

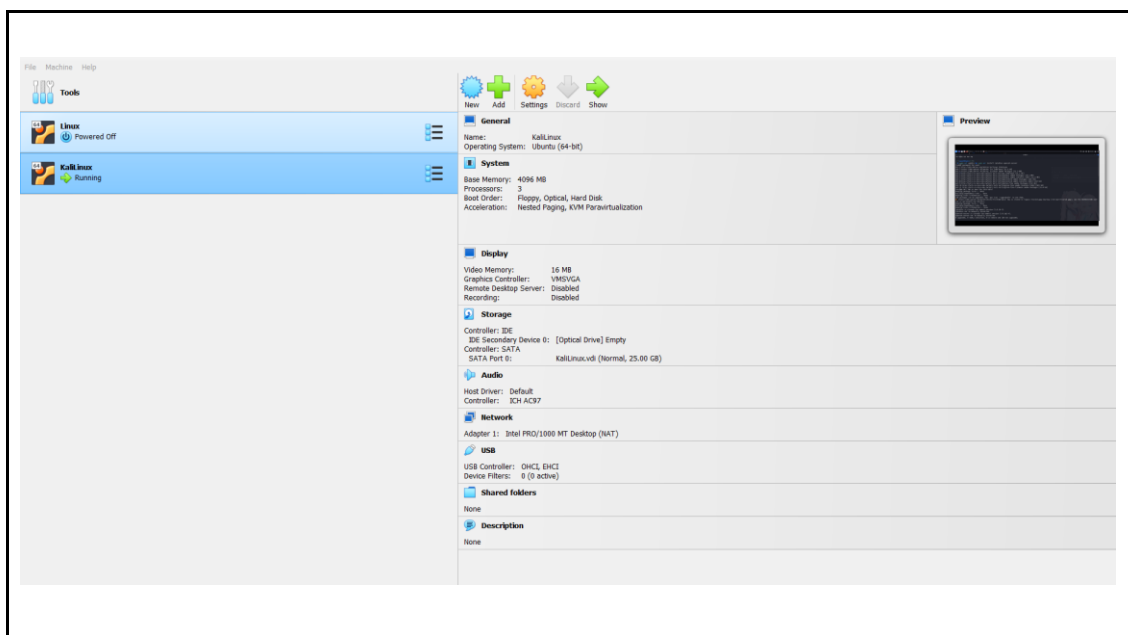


LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Langkah Praktikum

1. Lakukan instalasi sistem operasi Ubuntu (Desktop/Server) pada aplikasi Virtual Machine (VM), pastikan instance/hasil instalasinya terhubung dengan jaringan komputer Host.



2. Jalankan command berikut pada Ubuntu VM Terminal:

```
sudo apt update && sudo apt install iptables openssh server
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
└─$ sudo apt update && sudo apt install iptables openssh-server
[sudo] password for user:
Hit:1 http://deb.debian.org/debian bullseye InRelease
Get:3 http://deb.parrot.sh/parrot lts InRelease [14.6 kB]
Get:4 http://deb.parrot.sh/parrot lts/main amd64 Packages [15.5 MB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling InRelease [41.5 kB]
Get:5 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Packages [19.1 MB]
Get:6 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [44.6 MB]
Get:7 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Packages [101 kB]
Get:8 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Contents (deb) [219 kB]
Get:9 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:10 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Contents (deb) [863 kB]
Get:11 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free-firmware amd64 Packages [33.0 kB]
Fetched 80.7 MB in 1min 39s (816 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
350 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://deb.parrot.sh/parrot/dists/lts/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3).
iptables set to manually installed.
openssh-server is already the newest version (1:9.6p1-4).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 350 not upgraded.
```

1 Nama : Dani Adrian
2 NIM : 225150201111009
3

Penjelasan :

- `sudo apt update`: Memperbarui daftar paket di repository untuk memastikan bahwa informasi terbaru tentang paket yang tersedia sudah diperoleh.
- `sudo apt install iptables openssh-server`: Menginstal paket `iptables` (perangkat lunak firewall) dan `openssh-server` (untuk mengaktifkan layanan SSH pada mesin Anda).

