

LAPORAN PRAKTIKUM KEAMANAN KOMPUTER
INSTALL PORTSENTRY



Oleh:

Nama : Faisol Al-Jufri
NIM : 1600631018
Prodi : MI

PRODI MANAJEMEN INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER

2017

I. Tujuan Instruksional Khusus (TIK)

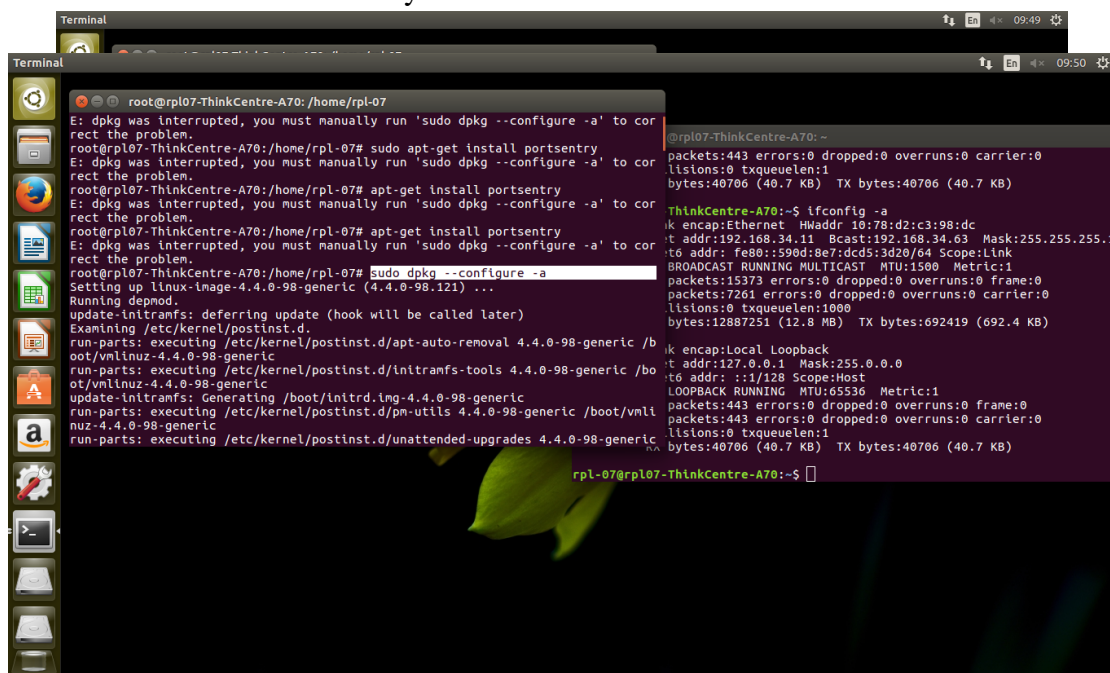
1. Mahasiswa mampu mengamankan komputer dengan aplikasi portsentry.
2. Mahasiswa mampu memahami tentang cara dan penganggulangan scamming.

II. Tugas Praktikum

- Install Portsentry
- konfigurasi Portsentry
- menjalankan dan menghentikan Portsentry
- uji coba port Scanning dengan nmap
- cara melihatkan log yang dihasilkan oleh portsentry

