

# Metode *Port Knocking* dengan shorewall untuk membuka port SSH

By Henry Saptono <[boypyt@gmail.com](mailto:boypyt@gmail.com)>

April 2011

Pada artikel sebelumnya penulis telah menjelaskan tentang metode port knocking dengan menggunakan iptables untuk membuka dan menutup port layanan SSH. Dalam artikel kali ini penulis akan menerapkan hal yang sama namun pada sistem komputer linux yang menggunakan shorewall sebagai tool administrasi firewallnya. Dalam tulisan ini penulis tidak akan menjelaskan panjang lebar tentang apa itu shorewall, pembaca diharapkan membaca lebih detil di <http://www.shorewall.net/Documentation.html>. Penulis juga tidak akan menjelaskan panjang lebar tentang metode port knocking, karena sebelumnya juga telah dibahas dalam artikel berjudul "*Metode Port Knocking dengan iptables untuk membuka port SSH*".

Tujuan utama dari port knocking adalah untuk mencegah penyerang dari pemindaian sistem untuk layanan berpotensi dieksploitasi (seperti ssh) dengan melakukan port scanning, jika penyerang mengirimkan urutan ketukan koneksi yang salah, maka port yang dilindungi tidak akan muncul/terbuka. Untuk menerapkan metode port knocking umumnya membutuhkan suatu service atau aplikasi yang harus berjalan secara terus menerus sebagai daemon yang akan mengamati log dari firewall atas percobaan koneksi terhadap port tertentu, yang kemudian membukakan port yang dimaksud secara dinamis sesuai urutan atau aturan tertentu. Selain menggunakan suatu sistem service untuk menerapkan port knocking, kita juga dapat menggunakan solusi lainnya yang tidak terlalu bergantung dengan suatu service, yaitu menggunakan mekanisme firewall pada kernel linux.

Pada beberapa kasus mesin server linux terkadang menerapkan firewall dengan menggunakan tool administrasi firewall yaitu shorewall. Shorewall merupakan tool administrasi firewall berbasis iptables yang cukup populer di lingkungan sistem operasi linux.

## **Skenario**

Untuk memudahkan penjelasan tentang penerapan Metode *Port Knocking* dengan shorewall untuk membuka port layanan ssh, penulis membuat skenario sebagai berikut:

- Komputer yang akan diakses dan diamankan layanan ssh-nya dengan metode port knocking adalah komputer 192.168.1.212.
- Guna mengamankan service ssh pada komputer 192.168.1.212 tersebut diterapkan kebijakan firewall yang akan menolak (DROP) semua koneksi dari manapun ke komputer tersebut. Namun koneksi apapun yang berasal dari komputer 192.168.1.212 tidak ditolak (ACCEPT).
- Shorewall akan membukakan port 22 secara dinamis, jika pengguna lain dari jaringan melakukan percobaan koneksi ke **port 2222** pada komputer 192.168.1.212 sebanyak **3 kali**

- percobaan dan dalam **interval waktu 10 detik**.
- Setelah pengguna berhasil diterima koneksi ssh nya dan kemudian keluar atau mengakhiri sesi koneksi ssh, maka pengguna tidak akan dapat lagi melakukan koneksi ssh. Koneksi hanya akan bisa dilakukan lagi jika pengguna dari jaringan menghubungi terlebih dahulu **port 3333** pada komputer 192.168.1.212.
  - Komputer 192.168.1.212 ini menggunakan sistem Linux Ubuntu 10.04, dan menggunakan tool administrasi firewall yaitu shorewall versi 4.4.6.

## ***Instalasi shorewall***

Langkah pertama adalah menginstal shorewall pada komputer 192.168.1.212, dengan asumsi komputer telah terhubung dengan internet ketiklah perintah berikut:

```
root@master:~# apt-get install shorewall
```

Agar shorewall dapat diaktifkan secara otomatis setiap kali komputer booting maka edit file **/etc/default/shorewall**, kemudian ubah nilai parameter 'startup=0' menjadi **'startup=1'**.

Kemudian pastikan bahwa parameter **STARTUP\_ENABLED** pada file **/etc/shorewall/shorewall.conf** bernilai **'Yes'**.

