

MODUL 4

KONFIGURASI FIREWALL

[TCP WRAPPER]

TUJUAN PEMBELAJARAN:

1. Memperkenalkan konsep dasar firewall yang lain pada linux, yaitu tcp wrapper
2. Memahami perbedaan konsep firewall iptables dan tcp wrapper
3. Mampu mengaplikasikan tcp wrapper

DASAR TEORI

Pada sistem operasi pada umumnya mempunyai program aplikasi yang jalan pada sistem operasi tersebut. Pada sistem operasi linux, dikenal istilah service untuk menggantikan nama aplikasi secara global. Ada beberapa service yang dimanage di linux:

- Beberapa Aplikasi ditimbulkan melalui init
Service ini menyediakan dumb terminal (virtual terminal), dalam satu mesin bisa menjalankan beberapa terminal biasanya dengan menekan tombol ctrl+alt+Fx. Dikonfigurasi pada /etc/inittab. Perubahan inittab bisa diaktifkan menggunakan command `init q`
- Beberapa Service dimanage pada :
 - o System V Scripts
Merupakan metode yang paling umum digunakan untuk menaging service, Biasanya membutuhkan file konfigurasi. Service distart dengan script di /etc/init.d/. Misal untuk network :
`/etc/init.d/network restart` atau `Service network restart`
 - o inetd
Hanya beberapa service yang ada pada xinetd, service ini tidak memerlukan start/stop terhadap service. Dan file Konfigurasi yang biasa dipakai adalah :
`/etc/inetd.conf` → Top level configuration file
`/etc/init.d/inetd restart` → service specification configuration

TCP Wrapper

Merupakan salah satu pengelolaan service yang diatur pada /etc/inetd.conf dan system v scripts. Penglolaan service ini bisa melakukan blocking service tertentu kepada client atau nomor IP tertentu.

Ada dua file yang dipakai untuk melakukan blocking dan unblocking yaitu /etc/hosts.allow (diperbolehkan access) dan hosts.deny (dilarang akses)

Dengan Basic Syntax sbb :

`daemon_list: client_list [:option]`

Contoh syntax yang dipakai adalah sbb :

```
/etc/hosts.allow
vsftpd:192.168.0.
in.telnetd, portmap: 192.168.0.8
```

/etc/host.deny

sshd: ALL EXCEPT .cracker.org EXCEPT trusted.cracker.org

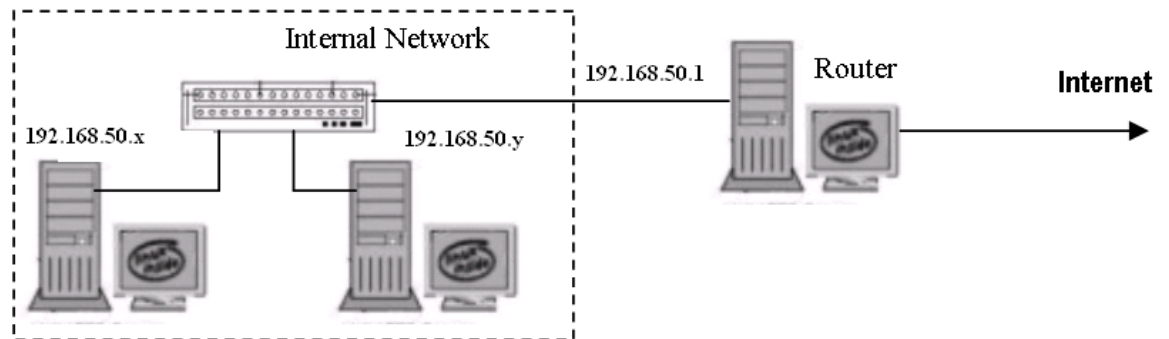
sshd: 192.168.0. EXCEPT 192.168.0.4

TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep tcp wrapper ?
2. Sebutkan fasilitas tcp wrapper yang ada di linux !
3. Sebutkan contoh konfigurasi menggunakan tcp wrapper.

PERCOBAAN

1. Bangun jaringan sebagai berikut :



NB:

Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.