III. Hasil Praktikum

- Install Portsentry



```
root@rpl07-ThinkCentre-A70: /home/rpl-07
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
root@rpl07-ThinkCentre-A70: /home/rpl-07# sudo apt-get install portsentry
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
root@rpl07-ThinkCentre-A70: /home/rpl-07# apt-get install portsentry
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
root@rpl07-ThinkCentre-A70: /home/rpl-07# sudo dpkg --configure -a
Setting up linux-image-4.4.0-98-generic (4.4.0-98.121) ...
Running depmod.
update-initramfs: deferring update (hook will be called later)
Examining /etc/kernel/postinst.d.
run-parts: executing /etc/kernel/postinst.d/apt-auto-removal 4.4.0-98-generic /boot/vmlinuz-4.4.0-98-generic
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 4.4.0-98-generic /boot/vmlinuz-4.4.0-98-generic
update-initramfs: Generating /boot/initrd.img-4.4.0-98-generic
run-parts: executing /etc/kernel/postinst.d/pm-utils 4.4.0-98-generic /boot/vmlinuz-4.4.0-98-generic
run-parts: executing /etc/kernel/postinst.d/unattended-upgrades 4.4.0-98-generic
rpl-07@rpl07-ThinkCentre-A70:~$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  MTU=1500  Metric=1
        packets:443 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        bytes:12887251 (12.8 MB)  TX bytes:692419 (692.4 KB)

lo: flags=73<UP,LOOPBACK,RUNNING>  MTU=65536  Metric=1
        packets:443 errors:0 dropped:0 overruns:0 frame:0
        packets:443 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        bytes:40706 (40.7 KB)  TX bytes:40706 (40.7 KB)
```

```
Terminal
root@rpl07-ThinkCentre-A70: /home/rpl-07
done
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Setting up libpoppler58:amd64 (0.41.0-0ubuntu1.5) ...
Setting up libpoppler-glib8:amd64 (0.41.0-0ubuntu1.5) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
root@rpl07-ThinkCentre-A70: /home/rpl-07# apt-get install portsentry
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic
  linux-image-4.4.0-21-generic linux-image-extra-4.4.0-21-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  linux-image-extra-4.4.0-98-generic
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
The following packages will be upgraded:
  linux-image-extra-4.4.0-98-generic
1 upgraded, 1 newly installed, 0 to remove and 367 not upgraded.
1 not fully installed or removed.
Need to get 64.5 kB/36.2 MB of archives.

@rpl07-ThinkCentre-A70: ~
portsentry
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)

ThinkCentre-A70:~$ ifconfig -a
ik encap:Ethernet HWaddr 10:78:d2:c3:98:dc
t addr:192.168.34.11 Bcast:192.168.34.63 Mask:255.255.255.1
t6 addr: fe80::590d:8e7:dc5:3d20/64 Scope:Link
BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
packets:15373 errors:0 dropped:0 overruns:0 frame:0
packets:7261 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1000
bytes:12887251 (12.8 MB) TX bytes:692419 (692.4 KB)

ik encap:Local Loopback
t addr:127.0.0.1 Mask:255.0.0.0
t6 addr: ::1/128 Scope:Host
LOOPBACK RUNNING MTU:65536 Metric:1
packets:443 errors:0 dropped:0 overruns:0 frame:0
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)

rpl-07@rpl07-ThinkCentre-A70:~$
```

- konfigurasi Portsentry

```
Terminal
root@rpl07-ThinkCentre-A70: /home/rpl-07
Found mentest86+ image: /boot/mentest86+.elf
Found mentest86+ image: /boot/mentest86+.bin
Found Windows 7 (loader) on /dev/sda1
done
Setting up portsentry (1.2-14) ...
Processing triggers for systemd (229-4ubuntu10) ...
root@rpl07-ThinkCentre-A70: /home/rpl-07# ls -l etc/portdnrny
ls: cannot access 'etc/portdnrny': No such file or directory
root@rpl07-ThinkCentre-A70: /home/rpl-07# ls -l /etc/portdnrny
ls: cannot access '/etc/portdnrny': No such file or directory
root@rpl07-ThinkCentre-A70: /home/rpl-07# 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 09:25 portsentry.ignore
-rw-r--r-- 1 root root 699 Okt 30 2014 portsentry.ignore.static
root@rpl07-ThinkCentre-A70: /home/rpl-07# nano portsentry.conf
root@rpl07-ThinkCentre-A70: /home/rpl-07# nano portsentry.ignore
root@rpl07-ThinkCentre-A70: /home/rpl-07# nano portsentry.ignore.static
root@rpl07-ThinkCentre-A70: /home/rpl-07# grep portsentry /var/log/syslog
Nov 6 09:25:38 rpl07-ThinkCentre-A70 systemd[1]: Starting LSB: # start and stop
portsentry...
Nov 6 09:25:39 rpl07-ThinkCentre-A70 portsentry[14663]: adminalert: PortSentry
1.2 is starting.

@rpl07-ThinkCentre-A70: ~
portsentry
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)

ThinkCentre-A70:~$ ifconfig -a
ik encap:Ethernet HWaddr 10:78:d2:c3:98:dc
t addr:192.168.34.11 Bcast:192.168.34.63 Mask:255.255.255.1
t6 addr: fe80::590d:8e7:dc5:3d20/64 Scope:Link
BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
packets:15373 errors:0 dropped:0 overruns:0 frame:0
packets:7261 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1000
bytes:12887251 (12.8 MB) TX bytes:692419 (692.4 KB)

ik encap:Local Loopback
t addr:127.0.0.1 Mask:255.0.0.0
t6 addr: ::1/128 Scope:Host
LOOPBACK RUNNING MTU:65536 Metric:1
packets:443 errors:0 dropped:0 overruns:0 frame:0
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listens:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)

rpl-07@rpl07-ThinkCentre-A70:~$
```

