

LAPORAN KEAMANAN KOMPUTER

Instal Portsentry



Disusun oleh:

Nama : Ella Cinthia Fajar Asih

NIM : 1600631010

MANAJEMEN INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2017/2018

1. PENGERTIAN

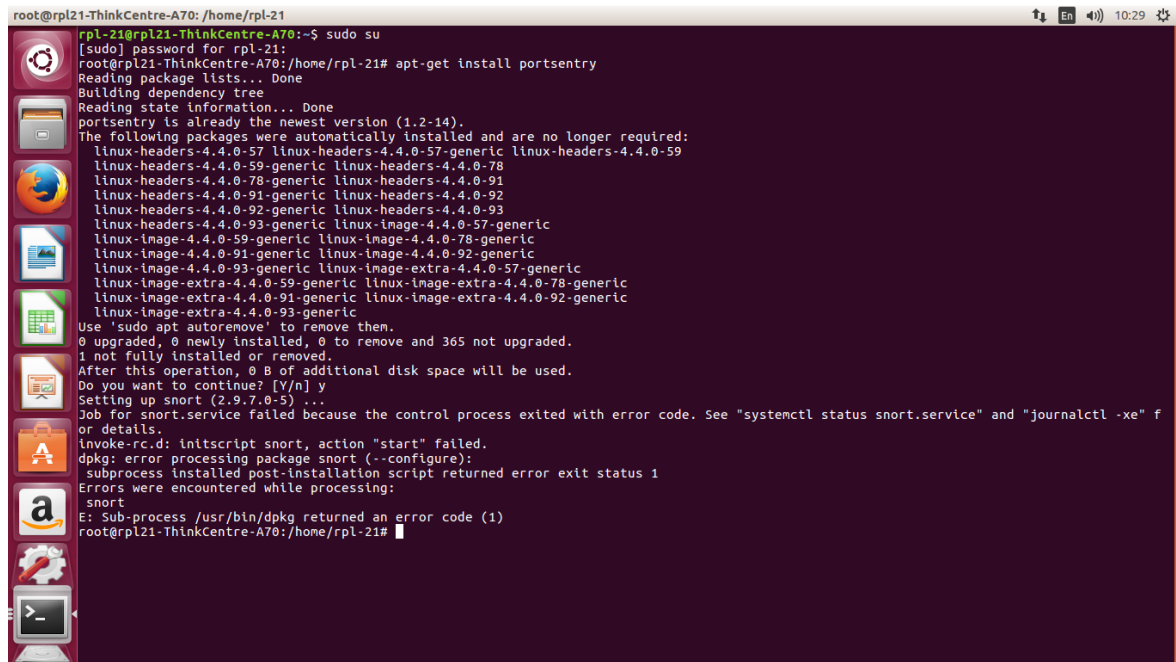
Definisi PortSentry

PortSentry adalah sebuah perangkat lunak yang dirancang untuk mendeteksi adanya port scanning & meresponds secara aktif jika ada port scanning. Port scan adalah proses scanning berbagai aplikasi servis yang dijalankan di server Internet. Port scan adalah langkah paling awal sebelum sebuah serangan di lakukan.

2. LANGKAH-LANGKAH PRATIKUM

1. Install Portsentry

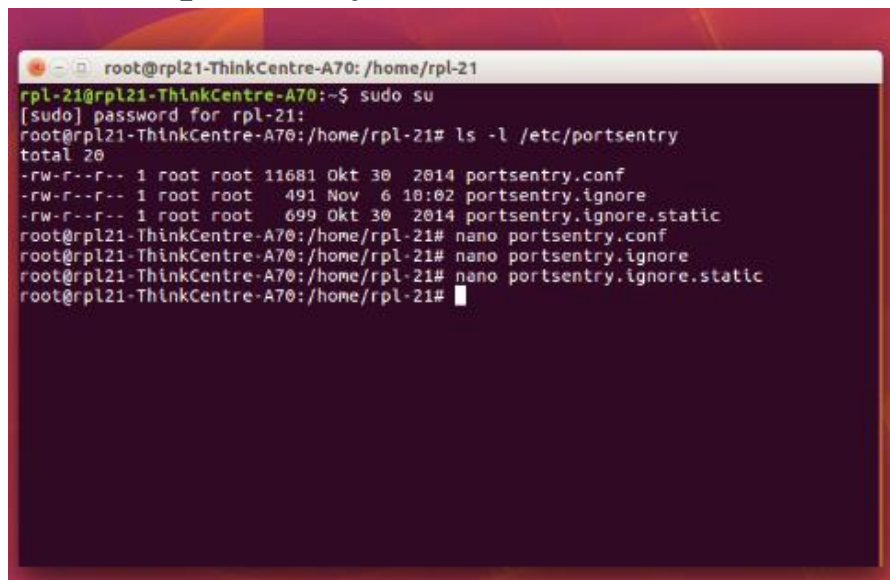
Apt-get install portsentry



```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# apt-get install portsentry
Reading package lists... Done
Building dependency tree
Reading state information... Done
portsentry is already the newest version (1.2-14).
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-headers-4.4.0-93
linux-headers-4.4.0-93-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-4.4.0-93-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
linux-image-extra-4.4.0-93-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 365 not upgraded.
1 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Setting up snort (2.9.7.0-5) ...
Job for snort.service failed because the control process exited with error code. See "systemctl status snort.service" and "journalctl -xe" for details.
invoke-rc.d: initscript snort, action "start" failed.
dpkg: error processing package snort (--configure):
 subprocess installed post-installation script returned error exit status 1
Errors were encountered while processing:
 snort
E: Sub-process /usr/bin/dpkg returned an error code (1)
root@rpl21-ThinkCentre-A70: /home/rpl-21#
```

