

Mengamankan Server dengan Portsentry

Jika server Anda sering menjadi sasaran *scanning* keamanan maupun virus jaringan, Anda perlu memasang portsentry untuk menghalau berbagai ancaman tersebut.

Portsentry merupakan salah satu program aplikasi *firewall*, yang bisa melakukan pemblokiran terhadap *user* yang mencoba melakukan scanning port sistem atau mencoba melakukan aktivitas yang “tidak terpuji”, antara lain melakukan penyusupan melalui alamat port yang ada.

Dengan adanya portsentry, semua alamat IP yang melakukan aktivitas yang dianggap “mencurigakan”, baik yang melalui port TCP maupun UDP akan segera diblokir. Sehingga semua *user* yang menggunakan alamat IP yang sama seperti warnet, perkantoran, dan anggota ISP, tidak akan bisa mengakses server kita lagi.

Download

Untuk mendapatkan program portsentry, Anda bisa mengambilnya pada situs [sourceforge.net](http://sourceforge.net/projects/sentrytools/) berikut:

Instalasi portsentry

Untuk melakukan instalasi portsentry, Anda bisa mengikuti petunjuk berikut ini:

1. Pada konsol, lakukan *login* sebagai root, seperti terlihat pada contoh berikut ini:

```
login: root
Password: password (ganti dengan password Anda)
```

2. Dengan asumsi Anda menyimpan file portsentry-1.1.tar.gz pada direktori /home/user, Anda bisa menjalankan langkah-langkah ekstraksi file berikut ini:

```
[root@localhost:~] # cd /usr/src
[root@localhost:src] # tar -zxvf /home/user/portsentry-1.1.tar.gz
```

3. Selanjutnya, Anda masuk ke direktori portsentry-1.1 dan jalankan proses kompilasi sebagai berikut:

```
[root@localhost:src] # cd portsentry-1.1
[root@localhost:portsentry-1.1] # make linux
[root@localhost:portsentry-1.1] # make install
```

Konfigurasi portsentry

Secara *default*, portsentry akan ditempatkan ke direktori: /usr/local/psionic/portsentry.

Kemudian, kita akan melakukan *setting* konfigurasi portsentry sebagai berikut:

1. Anda masih login sebagai root dan masih berada pada direktori:

```
/usr/src/portsentry-1.1
```

2. Masuk ke direktori /usr/local/psionic/portsentry, dengan mengetikkan sintaks perintah sebagai berikut:

```
[root@localhost:portsentry-1.1] # cd /usr/local/psionic/portsentry
```

3. Lakukan editing file portsentry.conf, dengan mengetikkan sintaks perintah berikut ini:

```
[root@localhost:portsentry-1.1] # vi portsentry.conf
```

4. Selanjutnya, Anda akan menjumpai isi dari file portsentry.conf, seperti berikut ini:

```
# Un-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,[...]"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,[...]"
#
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,[...]"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
```

```
#TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,[...]"
#UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
```

Baris kalimat di atas menunjukkan port-port UDP/TCP standar yang akan diblokir setiap saat ada client melakukan scanning port-port tersebut. Anda bisa menambahkan port-port yang dibuka atau port-port yang Anda khawatirkan akan di-scan atau ada pihak yang mencoba menyusup ke dalamnya.

5. Anda juga akan menjumpai baris-baris kalimat sebagai berikut:

```
IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.conf"
```

```
ignore"
HISTORY_FILE="/usr/local/
psionic/portsentry/portsentry.
history"
BLOCKED_FILE="/usr/local/
psionic/portsentry/portsentry.
blocked"
```

- IGNORE_FILE menunjukkan portsentry menempatkan file yang berisi user-user dengan alamat IP tertentu yang tetap diperbolehkan melakukan scanning sistem, misalnya dengan alasan untuk percobaan dan penelitian. Dengan demikian, jika ada scanning server dari alamat IP yang sudah terdaftar, portsentry akan mengabaikannya. File yang mencatat alamat IP dari user yang diijinkan melakukan scanning terletak pada file:

```
/usr/local/psionic/portsentry/
portsentry.ignore
```

