatidak
  ps -eaf | grep -v grep | grepportsentry | wc -l
  ./portsentrystart
- utukmelihat status portsentry
  ps -eaf |grep -v grep | grepportsentry
- untukmemeriksa status portsentry yang aktif
  ps -eaf | grep -vgrep | grepportsentry | wc –l
- cek status portsentry
  service portsentry status

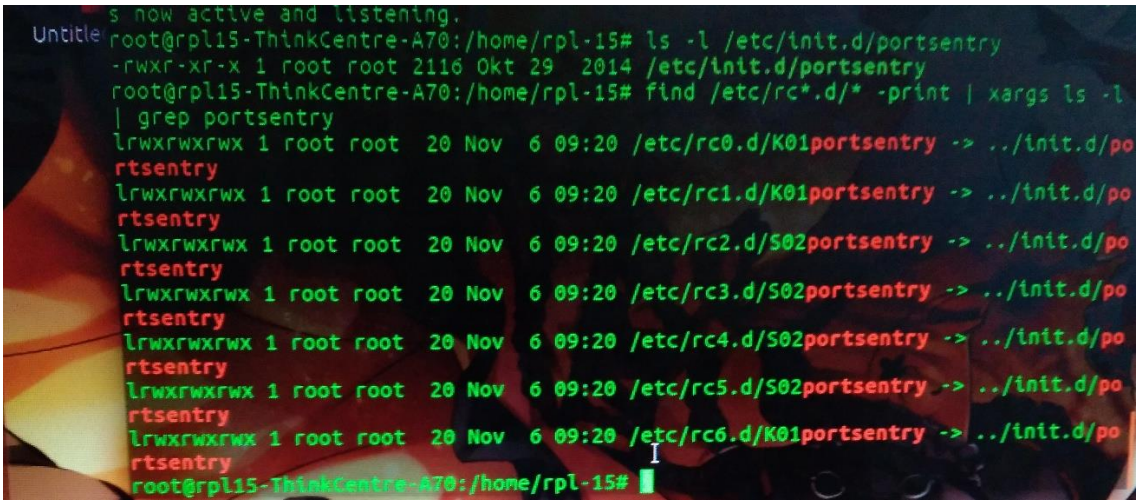
untukmelakukan scanning dari port 1 - 65535
nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 IPTEMENNYA

- untukmencari data serangan yang dibuatoleh port sentry
  grep “attackalert” /var/log/syslog