2. Melihat konfigurasi portsentry

Ls -l /etc/portsentry



```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# ls -l /etc/portsentry
total 20
-rw-r--r-- 1 root root 11681 Okt 30 2014 portsentry.conf
-rw-r--r-- 1 root root 491 Nov 6 10:02 portsentry.ignore
-rw-r--r-- 1 root root 699 Okt 30 2014 portsentry.ignore.static
root@rpl21-ThinkCentre-A70: /home/rpl-21# nano portsentry.conf
root@rpl21-ThinkCentre-A70: /home/rpl-21# nano portsentry.ignore
root@rpl21-ThinkCentre-A70: /home/rpl-21# nano portsentry.ignore.static
root@rpl21-ThinkCentre-A70: /home/rpl-21#
```

3. Melihat pesan yang dibuat portsentry Grep portsentry /var/log/syslog

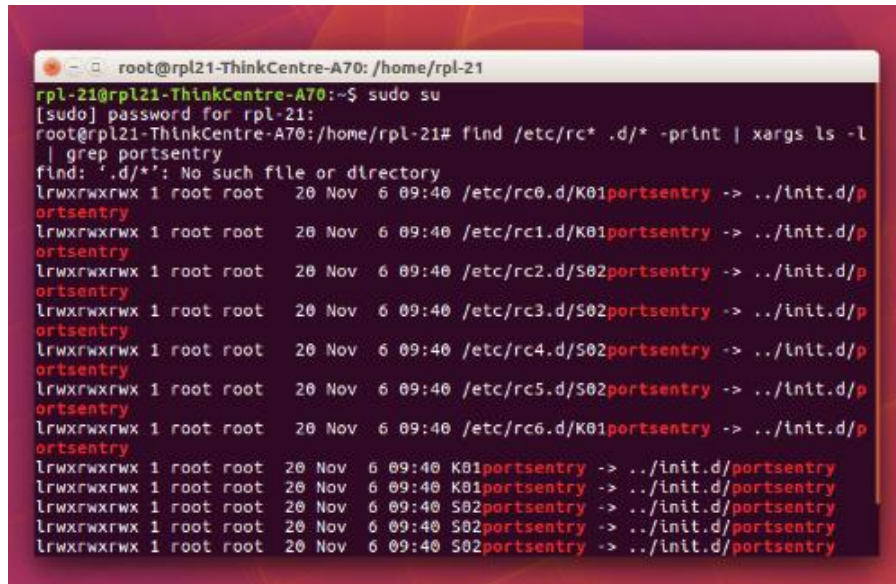
```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# grep portsentry /var/log/syslog
Nov  6 09:40:36 rpl21-ThinkCentre-A70 systemd[1]: Starting LSB: # start and stop
portsentry...
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1941]: adminalert: PortSentry 1
.2 is starting.
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on ICP port: 1
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 11
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 15
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 79
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 111
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 119
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 143
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
isten mode on TCP port: 540
Nov  6 09:40:37 rpl21-ThinkCentre-A70 portsentry[1942]: adminalert: Going into l
```

4. Kode menjalankan portsentrymanual maupun otomatis Ls -l /etc/init.d/portsentry

```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# ls -l /etc/init.d/portsentry
-rwxr-xr-x 1 root root 2116 Okt 29  2014 /etc/init.d/portsentry
root@rpl21-ThinkCentre-A70: /home/rpl-21#
```

