Untuk membuat server linux yang aman tentunya banyak sekali caranya, mulai dari hardwarenya yang ada pada lokasi yang memang aksesnya terbatas seperti IDC, maupun mengamankannya secara system, yaitu dengan memasang firewall di linux , melakukan pacthing server linux , dan juga memasang anti rootkit pada server linux tersebut, dll. Tujuannya tentu adalah agar server linux kita aman dari akses yang dilakukan oleh pihak yang tidak berkepentingan.

Saat ini yang akan saya bahas adalah bagaimana caranya mengamankan server linux dengan menggunakan PortSentry. Program PortSentry ini gratis dan free, serta memiliki licensi GPL.

Portsentry merupakan tools yang digunakan untuk menghindari berbagai aktifitas scanning (terutama stealth scanning) yang dilakukan oleh hacker. Portsentry dapat mengingat ip address dari si hacker. Portsentry juga dapat membuat server kita seolah-olah menghilang dari hadapan hacker bilamana terjadi aktifitas scanning dan juga dapat memblok IP hacker tersebut juga secara otomatis. Tujuannya adalah untuk melindungi dari scanning yang dilakukan oleh pihak lain.

Berikut penjelasannya, disini saya ada 2 buah OS atau Komputer :

- IP target - 10.10.10.1 - Ubuntu
- IP Scanner - 10.10.10.2 - Centos

Pertama kali si IP Scanner melakukan scanning terhadap IP Target dengan menggunakan Nmap sebelum IP target dipasang PortSentry :

```
# nmap -sS -vv -P0 -sV 10.10.10.1

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-18 16:45 WIT
Initiating ARP Ping Scan against 10.10.10.1 [1 port] at 16:45
The ARP Ping Scan took 0.00s to scan 1 total hosts.
DNS resolution of 1 IPs took 0.00s.
Initiating SYN Stealth Scan against 10.10.10.1 [1680 ports] at 16:45
Discovered open port 322/tcp on 10.10.10.1
Discovered open port 139/tcp on 10.10.10.1
Discovered open port 445/tcp on 10.10.10.1
The SYN Stealth Scan took 1.20s to scan 1680 total ports.
Initiating service scan against 3 services on 10.10.10.1 at 16:45
The service scan took 11.01s to scan 3 services on 1 host.
Host 10.10.10.1 appears to be up ... good.
Interesting ports on 10.10.10.1:
Not shown: 1677 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
322/tcp open  ssh         (protocol 2.0)
```

445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port322-TCP:V=4.11%I=7%D=10/18%Time=4E9D4AAB%P=i686-redhat-linux-gnu%r(
SF:NULL,27,"SSH-2.0-OpenSSH_5.8p1x20Debian-7ubuntu1rn");

Nmap finished: 1 IP address (1 host up) scanned in 12.352 seconds
Raw packets sent: 1682 (74.006KB) | Rcvd: 1684 (77.478KB)

Dari hasil scan nmap terlihat bahwa pada IP Target ada 3 buah port yang terbuka, yaitu port 322 (ssh server), 445 dan 139 (samba).

Lalu kemudian si IP Target memasang PortSentry :

$ sudo apt-get install portsentry

Kemudian melakukan sedikit konfigurasi pada portsentry agar dapat melindungi dari scanning yang dilakukan oleh IP Scanner :

$ sudo pico /etc/portsentry/portsentry.conf

Cari bari ini :

0 = Do not block UDP/TCP scans.
1 = Block UDP/TCP scans.
2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="0"
BLOCK_TCP="0"

Ubah menjadi :

BLOCK_UDP="1"
BLOCK_TCP="1"

Dan juga pastikan baris ini aktif :

KILL_ROUTE="/sbin/route add -host $TARGET$ reject"

Setelah itu IP Target mengaktifkan service portsentry yang sudah di install tadi :