- HISTORY_FILE merupakan konfigurasi yang menunjukkan tempat portsentry meletakkan file-file, yang berisi catatan/log dari user-user beserta alamat IP yang sudah diblokir. Isi dari log-log ini diletakkan pada:

```
/usr/local/psionic/
portsentry/portsentry.history
```

- BLOCKED_FILE merupakan konfigurasi, di mana portsentry menempatkan daftar dari user-user beserta alamat IP yang masuk dalam daftar hitam/black list dari portsentry. Daftar dari user-user beserta alamat IP ini ditempatkan pada file:

```
/usr/local/psionic/portsentry/
portsentry.blocked
```

User-user ini akan diblokir secara permanen oleh portsentry, sehingga selamanya tidak akan diizinkan untuk mengakses server Anda, sampai Anda menghapusnya dari dua file berikut:

```
/usr/local/psionic/portsentry/
portsentry.blocked
/etc/hosts.deny
```

6. Selanjutnya, Anda cari kalimat sesuai contoh di bawah ini:

```
#KILL_ROUTE="/usr/local/sbin/
```

```
iptables -I INPUT -s $TARGET$
-j DROP"
```

Kegunaan dari kalimat di atas adalah untuk memutuskan routing dari alamat-alamat IP yang terdaftar pada file: /etc/hosts.deny. Untuk mengaktifkannya, Anda bisa menghapus tanda pagar (#), yang terletak di depan kalimat tersebut. Anda juga harus memastikan jalur (path) direktori letak program iptables berada. Secara default (bawaan), iptables berada pada direktori: /sbin/. Namun jika Anda melakukan instalasi secara terpisah, program iptables akan diletakkan pada direktori: /usr/local/sbin.

7. Selain melakukan pemblokiran dengan iptables, Anda juga bisa melakukan pemblokiran dengan menggunakan tcp_wrappers, dengan menggunakan parameter sebagai berikut:

```
KILL_HOSTS_DENY="ALL: $TARGET$
# Portsentry blocked"
```

8. Selanjutnya, simpan hasil pekerjaan Anda

da dengan mengetikkan sintaks perintah sebagai berikut:

```
[Esc]:wq [Enter]
```

Membuat konfigurasi daemon

Selanjutnya, agar portsentry bisa dijalankan secara otomatis setiap saat PC dinyalakan, Anda bisa membuat skrip untuk menjalankan daemon portsentry sebagai berikut:

1. Status Anda saat ini, masih login sebagai root.
2. Pada konsol, pindah ke direktori /etc/init.d/, dengan mengetikkan sintaks perintah berikut ini:

```
[root@localhost:~] # cd /etc/
init.d/
```

3. Buat file portsentry, dengan menggunakan vi:

```
[root@localhost:~] # vi
portsentry
```

4. Isikan kalimat sebagai berikut:

```
#!/bin/bash
# Program /etc/init.d/
portsentry
```

MORE SPACE RELIABILITY & TIME & MONEY

LESS...

LINUX and FreeBSD

Features :

- Unlimited data transfer
- Complete control panels
- POP3 email, FTP access
- SSH, CGI, SQL.
- and much more...
- Start from Rp. 19.500,-/ month
- Free Setup *)
- 2 Months Free **)

Server Hosting

Features :

- Location NOC Jakarta - Indonesia (IIX)
- Size server : 1 U Rackmount
- Bandwidth : 128 kbps
- IP Address : 8 (max)
- Colocation : Rp. 1.000.000,-/ month

ALSO

- Colocation & Dedicated Server in USA
- Domain Name Register
- Benefit Reseller Program