## ***Konfigurasi dasar shorewall***

Direktori konfigurasi shorewall adalah pada direktori **/etc/shorewall**. Anda perlu membuat beberapa file konfigurasi dasar shorewall, namun untuk kemudahan Anda dapat menyalinnya dari direktori **/usr/share/doc/shorewall/default-config**. Untuk menyalin file sample konfigurasi shorewall dapat menggunakan perintah berikut ini:

```
root@master:~# cp /usr/share/doc/shorewall/default-config/* /etc/shorewall/
```

Selanjutnya, mendefinisikan zone jaringan atau segmen jaringan, dengan mengedit file **/etc/shorewall/zones**. Tambahkan entri 'net ipv4' pada akhir file tersebut, sehingga file **/etc/shorewall/zones** menjadi sebagai berikut:

```
fw    firewall
net   ipv4
```

Berikutnya mendefinisikan interface network yang terhubung dengan zone **net** yang telah didefinisikan, dengan mengedit file **/etc/shorewall/interfaces**. Tambahkan entri berikut ini pada file tersebut:

```
net   eth0
```

Kemudian mendefinisikan kebijakan default firewall. Untuk itu edit file **/etc/shorewall/policy**, dan tambahkan entri sebagai berikut:

```
fw    net    ACCEPT
```

```
net fw DROP info
all all DROP
```

sampai disini konfigurasi dasar shorewall telah selesai, kemudian aktifkan shorewall dengan perintah berikut:

```
root@master:~# shorewall start
```

## Konfigurasi shorewall untuk port knocking SSH

Langkah pertama untuk konfigurasi port knocking adalah mendefinisikan action (untuk mengetahui tentang action dalam shorewall lihat di <http://www.shorewall.net/Actions.html>) dengan nama action SSHKnock, dengan mengedit file `/etc/shorewall/actions`. Tambahkan entri berikut pada akhir baris file tersebut:

```
SSHKnock
```

Selanjutnya buatlah file kosong dengan nama file `action.SSHKnock` (ekstensi SSHKnock adalah nama yang sesuai dengan nama action yang telah Anda tentukan pada file `/etc/shorewall/actions`) seperti berikut ini:

```
root@master:~# touch /etc/shorewall/action.SSHKnock
```

Langkah berikutnya adalah membuat file `/etc/shorewall/SSHKnock` seperti berikut ini (file SSHKnock yang penulis buat ini berbasiskan contoh pada <http://www.shorewall.net/PortKnocking.html>) :

```
use Shorewall::Chains;

if ( $level ) {
    log_rule_limit( $level,
                    $chainref,
                    'SSHKnock',
                    'ACCEPT',
                    '',
                    $tag,
                    'add',
                    '-p tcp --dport 22 -m recent --rcheck --name SSHKnock ' );

    log_rule_limit( $level,
                    $chainref,
                    'SSHKnock',
                    'DROP',
                    '',
                    $tag,
                    'add',
                    '-p tcp ! --dport 22 ' );
}

add_rule( $chainref, '-p tcp --dport 22 -m recent --rcheck --hitcount 3 --seconds 10 --name SSHKnock -j ACCEPT' );
add_rule( $chainref, '-p tcp --dport 2222 -m recent --name SSHKnock --set -j DROP' );
add_rule( $chainref, '-p tcp --dport 3333 -m recent --name SSHKnock --remove -j DROP' );

1;
```

Berikutnya mendefinisikan rule spesifik untuk port knocking ssh dengan mengedit file `/etc/shorewall/rules`. Tambahkan entri berikut ini pada file tersebut.

```
SSHKnock:info net fw tcp 22,2222,3333
```

Selanjutnya restart shorewall dengan perintah berikut:

```
root@master:~# shorewall restart
```

## Uji coba

Untuk menguji konfigurasi shorewall untuk port knocking ssh, maka coba Anda akses terlebih dahulu service ssh pada komputer 192.168.1.212 dari komputer lainnya. Dapat dipastikan percobaan akses service ssh tidak akan diterima alias ditolak (dapat Anda buktikan dengan melihat log `/var/log/messages`). Kemudian cobalah perintah berikut ini untuk mengakses service ssh pada komputer 192.168.1.212 dengan mengetuk pintu port 2222 (port knocking) sebanyak 3x didalam interval waktu 10 detik. Perintah uji cobanya seperti berikut ini:

```
root@others:~# nc -w 1 192.168.1.212 2222 || nc -w 1 192.168.1.212 2222 ||  
nc -w 1 192.168.1.212 2222 || ssh 192.168.1.212
```

Jika Anda berhasil melakukan ssh, maka sesungguhnya saat ini pada komputer firewall (192.168.1.212) jika Anda lihat isi dari file `/proc/net/xt_recent/sshknock`, akan tampak list ip komputer client yang berhasil melakukan koneksi ssh.

Jika kemudian client logout dari sesi ssh pada komputer 192.168.1.212, dan kemudian mencoba melakukan ssh kembali, maka tidak akan pernah bisa, sebelum melakukan penghapusan list pada file `/proc/net/xt_recent/sshknock`, dengan cara client menghubungi port 3333 terlebih dahulu, seperti berikut ini:

```
root@others:~# nc -w 1 192.168.1.212 3333
```

Sebagai pembuktiannya coba sekarang lihat isi file `/proc/net/xt_recent/sshknock`.

**SELAMAT MENCOBA**