

# **PRAKTIKUM KEAMANAN KOMPUTER**

## **LAPORAN 5**

### **PORTSENTRY**



**Disusun Oleh :**

<b>Nama</b>	<b>: Febriyan Fathur RF</b>
<b>NIM</b>	<b>: 1600631002</b>

**JURUSAN**

**MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2017**

## TUJUAN PEMBELAJARAN :

1. Mengenalkan pada mahasiswa tentang konsep dasar autentikasi linux
2. Memahami konsep Portsentry
3. Memahami cara menjalankan portsentry dalam linux

## Praktikum 5

- Install Portsentry  
buka terminal  
ketik `sudo` :  
install dengan cara : `apt-get install portsentry`
- melihat konfigurasi portsentry :  
`ls -l /etc/portsentry`  
ada 3 file konfigurasi portsentry yaitu :
- `nanoportsentry.conf`
  1. `nanoportsentry.ignore` : alamat ip komputer sebelumnya  
`ifconfig -a`
  2. `nanoportsentry.ignore.static`  
untuk melihat pesan yang dibuat portsentry
  3. `grep portsentry /var/log/syslog`  
kode untuk menjalankan portsentry baik manual maupun otomatis  
`ls -l /etc/init.d/portsentry`
- untuk mencari identitas id portsentry  
`find /etc/rc*.d/* -print | xargs ls -l | grep portsentry`  
`runlevel`  
N  
0 = system halt  
1 = single user  
2 = full multi user mode (default)  
3-5 = sama seperti 2  
6 = system reboot
- menjalankan dan menghentikan portsentry secara manual  
`cd /etc/init.d`  
`./portsentry stop`
- mengecek portsentry sedang jalan atau tidak  
`ps -eaf | grep -v grep | grep portsentry | wc -l`  
`./portsentry start`
- untuk melihat status portsentry  
`ps -eaf | grep -v grep | grep portsentry`
- untuk memeriksa status portsentry yang aktif  
`ps -eaf | grep -v grep | grep portsentry | wc -l`
- cek status portsentry  
`service portsentry status`

untuk melakukan scanning dari port 1 - 65535

`nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 IPTEMENNYA`

- untuk mencari data serangan yang dibuat oleh port sentry  
grep "attackalert" /var/log/syslog

## LAPORAN PRAKTIKUM 4 PORTSENTRY

### 1. Proses instalasi portsentry

```
root@rpl15-ThinkCentre-A70: /home/rpl-15
rpl-15@rpl15-ThinkCentre-A70:~$ sudo su
[sudo] password for rpl-15:
root@rpl15-ThinkCentre-A70:~# 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-4.4.0-71 linux-headers-4.4.0-71-generic linux-headers-4.4.0-72
  linux-headers-4.4.0-72-generic linux-image-4.4.0-71-generic
  linux-image-4.4.0-72-generic linux-image-extra-4.4.0-71-generic
  linux-image-extra-4.4.0-72-generic
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
0 upgraded, 1 newly installed, 0 to remove and 368 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 xential/universe amd64 portsentry amd64
  1.2-14 [64,5 kB]
Fetched 64,5 kB in 1s (44,7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package portsentry.
```

```
Untitled s now active and listening.
root@rpl15-ThinkCentre-A70:~# ls -l /etc/init.d/portsentry
-rwxr-xr-x 1 root root 2116 Okt 29 2014 /etc/init.d/portsentry
root@rpl15-ThinkCentre-A70:~# find /etc/rc*.d/* -print | xargs ls -l
| grep portsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc0.d/K01portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc1.d/K01portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc2.d/S02portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc3.d/S02portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc4.d/S02portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc5.d/S02portsentry -> ../init.d/po
rtsentry
lrwxrwxrwx 1 root root 20 Nov 6 09:20 /etc/rc6.d/K01portsentry -> ../init.d/po
rtsentry
root@rpl15-ThinkCentre-A70:~#
```



## 2. Cara konfigurasi portsentry

```
-rw-r--r-- 1 root root 11681 Okt 30 2014 portsentry.conf
-rw-r--r-- 1 root root 491 Nov 6 09:20 portsentry.ignore
-rw-r--r-- 1 root root 699 Okt 30 2014 portsentry.ignore.static
root@rpl15-ThinkCentre-A70:/home/rpl-15# nano portsentry.conf
root@rpl15-ThinkCentre-A70:/home/rpl-15# nano portsentry.ignore
root@rpl15-ThinkCentre-A70:/home/rpl-15#
```

- Untuk Konfigurasi Komputer Teman

```
rpl-15@rpl15-ThinkCentre-A70: ~
rpl-15@rpl15-ThinkCentre-A70:~$ ifconfig -a
ens32      Link encap:Ethernet  HWaddr 10:78:d2:a3:50:f7
            inet addr:192.168.34.16  Bcast:192.168.34.63  Mask:255.255.255
            inet6 addr: fe80::3484:dce3:14ef:146e/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:6340 errors:0 dropped:1 overruns:0 frame:0
            TX packets:450 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1153196 (1.1 MB)  TX bytes:38381 (38.3 KB)
```

- Hasil konfigurasi

```
root@rpl15-ThinkCentre-A70:/home/rpl-15# nano portsentry.ignore.static
root@rpl15-ThinkCentre-A70:/home/rpl-15# grep portsentry /var/log/syslog
Nov 6 09:20:48 rpl15-ThinkCentre-A70 systemd[1]: Starting LSB: # start and stop
portsentry...
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2660]: adminalert: PortSentry 1
.2 is starting.
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 1
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 11
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 15
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 79
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 111
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 119
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 143
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
isten mode on TCP port: 540
Nov 6 09:20:49 rpl15-ThinkCentre-A70 portsentry[2661]: adminalert: Going into l
```



### 3. Cara menjalankan dan menghentikan portsentry

- Untuk Menjalankan Portsentry

```
root@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/SUCCESS)
Process: 2923 ExecStart=/etc/init.d/portsentry start (code=exited, status=0/SUCCESS)
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 lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: Going into lockdown
Nov 06 10:01:34 rpl15-ThinkCentre-A70 portsentry[2939]: adminalert: PortSentry is active
Nov 06 10:01:34 rpl15-ThinkCentre-A70 systemd[1]: Started LSB: # start and stop
```

### 4. Cara ujicoba port scanning dengan nmap

```
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 dihasilkan oleh nmap

- Dalam Langkah terakhir ini kita inputkan IP Komputer teman anda

```
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
```