Modul Praktikum 7

Firewell Host (Iptables)

Kompetensi:

- ❖ Mahasiswa memahami konsep dan penerapan firewall pada host menggunakan command iptables

Alat Dan Bahan:

- PC dengan Sistem Operasi linux debian (2 PC atau VM)
- Iptables tools

Ulasan Teori:

1. Firewall Iptables

Iptables adalah *firewall tools* dari sistem operasi linux yang dapat dijalankan dengan perintah-perintah pada *command-line / console*. Secara *default*, linux akan memperbolehkan semua *traffic* jaringan yang masuk dan keluar dari *host* linux tersebut. Jika kita ingin mengatur traffic jaringan pada host linux, kita bisa memanfaatkan tools iptables. Iptables akan memonitor dan mengelola traffic jaringan dari host maupun menuju host linux menggunakan tabel-tabel. Tabel-tabel tersebut berisi sekumpulan aturan yang disebut dengan CHAIN, yang akan menyaring paket data *incoming* maupun *outgoing*. Setiap ada paket yang cocok dengan sebuah rule/aturan yang ditetapkan, maka paket tersebut akan dilakukan aksi yang disebut dengan TARGET. Target ditetapkan bersamaan dengan rule.

Berbagai macam aksi atau TARGET yang bisa diterapkan pada paket data yang diterima, adalah :

- **ACCEPT** : menerima/memperbolehkan paket untuk lewat
- **REJECT** : packet ditolak (dapat disertai pesan ke pengirim paket tersebut)
- **DROP** : paket data ditolak (tanpa pesan)
- **LOG** : informasi packet dicatat pada log(syslog) dan dilanjutkan ke rule selanjutnya

- **DNAT** : memodifikasi alamat ip tujuan (destination ip address)
- **SNAT** : memodifikasi alamat ip sumber(source ip address)
- **MASQUERADE** : mirip SNAT dengan default source ip address = ip interface firewall (ke luar)
- Nama chain yang didefinisikan sendiri

Tabel pada iptables digunakan untuk mengelompokkan aturan-aturan yang diterapkan. Beberapa tabel yang digunakan oleh iptables antara lain adalah :

- Filter → tabel default iptables
- NAT → tabel yang digunakan untuk pemetaan alamat (alamat private ke public atau sebaliknya)
- MANGLE → tabel yg digunakan untuk mengubah paket
- RAW → tabel yang digunakan untuk menandai (mark) dari paket

Sedangkan macam-macam aturan / CHAIN yang sudah disediakan (*built-in*) pada iptable adalah :

- INPUT → semua paket menuju host yg kita setting
- OUTPUT → semua paket dari host yg kita setting
- FORWARD → semua paket yang melewati host kita (bukan dari host dan bukan menuju host kita), bisa dipakai untuk host yg memilki 2 interface dan bekerja sebagai router.
- PREROUTING → paket akan diproses sebelum proses INPUT, sering kali digunakan untuk marking paket (menandai paket)
- POSTROUTING → kebalikan dari chain PREROUTING. Paket akan diproses setelah proses lokal di host/router. Juga sering digunakan untuk menandai paket.

Setiap Tabel memiliki Chains (sekumpulan aturan) yang berbeda-beda.

TABEL	CHAINS
Filter	Input, Output, Forward
NAT	Prerouting, Postrouting, Output
Mangle	Prerouting, Postrouting, input, output, forward
Raw	Prerouting, Output

2. Menginstall iptables

Untuk dapat menggunakan tools iptables pada linux anda, pastikan bahwa iptables telah terinstall. Untuk menginstall iptables pada linux debian gunakan perintah sebagai berikut :

```
sudo apt-get updates
sudo apt-get install iptables
```

3. Perintah Umum iptables

Untuk menampilkan rule yang ada pada tabel default (tabel Filter) kita dapat menggunakan perintah :

```
sudo iptables -L
```

```
root@DosenLinux:/home/debian# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Atau untuk menampilkan rule-rule beserta nomornya, kita gunakan perintah :

```
sudo iptables -L  -line-numbers
```

```
root@DosenLinux:/home/debian# sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

4. Menambah Rule pada iptables

Untuk menambah rule pada iptables kita gunakan perintah dasar : sudo iptables -A diikuti dengan opsi / parameter tambahan seperti :

- -i (interface) → interface jaringan dimana kita ingin menyaring paket
- -p (protokol) → protokol jaringan dimana proses filtering diterapkan, seperti **tcp, udp, udplite, icmp, sctp, icmpv6** dan seterusnya. Kita juga bisa menggunakan opsi **all** untuk semua jenis protokol.
- -s (source) → alamat darimana paket datang, bisa nama host, bisa juga kita gunakan alamat IP

