LAPORAN PRAKTIKUM

KEAMANAN KOMPUTER

INSTALLASI PORTSENTRY

DI SUSUN OLEH :

NAMA : Fani Firmansyah

NIM : 1600631005

FAKULTAS TEKNIK

MANAJEMEN INFORMTIKA

TAHUN 2017

Langkah Tugas Praktikum :

1. Buka terminal terlebih dahulu

2. ketik pada terminal : sudo su sebagai langkah awal

```
rpl-26@rpl26-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-26:
```

3. Lakukan penginstalan portsentry

```
root@rpl26-ThinkCentre-A70:/home/rpl-26# apt-get install portsentry
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
0 upgraded, 1 newly installed, 0 to remove and 594 not upgraded.
Need to get 64,5 kB of archives.
After this operation, 228 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu xenial/universe amd64 portsentry amd64 1.2-14 [64,5 kB]
Fetched 64,5 kB in 1s (43,5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package portsentry.
(Reading database ... 172133 files and directories currently installed.)
Preparing to unpack .../portsentry_1.2-14_amd64.deb ...
Unpacking portsentry (1.2-14) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Processing triggers for systemd (229-4ubuntu4) ...
Setting up portsentry (1.2-14) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for systemd (229-4ubuntu4) ...
root@rpl26-ThinkCentre-A70:/home/rpl-26# ls -l/etc/portsentry
ls: invalid option -- '/'
Try 'ls --help' for more information.
```

4 . Ketik : ls -l /etc/portsentryls untuk melakukan konfigurasi

```
root@rpl26-ThinkCentre-A70:/home/rpl-26# 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 09:42 portsentry.ignore
-rw-r--r-- 1 root root   699 Okt 30  2014 portsentry.ignore.static
root@rpl26-ThinkCentre-A70:/home/rpl-26# nano portsentry.conf
Use "fg" to return to nano.

[1]+  Stopped                 nano portsentry.conf
root@rpl26-ThinkCentre-A70:/home/rpl-26# nano portsentry.ignore
root@rpl26-ThinkCentre-A70:/home/rpl-26# nano portsentry.ignore.static
```

5. Ketikkan: grep portsentry /var/log/syslog untuk melihat pesan yang dibuat portsentry

```
root@rpl26-ThinkCentre-A70:/home/rpl-26# grep portsentry /var/log/syslog
Nov  6 09:42:50 rpl26-ThinkCentre-A70 systemd[1]: Starting LSB: # start and stop portsentry...
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2080]: adminalert: PortSentry 1.2 is starting.
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
1
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
5
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 7
9
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
11
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
19
Nov  6 09:42:50 rpl26-ThinkCentre-A70 portsentry[2081]: adminalert: Going into listen mode on TCP port: 1
43
```

6. Ketik : find /etc/rc*.d/* -print | xargs ls -l | grep portsentry untuk mencari identitas id portsentry

```
root@rpl26-ThinkCentre-A70:/home/rpl-26# find /etc/rc*.d/* -print | xargs ls -l |grep portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc0.d/K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc1.d/K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc2.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc3.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc4.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc5.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc6.d/K01portsentry -> ../init.d/portsentry
root@rpl26-ThinkCentre-A70:/home/rpl-26# runlevel
N 5
root@rpl26-ThinkCentre-A70:/home/rpl-26# cd /etc/init.d
root@rpl26-ThinkCentre-A70:/etc/init.d# ./portsentry stop
[ ok ] Stopping portsentry (via systemctl): portsentry.service.
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry | wc -l
```