$ sudo /etc/init.d/portsentry start

Nah sekarang, si IP Scanner mencoba kembali melakukan scanning terhadap IP Target yang sudah dipasang PortSentry :

nmap -sS -vv -P0 -sV 10.10.10.1

nmap -sS -vv -P0 -sV 10.10.10.1

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-18 16:45 WIT
Initiating ARP Ping Scan against 10.10.10.1 [1 port] at 16:45
The ARP Ping Scan took 0.01s to scan 1 total hosts.
DNS resolution of 1 IPs took 0.01s.
Initiating SYN Stealth Scan against 10.10.10.1 [1680 ports] at 16:45
Discovered open port 32774/tcp on 10.10.10.1
Discovered open port 32773/tcp on 10.10.10.1
Discovered open port 143/tcp on 10.10.10.1
Discovered open port 79/tcp on 10.10.10.1
Discovered open port 32771/tcp on 10.10.10.1
Discovered open port 1/tcp on 10.10.10.1
Discovered open port 139/tcp on 10.10.10.1
Discovered open port 111/tcp on 10.10.10.1
Discovered open port 54320/tcp on 10.10.10.1
Discovered open port 15/tcp on 10.10.10.1
Discovered open port 445/tcp on 10.10.10.1
Discovered open port 27665/tcp on 10.10.10.1
Discovered open port 119/tcp on 10.10.10.1
Discovered open port 12345/tcp on 10.10.10.1
Discovered open port 31337/tcp on 10.10.10.1
Discovered open port 1524/tcp on 10.10.10.1
Discovered open port 1080/tcp on 10.10.10.1
Discovered open port 2000/tcp on 10.10.10.1
Discovered open port 6667/tcp on 10.10.10.1
Discovered open port 12346/tcp on 10.10.10.1
Discovered open port 322/tcp on 10.10.10.1
Discovered open port 32772/tcp on 10.10.10.1
Discovered open port 540/tcp on 10.10.10.1
Discovered open port 11/tcp on 10.10.10.1
Discovered open port 635/tcp on 10.10.10.1
The SYN Stealth Scan took 0.14s to scan 1680 total ports.
Initiating service scan against 25 services on 10.10.10.1 at 16:45
```

--- Berhenti sampai disini karena IP Scanner sudah terblokir secara otomatis oleh portsentry yang ada pada IP Target ---

Kalau dilihat sekarang, PortSentry ini banyak membuat daemon/service palsu pada server IP Target, sehingga tentunya akan menyulitkan bagi si IP Scanner untuk mencari lebih dalam dari port yang ada pada IP Target, dan juga saat ini IP Scanner telah masuk kedalam blokir atau

blacklist dari portsentry yang ada di IP Target.

PortSentry ini melakukan deteksi terhadap IP yang melakukan scanning dan kemudian melakukan blocking terhadap IP tersebut. hal ini bisa dilihat pada log yang ada di IP Target dimana portsentry berada :

```
# tail -f /var/log/syslog
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Connect from host:
10.10.10.2/10.10.10.2 to TCP port: 79
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Host: 10.10.10.2 is already blocked.
Ignoring
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Connect from host:
10.10.10.2/10.10.10.2 to TCP port: 111
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Host: 10.10.10.2 is already blocked.
Ignoring
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Connect from host:
10.10.10.2/10.10.10.2 to TCP port: 119
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Host: 10.10.10.2 is already blocked.
Ignoring
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Connect from host:
10.10.10.2/10.10.10.2 to TCP port: 143
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Host: 10.10.10.2 is already blocked.
Ignoring
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Connect from host:
10.10.10.2/10.10.10.2 to TCP port: 540
Oct 18 16:45:50 IP-Target portsentry[9621]: attackalert: Host: 10.10.10.2 is already blocked.
Ignoring
```

PortSentry ini melakukan bloking terhadap IP Scanner dan memasukannya kedalam file /etc/hosts.deny dan juga membuat routing ke IP Scanner menjadi null routing atau Network is unreachable.

Jika dilihat routingnya dari IP Target seperti ini jadinya :

```
$ route -n
10.10.0.0       0.0.0.0         255.255.0.0   U     1      0        0 eth0
10.10.10.2      -               255.255.255.255 !H    0      -        0 -
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
```

Pertanyaannya sekarang adalah bagaimana cara nya untuk merelease atau membuka blokir yang dilakukan oleh portsentry??

Caranya pertama-tama adalah membuang IP Scanner (IP yang terblokir) dari /etc/hosts.deny

dan setelah itu hapus juga routing null nya di IP Target (dimana portsentry di install) :

$ sudo route del 10.10.10.2

Lakukan juga restart service portsentry nya :

/etc/init.d/portsentry stop
Stopping anti portscan daemon: portsentry.
/etc/init.d/portsentry start
Starting anti portscan daemon: portsentry in tcp & udp mode.

Jika kita ingin menambahkan whitelist di portsentry ini dapat di masukan block IP nya kedalam file yang ada pada :

/etc/portsentry/portsentry.ignore

IP yang ditambahkan pada file tersebut diatas maka akan di abaikan oleh portsentry.