- -dport (destiantion port) → port tujuan paket yang ingin kita filter, seperti port 22 (untuk SSH), port 443 (https) dsb.
- -j (target / aksi) → nama target yang kita inginkan (Accept, Drop, Reject, dsb)

Jika kita terapkan, kita gunakan perintah lengkapnya dengan urutan sebagai berikut :

```
sudo iptables -A <chain> -i <interface> -p <protocol (tcp/udp) > -s
<source> --dport <port no.>  -j <target>
```

Contoh penggunaan :

- **Untuk mendrop service ssh**

  #sudo iptables -A FORWARD -p tcp --dport 22 -j DROP
- **Untuk mendrop icmp (ping) -> semuanya**

  #sudo iptables -A FORWARD -p icmp -j DROP
- **Drop icmp dari jaringan 192.168.56.0**

  #sudo iptables -A FORWARD -s 192.168.56.0/24 -p icmp -j DROP
- **Drop semuanya kecuali dari IP tertentu**

  #sudo iptables -A FORWARD -s ! 192.168.56.100 -p icmp -j DROP
- **Drop ke port 80 (http)**

  #sudo iptables -A FORWARD -p tcp --dport 80 -j DROP
- **Untuk menambah daftar**

  #sudo iptables -A FORWARD -s 192.168.56.100/32 -j DROP
- **Untuk melihat daftar**

  #sudo iptables -nL
- **Untuk menghapus daftar**

  #sudo iptables -D FORWARD -s 192.168.56.100/32 -j DROP
- **Untuk menghapus semua daftar**

  #sudo iptables -F
- **Untuk menyimpan iptables**

  #sudo iptables-save

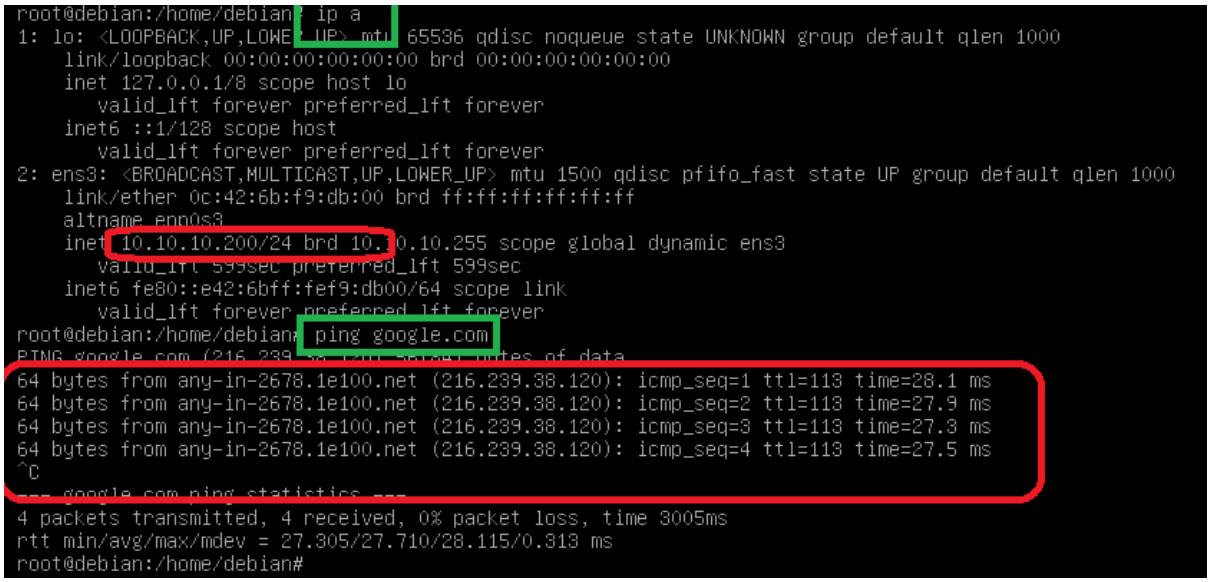
PERSIAPAN PRAKTIKUM

Untuk praktikum iptables, siapkan minimal 2 VM atau 2 PC linux debian. Bisa gunakan GNS3 dengan membuka project sesuai kelas anda.

Jika menggunakan GNS3, setelah buka project kelas anda, gunakan VM linux sesuai dengan nomor absen.

LANGKAH PRAKTIKUM

Langkah 1: Pastikan linux anda sudah terkonfigurasi jaringannya, sudah mendapatkan ip (dinamis maupun statis) dan bisa terkoneksi ke internet apabila membutuhkan instalasi paket maupun browsing.