192.168.50.x & y : IP dari router

2. Install paket layanan sebagai berikut pada PC Server :

Misal di kelompok 1 mendapat IP dari router sbb :

192.168.50.10 => jadikan sebagai client

192.168.50.11 => jadikan sebagai server

- a. Install telnet-server

```
# apt-get install telnetd
```

- b. Install openssh

```
# apt-get install openssh-server
```

NB :

Untuk konfigurasi telnet :

```
# vim /etc/inetd.conf
```

```
# /etc/init.d/openbsd-inetd restart
```

Untuk konfigurasi ssh :

```
# vim /etc/ssh/sshd_config
```

```
# /etc/init.d/ssh restart
```

- b. Amati dan catat, apakah paket tersebut sudah berjalan atau belum :

```
# netstat -nlptu | grep sshd => untuk ssh
```

```
# netstat -nlptu | grep inetd => untuk telnet
```

- c. Lakukan tes koneksi telnet dan ssh dari client ke server, dan pastikan berhasil.

3. Beri rule pada server sebagai berikut dan amati yang terjadi dengan melakukan akses dari client.
 - Pada **/etc/hosts.allow**
 - a. Agar telnet bisa diakses dari host 192.168.50.10, selain itu akan ditolak
in.telnetd: 192.168.50.10
in.telnetd: ALL: DENY
 - b. Agar ssh bisa diakses dari host 192.168.50.10, selain itu akan ditolak
sshd: 192.168.50.10
sshd: ALL: DENY
 - c. Uji rule tersebut, lakukan juga akses ke PC Server kelompok yang lainnya.
 - Pada **/etc/hosts.deny**, sebelumnya matikan rule pada /etc/hosts.allow dengan cara memberi tanda pagar ('#').
 - a. Agar telnet server tidak bisa diakses oleh 192.168.50.10
in.telnetd: 192.168.50.10
 - b. Agar ssh server bisa diakses dari host 192.168.50.10, selain itu akan ditolak
sshd: ALL EXCEPT 192.168.50.10
 - c. Uji rule tersebut dari client, lakukan juga akses ke PC Server kelompok yang lainnya.
 - Untuk memberi keterangan pada client, jika tidak dapat melakukan koneksi, bisa diberi keterangan dengan menggunakan twist, lakukan pada /etc/hosts.deny
in.telnetd: 192.168.1.20 : twist /bin/echo "Anda ditolak aksesnya, no ip anda adalah %a"

NB : %a menyatakan no ip client
 - Untuk mengetahui status log dari proses diatas :
tail -f /var/log/syslog
Catat hasilnya.
4. Dari rule diatas, amati yang terjadi, mana yang bisa masuk ke server telnet dan ssh dan mana yang tidak, catat di laporan.
5. Hapuslah semua rule pada langkah sebelumnya dan buat sebuah rule, dimana PC Client bisa mengakses telnet server, tetapi tidak bisa mengakses ssh server. Gunakan penggabungan rule pada kedua file /etc/hosts.allow dan /etc/hosts.deny
/etc/hosts.allow
in.telnetd: 192.168.50.10
/etc/hosts.deny
ALL : ALL

Ujilah rule anda dengan membuat pengaksesan dari client dan juga coba akses dari kelompok yang lainnya, dan tuliskan dalam laporan anda apa yang terjadi.

6. Lakukan langkah ke-5, tetapi dengan menggunakan iptables dengan terlebih dahulu menghapus semua rule di /etc/hosts.allow dan /etc/hosts.deny
7. Bandingkan hasilnya, dan buat kesimpulan sementara dari hasil percobaan diatas.

LAPORAN RESMI

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa perbedaan firewall yang ada pada iptables dan tcp wrapper, jelaskan secara singkat
3. Berdasarkan praktikum, service apa saja yang bisa diblok atau tida diblok oleh tcp wrapper?

LEMBAR ANALISA

Praktikum Network Security (Konfigurasi Firewall - TCPWrapper)

Tanggal Praktikum :

Kelas :

Nama dan NRP :

- A. Gambar topologi jaringan beserta dengan IP Addressnya
- B. Instal aplikasi telnet dan ssh pada Server dan lakukan tes koneksi dari client (poin 2)
- C. Buat rule pada Server dan uji rule tsb dengan melakukan koneksi dari client (poin 3) :
 - a. Pada file /etc/hosts.allow
 - b. Pada file /etc/hosts.deny
 - c. Memberi keterangan dengan twist
 - d. Mengetahui status log
- D. Catat dan analisa rule pada poin 5
- E. Perbandingan dengan iptables