Limited Offer :
Dedicated Server
Rp. 1.250.000,-/ mo

**"IT'S NEVER BEEN EASIER
TO TAKE YOUR BUSINESS ONLINE"**

Note : *) Transfer (restriction apply)
**) 1 year payment

CAKRAWEB
Supporting You to a Web Success

Cyber Building (d/h Elektrindo) 10 th Floor
Jl. Kuningan Barat No. 8 Jakarta Selatan 12710
Phone. (021) 526 8000 Fax. (021) 52 66 444
http://www.cakraweb.com - info@cakraweb.com

```
# copyright (c) R. Kresno Aji
<masaji@atlantisindonesia.
com>
# description: menjalankan
portsentry secara daemon,
sehingga portsentry akan \
# dijalankan secara otomatis,
setiap kali komputer
dinyalakan\
# processname: portsentry
# chkconfig: - 3 5
# pidfile: /var/run/
portsentry.pid
# config: /etc/sysconfig/
portsentry

# source function library
. /etc/init.d/functions
[ -e /etc/sysconfig/portsentry
] && . /etc/sysconfig/
portsentry

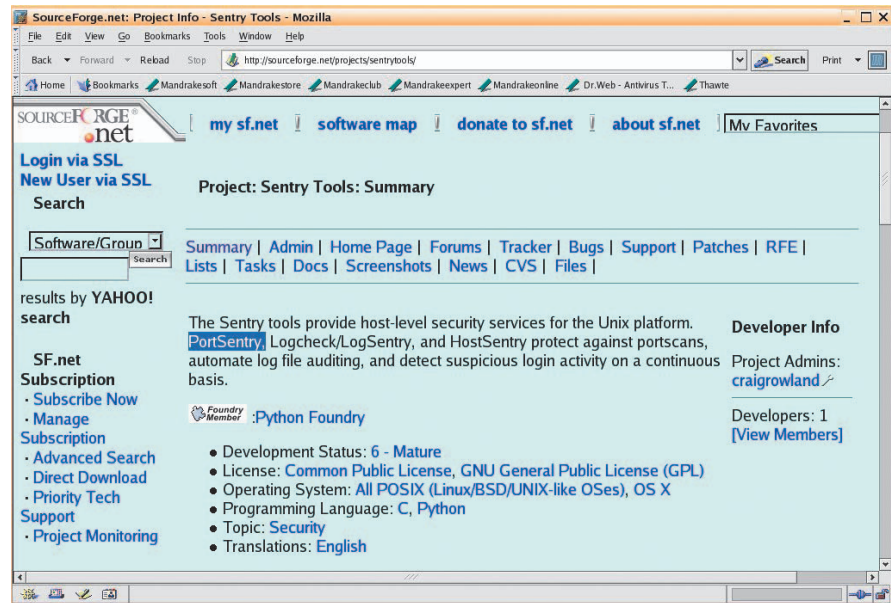
PORTSENTRY=/usr/local/psionic/
portsentry/portsentry
MODE=/etc/sysconfig/portsentry

RETVAL=0

start() {
    echo -n $"Mengaktifkan
portsentry: "
    if [ -f "$MODE" ];
    then
        . "$MODE"
    else
        echo $"(
konfigurasi
portsentry belum
ada)"
        exit 0
    fi

    if [ "$MODE" = "none"
]; then
        echo $"(
konfigurasi
portsentry belum
ada)"
        exit 0
    fi

    if [ "$MODE" = "tcp"
]; then
```



Gambar 1. Portsentry di Sourceforge.

```
MODE=tcp
fi

daemon $PORTSENTRY -
$MODE
RETVAL=$?
echo
[ $RETVAL -eq 0 ] &&
touch /var/lock/
subsys/portsentry
}

stop() {
    echo -n $"Menonaktifkan
portsentry: "
    killproc $PORTSENTRY
    RETVAL=$?

    echo
    [ $RETVAL -eq 0 ] &&
    rm -f /var/lock/
subsys/portsentry
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart|reload)
        restart
    stop
```

```
start
RETVAL=$?
;;
condrestart)
if [ -f /var/lock/subsys/
portsentry ]; then
    stop
    start
    RETVAL=$?
fi
;;
status)
status portsentry
RETVAL=$?
;;
*)
echo $"Usage: $0 {start|stop|
restart|condrestart|status}"
exit 1
esac

exit $RETVAL
```

5. Selanjutnya, simpan hasil pekerjaan Anda dengan mengetikkan sintaks perintah sebagai berikut:

```
[Esc]:wq [Enter]
```

6. Ketikkan sintaks perintah berikut ini, agar portsentry bisa berjalan secara otomatis:

```
[root@localhost:~] #
chkconfig portsentry on
```

7. Lanjutkan dengan membuat file parameter pada direktori: /etc/sysconfig/portsentry, dengan mengetikkan sintaks perintah berikut ini:

```
[root@localhost:~]# cd /etc/sysconfig
[root@localhost:~]# vi portsentry
```