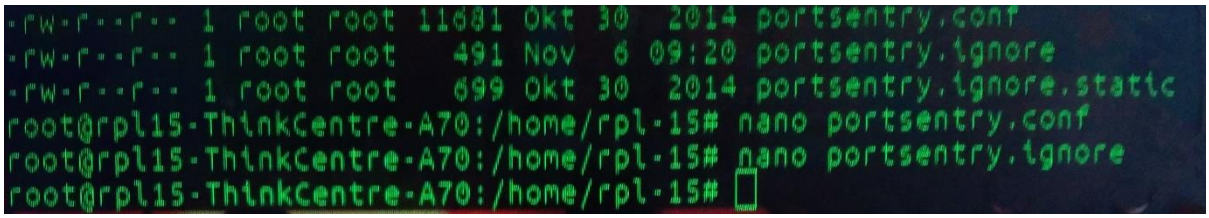
LAPORAN PRAKTIKUM 4 PORTSENTRY

1. Proses instalasiportsentry

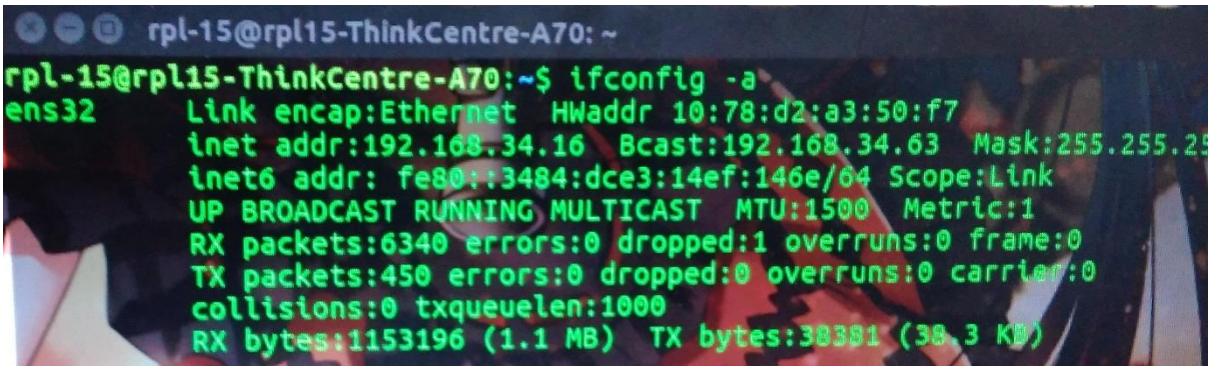




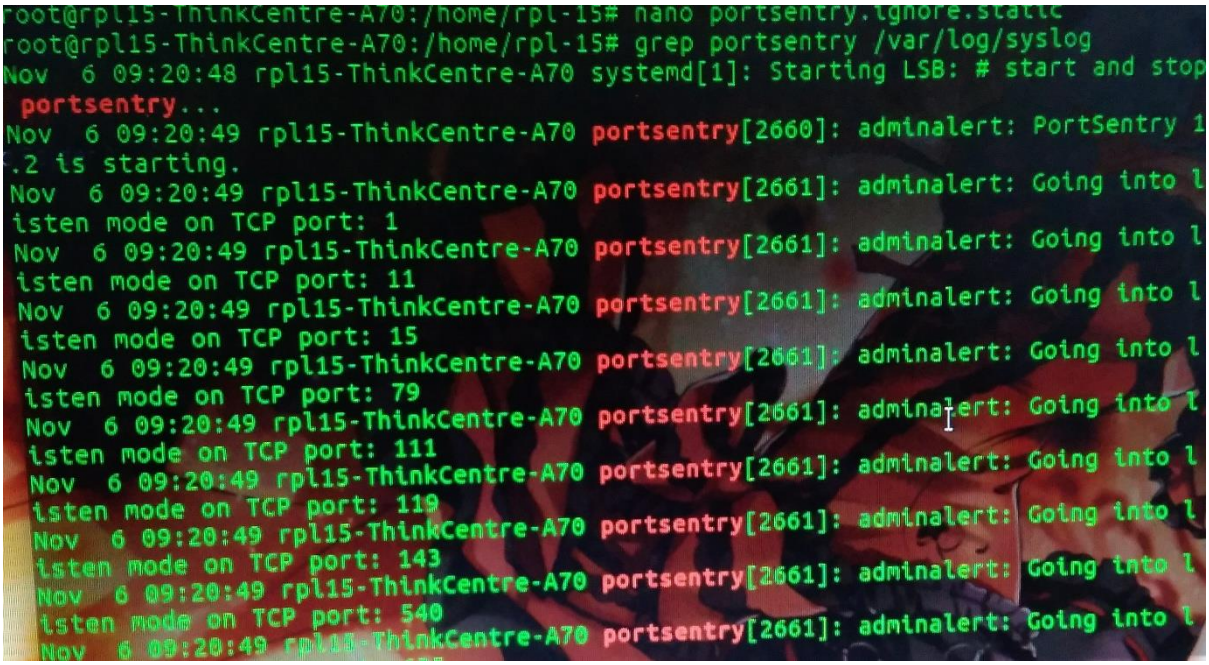
2. Cara konfigurasiportsentry



- Untuk Konfigurasi Komputer Teman



- Hasil konfigurasi

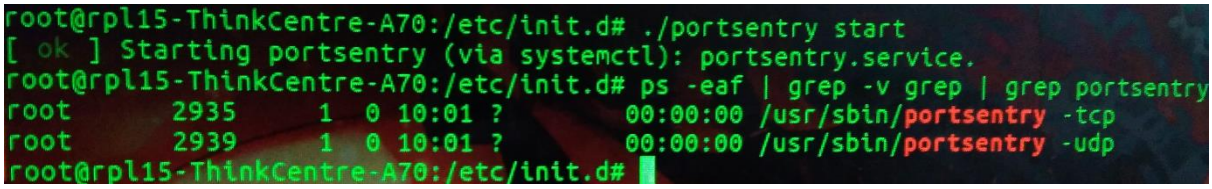


3. Cara menjalankandanmenghentikanportsentry

- Untuk Menjalankan Portsentry

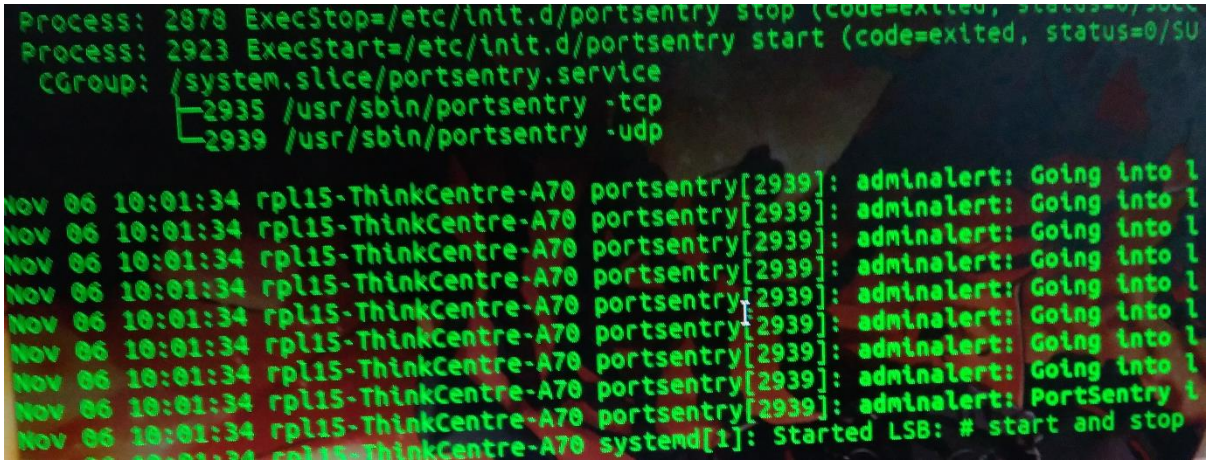
```
oot@rpl15-ThinkCentre-A70:/home/rpl-15# runlevel
N 5
root@rpl15-ThinkCentre-A70:/home/rpl-15# cd /etc/init.d
root@rpl15-ThinkCentre-A70:/etc/init.d# ./portsentry stop
[ ok ] Stopping portsentry (via systemctl): portsentry.service.
root@rpl15-ThinkCentre-A70:/etc/init.d# 
```

- Untuk Starting Portsentry



```
root@rpl15-ThinkCentre-A70:/etc/init.d# ./portsentry start
[ ok ] Starting portsentry (via systemctl): portsentry.service.
root@rpl15-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry
root      2935     1  0 10:01 ?        00:00:00 /usr/sbin/portsentry -tcp
root      2939     1  0 10:01 ?        00:00:00 /usr/sbin/portsentry -udp
root@rpl15-ThinkCentre-A70:/etc/init.d# 
```