7. Ketik : ps -eaf | grep -v grep | grep portsentry | wc –l Untuk mengecek portsentry sedang jalan apa tidak

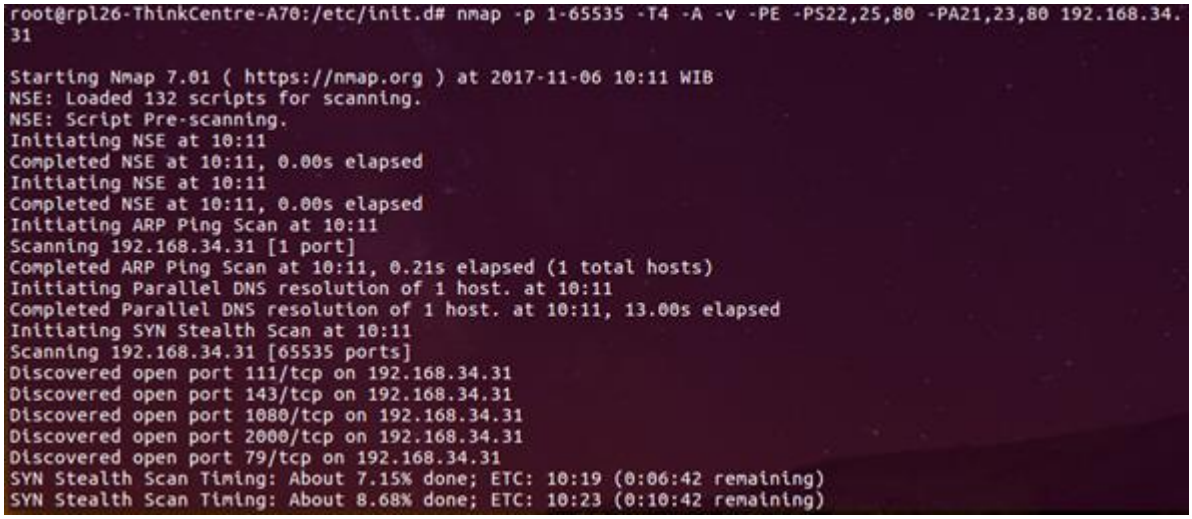
```
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry | wc -l
1
root@rpl26-ThinkCentre-A70:/etc/init.d# ./portsentry start
[ ok ] Starting portsentry (via systemctl): portsentry.service.
```

8. Ketik : ps -eaf | grep -v grep | grep portsentry utuk melihat status portsentry

Dan ps -eaf | grep -v grep | grep portsentry | wc -l untuk memeriksa status portsentry yang aktif

```
root@rpl26-ThinkCentre-A70:/home/rpl-26# ls -l /etc/init.d/portsentry
-rwxr-xr-x 1 root root 2116 Okt 29  2014 /etc/init.d/portsentry
root@rpl26-ThinkCentre-A70:/home/rpl-26# find /etc/rc*.d/* -print | xargs ls -l |grep portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc0.d/K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc1.d/K01portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc2.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc3.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc4.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc5.d/S02portsentry -> ../init.d/portsentry
lrwxrwxrwx 1 root root  20 Nov  6 09:42 /etc/rc6.d/K01portsentry -> ../init.d/portsentry
root@rpl26-ThinkCentre-A70:/home/rpl-26# runlevel
N 5
root@rpl26-ThinkCentre-A70:/home/rpl-26# cd /etc/init.d
root@rpl26-ThinkCentre-A70:/etc/init.d# ./portsentry stop
[ ok ] Stopping portsentry (via systemctl): portsentry.service.
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry | wc -l
1
root@rpl26-ThinkCentre-A70:/etc/init.d# cd /etc/init.d
root@rpl26-ThinkCentre-A70:/etc/init.d# ./portsentry stop
[ ok ] Stopping portsentry (via systemctl): portsentry.service.
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry | wc -l
1
root@rpl26-ThinkCentre-A70:/etc/init.d# ./portsentry start
[ ok ] Starting portsentry (via systemctl): portsentry.service.
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentryroot      2179
9:44 pts/3    00:00:00 nano portsentry.conf
root      2403     1  0 10:01 ?        00:00:00 /usr/sbin/portsentry -tcp
root      2407     1  0 10:01 ?        00:00:00 /usr/sbin/portsentry -udp
root@rpl26-ThinkCentre-A70:/etc/init.d# ps -eaf | grep -v grep | grep portsentry | wc -l
```

9. Ketik : nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 IPTEMENNYA misal (192.168.30.15) untuk scanning nmap dengan ip komputer temen


root@rpl26-ThinkCentre-A70:/etc/init.d# nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 192.168.34.
31
Starting Nmap 7.01 (https://nmap.org) at 2017-11-06 10:11 WIB
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating ARP Ping Scan at 10:11
Scanning 192.168.34.31 [1 port]
Completed ARP Ping Scan at 10:11, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:11
Completed Parallel DNS resolution of 1 host. at 10:11, 13.00s elapsed
Initiating SYN Stealth Scan at 10:11
Scanning 192.168.34.31 [65535 ports]
Discovered open port 111/tcp on 192.168.34.31
Discovered open port 143/tcp on 192.168.34.31
Discovered open port 1080/tcp on 192.168.34.31
Discovered open port 2000/tcp on 192.168.34.31
Discovered open port 79/tcp on 192.168.34.31
SYN Stealth Scan Timing: About 7.15% done; ETC: 10:19 (0:06:42 remaining)
SYN Stealth Scan Timing: About 8.68% done; ETC: 10:23 (0:10:42 remaining)

10.