5. Untuk mencari identitas id portsentry

Find /etc/rc* -print | xargs ls -l | grep portsentry

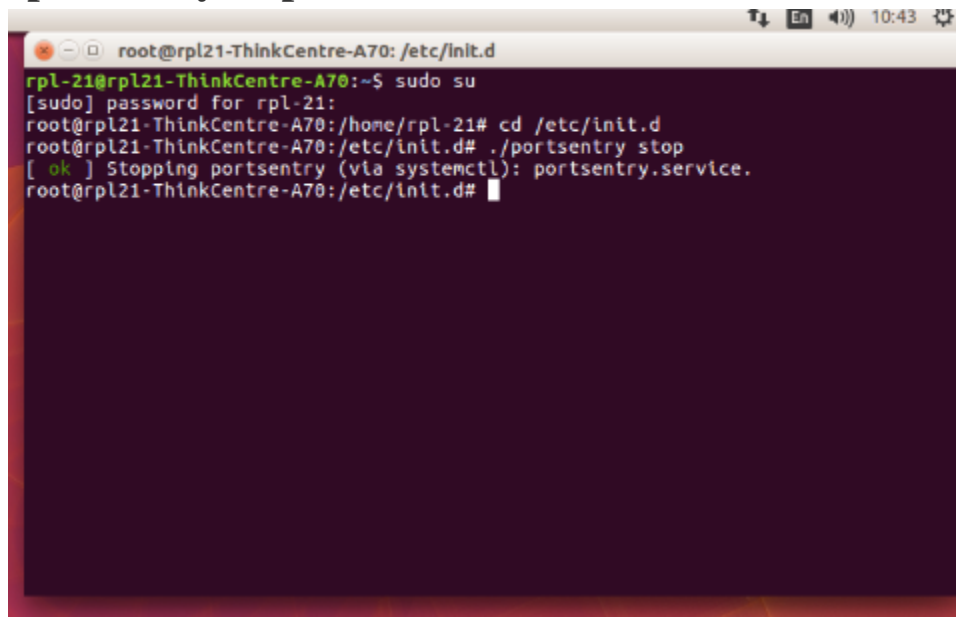


```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# find /etc/rc* -print | xargs ls -l
| grep portsentry
find: './d/*': No such file or directory
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc0.d/K01portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc1.d/K01portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc2.d/S02portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc3.d/S02portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc4.d/S02portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc5.d/S02portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 /etc/rc6.d/K01portsentry -> ../init.d/p
ortsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:40 S02portsentry -> ../init.d/portsentry
```

6. Menghentikan portsentry secara manual

Cd /etc/init.d

./portsentry.stop



```
root@rpl21-ThinkCentre-A70: /etc/init.d
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# cd /etc/init.d
root@rpl21-ThinkCentre-A70: /etc/init.d# ./portsentry stop
[ ok ] Stopping portsentry (via systemctl): portsentry.service.
root@rpl21-ThinkCentre-A70: /etc/init.d#
```


7. Cek status portsentry

Sevice portsentry status

```
root@rpl21-ThinkCentre-A70: /home/rpl-21
rpl-21@rpl21-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-21:
root@rpl21-ThinkCentre-A70: /home/rpl-21# service portsentry status
● portsentry.service - LSB: # start and stop portsentry
   Loaded: loaded (/etc/init.d/portsentry; bad; vendor preset: enabled)
   Active: inactive (dead) since Sen 2017-11-06 10:43:39 WIB; 4min 23s ago
     Docs: man:systemd-sysv-generator(8)
   Process: 3055 ExecStop=/etc/init.d/portsentry stop (code=exited, status=0/SUCCESS)

Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Host: 192.1
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Connect fro
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Host: 192.1
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Connect fro
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Host: 192.1
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Connect fro
Nov 06 10:11:18 rpl21-ThinkCentre-A70 portsentry[2350]: attackalert: Host: 192.1
Nov 06 10:43:39 rpl21-ThinkCentre-A70 systemd[1]: Stopping LSB: # start and stop
Nov 06 10:43:39 rpl21-ThinkCentre-A70 portsentry[3055]: Stopping anti portscan d
Nov 06 10:43:39 rpl21-ThinkCentre-A70 systemd[1]: Stopped LSB: # start and stop
lines 1-16/16 (END)
```

8. Cek nmap terlebih dahulu (nmap)

9. Melakukan uji coba scanning dengan nmap

Nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 IP
TEMENNYA

```
root@rpl21-ThinkCentre-A70: /home/rpl-21
root@rpl21-ThinkCentre-A70: /home/rpl-21# nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 192.168.34.23

Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-06 10:50 WIB
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating ARP Ping Scan at 10:50
Scanning 192.168.34.23 [1 port]
Completed ARP Ping Scan at 10:50, 0.43s elapsed (1 total hosts)
Nmap scan report for 192.168.34.23 [host down]
NSE: Script Post-scanning.
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.51 seconds
   Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
root@rpl21-ThinkCentre-A70: /home/rpl-21#
```

10. Melihat log yang dihasilkn oleh portsentry

[illegible]