LEMBAR PENGESAHAN

Nama Mata Kuliah	: Praktikum Keamanan Jaringan Komputer
No. Praktikum	: 04/TIK/TI.3C/PKJK/2022
Judul Praktikum	: Configurasi Firewall
Hari/Tanggal praktikum	: Kamis, 22 September 2022
Nilai	:
Link Github	:

Buketrata, 28 Oktober 2022

Mahasiswa	Dosen Pembimbing
Farah Salsabila	Muhammad Khadafi, S.T., M.T.
NIM : 2020573010022	NIP: 197507182002121004

DAFTAR ISI

MODUL 4
NETWORK SECURITY
KONFIGURASI FIREWALL(TCP WRAPPER)

4.1 Tujuan

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

4.2 Teori Dasar

Firewall adalah sebuah perangkat lunak (software) atau sistem keamanan jaringan berbasis hardware, yang mengontrol lalu lintas jaringan yang masuk dan keluar dengan cara menganalisis paket data, dan menentukan apakah mereka bisa diizinkan untuk diakses atau tidak, berdasarkan aturan setting yang telah ditetapkan sebelumnya.

Firewall biasanya sudah ada di dalam berbagai perangkat komputer, terutama di dalam Sistem operasionalnya. Sehingga memungkinkan komputer pribadi untuk menolak segala akses internet publik yang mengandung ancaman seperti virus, spam, dan lain sebagainya. Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk. Secara umum, firewall biasanya menjalankan fungsi:

Analisa dan filter paket

Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.

Bloking isi dan protocol

Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX,VBScript, Cookie.

Autentikasi koneksi dan enkripsi

Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish,IDEA dan sebagainya

Secara konseptual, terdapat dua macam firewall yaitu :

Network level

Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya Application level.

Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid.

Firewall IPTables packet filtering memiliki tiga aturan (policy), yaitu:

d.INPUT

Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. kita bias mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.

e. OUTPUT

Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuan firewall itu sendiri.

f. FORWARD

Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP. Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukkan koneksi di iptables diizinkan lewat atau tidak.

TARGET ada tiga macam yaitu:

d.ACCEPT

Akses diterima dan diizinkan melewati firewall

e. REJECT

Akses ditolak, koneksi dari komputer klien yang melewati firewall langsung terputus, biasanya terdapat pesan "Connection Refused". Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.

f. DROP

Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan – akan server yang dihubungi mengalami permasalahan teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

TCP Wrappers

Secara default redhat akan mengizinkan servis-servis tertentu (misal : telnet) dengan tanpa pembatasan. Untuk itu diperlukan pembatasan-pembatasan (proteksi) tertentu sehingga dapat mengurangi kerawanan keamanan jaringan.

Salah satu aplikasi pada sistem UNIX yang digunakan untuk melakukan packet filtering adalah TCP Wrappers. TCP Wrappers merupakan salah satu metode filter (access controllist) di sistem operasi Unix Like untuk membatasi suatu host yang ingin menggunakan service yang ada di server. Biasanya TCP Wrappers sudah terinstal secara default waktu penginstalan Linux.

Program ini bekerja dengan cara membungkus inetd (internet daemon : aplikasi yang menjalankan servis-servis internat) agar lebih aman. Sebagai contoh ada permintaan koneksi telnet dari internet, jika sistem kita tidak mempunyai tcp wrappers maka inetd akan memanggil telnetd dan session telnet akan terbentuk tanpa melakukan pembatasan apapun. Hal ini berbeda dengan TCP Wrappers yang telah terinstal, sebelum memanggil telnetd, TCP Wrapper akan memeriksa dulu berdasarkan pembatasan-pembatasan yang telah disetting kemudian memutuskan apakah koneksi tersebut akan diizinkan atau tidak. Lapisan network yang digunakan TCP Wrappers untuk memonitor dan mengontrol trafik

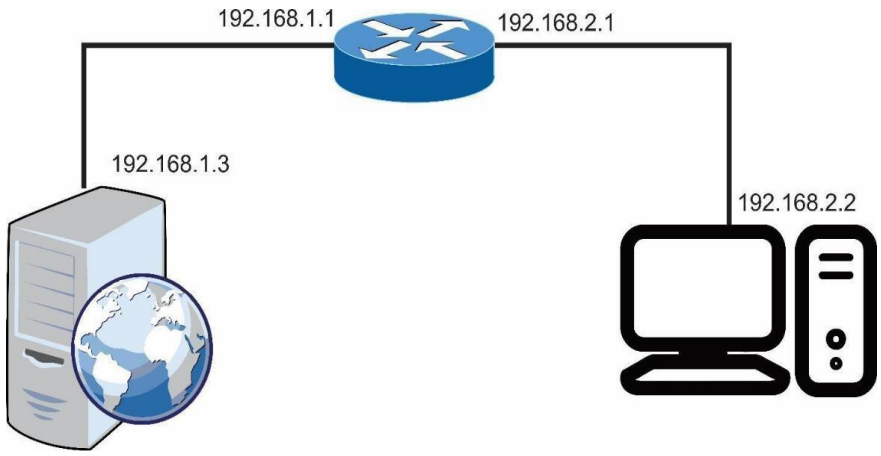
TCP di server adalah pada level aplikasi. Sistem yang menyediakan fasilitas seperti firewall. Sebuah host (dengan beberapa service) diisolasi dari jaringan luar. Fungsi yang disediakan seperti log dari request dan access control.