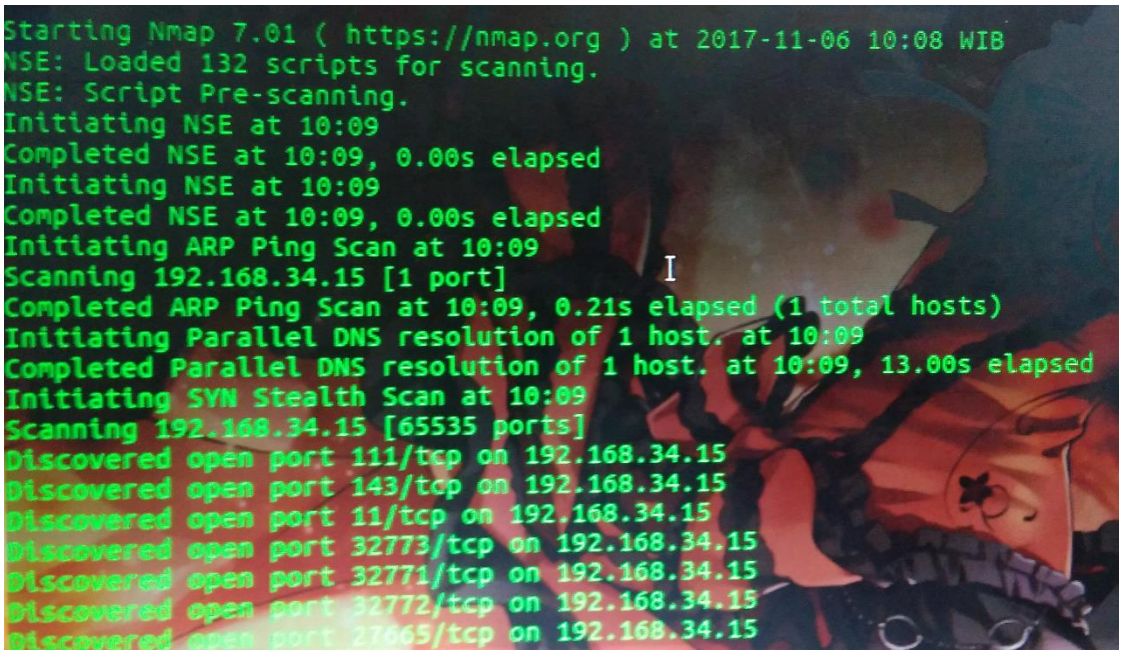
- Untuk Menghentikan Portsentry



```
 Process: 2878 ExecStop=/etc/init.d/portsentry stop (code=exited, status=0/SUCC
 Process: 2923 ExecStart=/etc/init.d/portsentry start (code=exited, status=0/SU
  CGroup: /system.slice/portsentry.service
          ├─2935 /usr/sbin/portsentry -tcp
          └─2939 /usr/sbin/portsentry -udp

Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into l
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: PortSentry i
Nov 06 10:01:34 rpl15-ThinkCentre-A70 systemd[1]: Started LSB: # start and stop
```

4. Cara ujicoba port scanning dengannmap



```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-06 10:08 WIB
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:09
Completed NSE at 10:09, 0.00s elapsed
Initiating NSE at 10:09
Completed NSE at 10:09, 0.00s elapsed
Initiating ARP Ping Scan at 10:09
Scanning 192.168.34.15 [1 port]
Completed ARP Ping Scan at 10:09, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:09
Completed Parallel DNS resolution of 1 host. at 10:09, 13.00s elapsed
Initiating SYN Stealth Scan at 10:09
Scanning 192.168.34.15 [65535 ports]
Discovered open port 111/tcp on 192.168.34.15
Discovered open port 143/tcp on 192.168.34.15
Discovered open port 11/tcp on 192.168.34.15
Discovered open port 32773/tcp on 192.168.34.15
Discovered open port 32771/tcp on 192.168.34.15
Discovered open port 32772/tcp on 192.168.34.15
Discovered open port 27665/tcp on 192.168.34.15
```

5. Cara melihat log yang dihasilkanolehportsentry

- Dalam Langkah terakhir ini kita inputkan IP Komputer teman anda