8. Isikan kalimat seperti contoh berikut:

```
# Parameter dalam menjalankan portsentry
# Copyright (c) R. Kresno Aji
# <masaji@atlantisindonesia.com>
# portsentry -tcp (basic port-bound TCP mode)
# portsentry -udp (basic port-bound UDP mode)
# portsentry -stcp (Stealth TCP scan detection)
# portsentry -atcp (Advanced TCP stealth scan detection)
# portsentry -sudp ("Stealth" UDP scan detection)
# portsentportsentry.htmlry
# -audp (Advanced "Stealth" UDP scan detection)

MODE=atcp
```

9. Selanjutnya, simpan hasil pekerjaan Anda dengan mengetikkan sintaks perintah sebagai berikut:

```
[Esc]:wq [Enter]
```

10. Pada kalimat tersebut di atas, Anda bisa mengisikan mode sebagai berikut:

tcp—untuk monitoring port-port tcp standard.

udp—untuk monitoring port-port udp standard.

stcp—untuk monitoring port-port tcp dengan mode stealth.

sudp—untuk monitoring port-port udp dengan mode stealth.

atcp—untuk monitoring port-port tcp dengan mode advance.

audp—untuk monitoring port-port udp dengan mode advance.

Anda bisa mengubah isi variabel MODE, sesuai dengan kebutuhan Anda.

11. Anda bisa langsung menjalankan portsentry, dengan mengetikkan sintaks

perintah sebagai berikut:

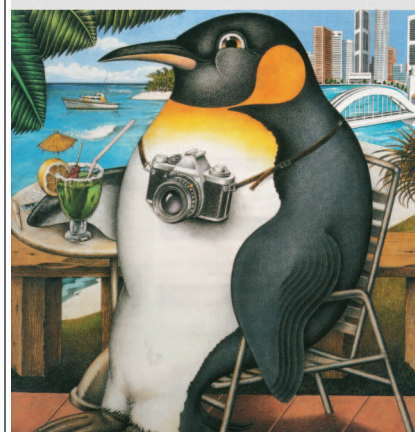
```
[root@localhost:~]# /etc/init.d/portsentry start
```

12. Sampai di sini, Anda sudah bisa mengamankan Server Anda dengan portsentry. Sebagai tambahan, berikut ini log history proses kerja dari portsentry yang selama ini berjalan di server kantor penulis:

```
1109617208 - 03/01/2005
02:00:08 Host:
81.52.197.215/81.52.197.215
Port: 42 TCP
Blocked
1109620048 - 03/01/2005
02:47:28 Host: 82.76.167.211/
82.76.167.211 Port: 22 TCP
Blocked
1109629366 - 03/01/2005
05:22:46 Host: 218.232.187.58
/218.232.187.58 Port: 22
TCP Blocked
1109630388 - 03/01/2005
05:39:48 Host: tamilxtreme.com/
213.251.132.169 Port: 22
TCP Blocked
1109634981 - 03/01/2005
06:56:21 Host: 219.238.239.10
/219.238.239.10 Port: 22
TCP Blocked
1109640274 - 03/01/2005
08:24:34 Host: ppp82.dyn190.
pacific.net.ph/210.23.190.82
Port: 443 TCP Blocked
1109643610 - 03/01/2005
09:20:10 Host: 205.209.130.210/
205.209.130.210 Port: 22
TCP Blocked
1109643912 - 03/01/2005
09:25:12 Host:
adsl-63-194-162-2.dsl.sktn01.
pacbell.net/63.194.162.2
Port: 57 TCP Blocked
1109646391 - 03/01/2005
10:06:31 Host: 210.108.91.29/
210.108.91.29 Port: 901 TCP
Blocked
1109648142 - 03/01/2005
10:35:42 Host:
ppp155.dyn170.pacific.net.
ph/210.23.170.155 Port: 443
TCP Blocked
```

R. Kresno Aji (masaji@atlantisindonesia.com)

Maintain Your Freedom!



We Keep Your Linux Systems Up & Running All The Times

Open Source All in One!

Migration, SetUp & Maintenance of Linux Systems

by the members of:

GudangLinux
Migration - Center
www.gudanglinux.net