- menjalankan dan menghentikan Portsentry

```
Terminal
root@rpl07-ThinkCentre-A70: /etc/init.d
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc3.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc4.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc5.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc6.d/K01portentry -> ../init.d/portentry
root@rpl07-ThinkCentre-A70: /home/rpl-07# runlevel
N 5
root@rpl07-ThinkCentre-A70: /home/rpl-07# cd /etc/init.d
root@rpl07-ThinkCentre-A70: /etc/init.d# ./portentry stop
[ OK ] Stopping portentry (via systemctl): portentry.service.
root@rpl07-ThinkCentre-A70: /etc/init.d# ps -eaf | grep -v grep | grep portentry | wc -l
0
grep -v: command not found
ps -eaf: command not found
root@rpl07-ThinkCentre-A70: /etc/init.d# ps -eaf | grep -v grep | grep portentry | wc -l
0
root@rpl07-ThinkCentre-A70: /etc/init.d# ./portentry start
[ OK ] Starting portentry (via systemctl): portentry.service.
root@rpl07-ThinkCentre-A70: /etc/init.d#

rpl-07@rpl07-ThinkCentre-A70:~$
```

```
Terminal
root@rpl07-ThinkCentre-A70: /etc/init.d
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc2.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc3.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc4.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc5.d/S02portentry -> ../init.d/portentry
lrwxrwxrwx 1 root root 20 Nov 6 09:25 /etc/rc6.d/K01portentry -> ../init.d/portentry
root@rpl07-ThinkCentre-A70: /home/rpl-07# runlevel
N 5
root@rpl07-ThinkCentre-A70: /home/rpl-07# cd /etc/init.d
root@rpl07-ThinkCentre-A70: /etc/init.d# ./portentry stop
[ OK ] Stopping portentry (via systemctl): portentry.service.
root@rpl07-ThinkCentre-A70: /etc/init.d# ps -eaf | grep -v grep | grep portentry | wc -l
0
grep -v: command not found
ps -eaf: command not found
root@rpl07-ThinkCentre-A70: /etc/init.d# ps -eaf | grep -v grep | grep portentry | wc -l
0
root@rpl07-ThinkCentre-A70: /etc/init.d#

rpl-07@rpl07-ThinkCentre-A70:~$
```

- uji coba port Scanning dengan nmap


```
Terminal
root@rpl07-ThinkCentre-A70: /etc/init.d
| wc -l
2
root@rpl07-ThinkCentre-A70: /etc/init.d# service portsentry status
● portsentry.service - LSB: # start and stop portsentry
   Loaded: loaded (/etc/init.d/portsentry; bad; vendor preset: enabled)
   Active: active (running) since Sen 2017-11-06 10:01:31 WIB; 3min 56s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 15071 ExecStop=/etc/init.d/portsentry stop (code=exited, status=0/SUC
           15165 ExecStart=/etc/init.d/portsentry start (code=exited, status=0/S
    CGroup: /system.slice/portsentry.service
            └─15177 /usr/sbin/portsentry -tcp
              15181 /usr/sbin/portsentry -udp

Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: Going into
Nov 06 10:01:31 rpl07-ThinkCentre-A70 portsentry[15181]: adminalert: PortSentry
lines 1-20/20 (END)

rpl-07@rpl07-ThinkCentre-A70:~$
@rpl07-ThinkCentre-A70: ~
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listions:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)

ThinkCentre-A70:~$ ifconfig -a
ik encap:Ethernet HWaddr 10:78:d2:c3:98:dc
t addr:192.168.34.11 Bcast:192.168.34.63 Mask:255.255.255.1
t6 addr: fe80::590d:8e7:dc05:3d20/64 Scope:Link
BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
packets:15373 errors:0 dropped:0 overruns:0 frame:0
packets:7261 errors:0 dropped:0 overruns:0 carrier:0
listions:0 txqueuelen:1000
bytes:12887251 (12.8 MB) TX bytes:692419 (692.4 KB)

ik encap:Local Loopback
t addr:127.0.0.1 Mask:255.0.0.0
t6 addr: ::1/128 Scope:Host
LOOPBACK RUNNING MTU:65536 Metric:1
packets:443 errors:0 dropped:0 overruns:0 frame:0
packets:443 errors:0 dropped:0 overruns:0 carrier:0
listions:0 txqueuelen:1
bytes:40706 (40.7 KB) TX bytes:40706 (40.7 KB)
```