4.3 Kegiatan Praktikum

4.3.1 Peralatan

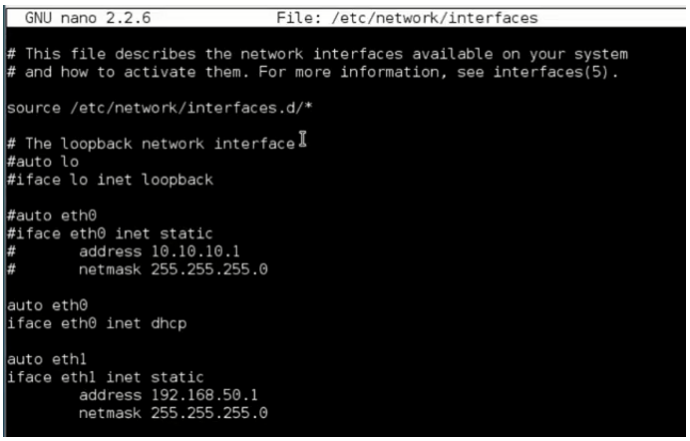
- 1 buah laptop
- Virtual Machine(VirtualBox/VMware)
- ISO : Debian dan Kali linux

4.3.2 Topologi



4.3.4 Langkah Kerja

1. Konigurasi ip pada router



2. Konfigurasi pada serve

```
 GNU nano 2.2.6                File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
#auto lo
#iface lo inet loopback

#auto eth0
#iface eth0 inet static
#       address 10.10.10.2
#       netmask 255.255.255.0
#       gateway 10.10.10.1

auto eth0
iface eth0 inet dhcp
```

3. Install paket telnet dan ssh pada Server

```
root@server:/home/setiawan# apt-get install openssh-server telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnetd is already the newest version.
openssh-server is already the newest version.
The following packages were automatically installed and are no longer required:
  libasn1-8-heimdal libgconf2-4 libgssapi3-heimdal libhcrypto4-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhx509-5-heimdal libkrb5-26-heimdal libroken18-heimdal libuuid-perl
  libwind0-heimdal
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
```

4. Mengkases server di clinet menggunakan telnet dan ssh

```
root@kali:~# telnet 192.168.50.5
Trying 192.168.50.5 ...
Connected to 192.168.50.5.
Escape character is '^]'.
Debian GNU/Linux 8
server login: coba
Password:
Last login: Tue Apr 28 05:27:31 WITA 2020 on pts/2
Linux server 3.16.0-10-amd64 #1 SMP Debian 3.16.81-1 (2020-01-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
coba@server:~$ exit
logout
Connection closed by foreign host.
root@kali:~# ssh 192.168.50.5
root@192.168.50.5's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr 28 05:27:12 2020 from 192.168.50.3
root@server:~#
```

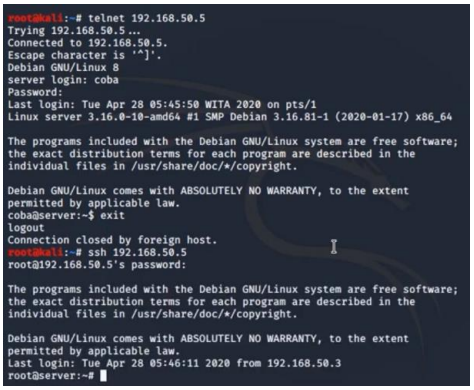
5. Mengecek apakah paket yang di install sudah jalan atau tidak pada server

```
File  Edit  View  Search  Terminal  Help
root@server:/home/setiawan# netstat -nlptu | grep sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      524/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      524/sshd
root@server:/home/setiawan# netstat -nlptu | grep inetd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      452/inetd
root@server:/home/setiawan#
```

6. Membuat rule pada server

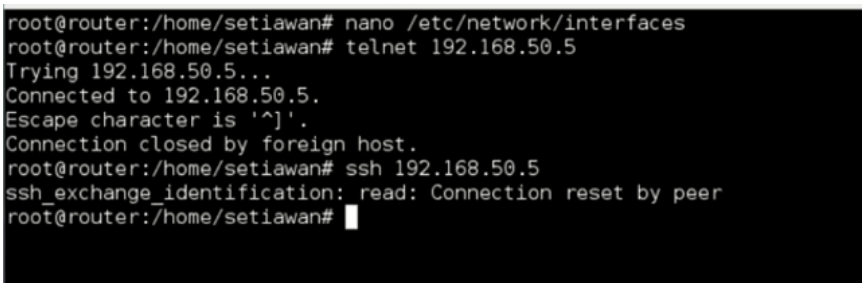
Hilangkan pagar pada rule kedua agar bisa di kases dari host yang artinya selain client tidak bisa mengakses telnet dan ssh dari server

Percobaan di client



Berhasil di akses

7. Percobaan di router



Akses di tolak oleh server

4.4 Kesimpulan

Kesimpulan dari praktek ini, saya dapat menjadikkan allow akses dan deny akses yang telah di tentukan di firewall.