Langkah 2: Pastikan linux anda sudah terinstal paket iptables. Jika belum, install terlebih dahulu dengan perintah :

```
#sudo apt-get update
#sudo apt-get install iptables
```

```
root@debian:/home/debian# sudo apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libip6tc2 libnetfilter-conntrack3 libnfnetlink0
Suggested packages:
  firewalld
The following NEW packages will be installed:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0
0 upgraded, 4 newly installed, 0 to remove and 24 not upgraded.
Need to get 472 kB of archives.
After this operation, 2,850 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libip6tc2 amd64 1.8.7-1 [35.0 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libnfnetlink0 amd64 1.0.1-3+b1 [13.9 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libnetfilter-conntrack3 amd64 1.0.8-3 [40.6 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 iptables amd64 1.8.7-1 [382 kB]
Fetched 472 kB in 1s (926 kB/s)
Selecting previously unselected package libip6tc2:amd64.
(Reading database ... 28155 files and directories currently installed.)
Preparing to unpack .../libip6tc2_1.8.7-1_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.7-1) ...
Selecting previously unselected package libnfnetlink0:amd64.
Preparing to unpack .../libnfnetlink0_1.0.1-3+b1_amd64.deb ...
Unpacking libnfnetlink0:amd64 (1.0.1-3+b1) ...
Selecting previously unselected package libnetfilter-conntrack3:amd64.
```

Langkah 3: Jika sudah selesai terinstal iptables, tampilkan daftar konfigurasi iptables host anda. (`sudo iptables -L` atau `sudo iptables -L --line-number`)

```
root@debian:/home/debian# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@debian:/home/debian# _
```

Disini anda akan lihat, tidak ada rule apapun dalam tabel default (tabel Filter) dari host anda.

Langkah 4: Ping ke google. Jika bisa, berarti host anda bisa terkoneksi ke internet.

```
root@debian:/home/debian# ping google
ping: google: Temporary failure in name resolution
root@debian:/home/debian# ping google.com
PING google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=114 time=27.8 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=114 time=26.9 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=114 time=26.6 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 26.632/27.120/27.785/0.486 ms
```

Langkah 5 : Tambahkan rule agar host anda tidak bisa/menerima ping dari google.com

Disini berarti kita akan membatasi (DROP) paket dengan chain INPUT (masuk ke host kita), jenis protokol ICMP (ping termasuk protokol ICMP) dan berasal dari google.com.

Maka gunakan perintah :

```
root@debian:/home/debian# sudo iptables -A INPUT -p ICMP -s google.com -j DROP
```

Langkah 6 : Sekarang coba lakukan ping ke google.com. Apakah hasilnya ? (Screenshot)

Langkah 7 : Lakukan ping ke detik.com. Apakah hasilnya ? (Screenshot)

Langkah 8 : Lihat /tampilkan isi konfigurasi iptables sekarang. (Screenshot) Apa yang berubah ? Ada rule baru ?

Langkah 9 : Hapus kembali rule yang anda gunakan untuk membatasi ping dari google. Dengan perintah :

```
root@debian:/home/debian# sudo iptables -D INPUT -p ICMP -s google.com -j DROP
_
```

Langkah 10 : Coba kembali ping dari google. Sekarang seharusnya sudah bisa kembali. (Screenshot)

TUGAS PRAKTIKUM

1. Batasi ping dari pc linux teman anda / berbeda.
2. Lakukan ssh dari pc linux teman anda ke komputer linux anda.
    i. Pastikan ssh server di komputer anda sudah terinstall dan aktif
    ii. PC Linux teman anda seharusnya tidak bisa ping tetapi bisa ssh ke komputer linux anda.
3. Tampilkan konfigurasi iptables anda sekarang.
4. Tambahkan rule agar pc linux anda tidak bisa menerima ping dari detik.com.
5. Simpan konfigurasi iptables anda dengan perintah
   `sudo /sbin/iptables-save`
6. Restart linux anda. Dan tampilkan kembali konfigurasi iptables anda. Apakah rule masih ada ?
7. Hapus semua rule iptables dengan perintah : `sudo iptables -F`
8. Restart kembali linux anda. Dan tampilkan kembali konfigurasi iptables anda. Apakah rule masih ada ?
9. Dokumentasikan langkah praktikum dan tugas praktikum dalam laporan, dan simpan file dengan format, : Kelas_Absen_Nama_Kemjar_praktikum06.pdf
   (Contoh: MI3F_23_Sofyan NA_Kemjar_praktikum06.pdf)