3. Jalankan command iptables pada Ubuntu VM Terminal:

```
sudo iptables -L -v
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali):~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
0 0 DOCKER-USER all -- any any anywhere          anywhere
0 0 DOCKER-ISOLATION-STAGE-1 all -- any any anywhere          anywhere
0 0 ACCEPT all -- any docker0 anywhere          anywhere
0 0 DOCKER all -- any docker0 anywhere          anywhere
0 0 ACCEPT all -- docker0 !docker0 anywhere          anywhere
0 0 ACCEPT all -- docker0 docker0 anywhere          anywhere
0 0 ACCEPT all -- any br-6997956cef8a anywhere          anywhere
0 0 DOCKER all -- any br-6997956cef8a anywhere          anywhere
0 0 ACCEPT all -- br-6997956cef8a !br-6997956cef8a anywhere          anywhere
0 0 ACCEPT all -- br-6997956cef8a br-6997956cef8a anywhere          anywhere
0 0 ACCEPT all -- any br-f541ac2194a9 anywhere          anywhere
0 0 DOCKER all -- any br-f541ac2194a9 anywhere          anywhere
0 0 ACCEPT all -- br-f541ac2194a9 !br-f541ac2194a9 anywhere          anywhere
0 0 ACCEPT all -- br-f541ac2194a9 br-f541ac2194a9 anywhere          anywhere
0 0 DOCKER all -- any br-ce32bd2847b2 anywhere          anywhere
0 0 ACCEPT all -- any br-ce32bd2847b2 !br-ce32bd2847b2 anywhere          anywhere
0 0 ACCEPT all -- br-ce32bd2847b2 br-ce32bd2847b2 anywhere          anywhere
0 0 ACCEPT all -- any br-8017fe66e144 anywhere          anywhere
0 0 DOCKER all -- any br-8017fe66e144 anywhere          anywhere
0 0 ACCEPT all -- br-8017fe66e144 !br-8017fe66e144 anywhere          anywhere
0 0 ACCEPT all -- br-8017fe66e144 br-8017fe66e144 anywhere          anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
```

Penjelasan :

Chain INPUT:

- Policy: ACCEPT (kebijakan default adalah menerima semua paket)
- Chain ini berlaku untuk paket-paket yang menuju ke lokal mesin.

Chain FORWARD:

- Policy: DROP (kebijakan default adalah menolak semua paket)
- Chain ini berlaku untuk paket-paket yang diteruskan melalui mesin, biasanya jika mesin tersebut bertindak sebagai router atau gateway.

Chain OUTPUT:

- Policy: ACCEPT (kebijakan default adalah menerima semua paket)
- Chain ini berlaku untuk paket-paket yang berasal dari lokal mesin.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

4. Jalankan command iptables berikut, dan cobalah melakukan koneksi ssh.

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

```
(user@kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP

(user@kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 68 packets, 5256 bytes)
 pkts bytes target     prot opt in     out     source                   destination
  0      0 DROP      tcp  --  any    any    anywhere                tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source                   destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target     prot opt in     out     source                   destination
```

Penjelasan :

Command `sudo iptables -L -v`:

- `sudo`: perintah dieksekusi dengan hak superuser (root).
- `iptables`: Perintah untuk mengonfigurasi aturan penyaringan paket dalam kerangka kerja netfilter Linux.
- `-L`: "list" untuk menampilkan semua aturan dalam suatu rantai atau semua rantai.
- `-v`: "verbose" untuk menampilkan informasi detail tentang setiap aturan, termasuk jumlah paket dan byte.

5. Melalui VM, cobalah mengakses ssh anda

```
ssh <USERNAME>@<IP LOCAL>
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:14:67:d1 brd ff:ff:ff:ff:ff:ff
   inet 192.168.100.53/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 86021sec preferred_lft 86021sec
   inet6 fe80::a00:27ff:fe14:67d1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: br-6997956cef8a: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
   link/ether 02:42:6e:18:29:10 brd ff:ff:ff:ff:ff:ff
   inet 172.19.0.1/16 brd 172.19.255.255 scope global dynamic noprefixroute br-6997956cef8a
       valid_lft forever preferred_lft forever
   inet6 fe80::42:6eff:fe18:2910/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: vx-8017fe66e144: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
   link/ether 02:42:6e:18:29:10 brd ff:ff:ff:ff:ff:ff
   inet 172.19.0.2/16 brd 172.19.255.255 scope global dynamic noprefixroute vx-8017fe66e144
       valid_lft forever preferred_lft forever
   inet6 fe80::42:6eff:fe18:2910/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
(user@kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP

Chain INPUT (policy ACCEPT 68 packets, 5256 bytes)
  pkts bytes target     prot opt in     out     source            destination
    0      0 DROP      tcp  --  any    any    anywhere          anywhere            tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain DOCKER (0 references)
  pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
  pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
  pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-USER (0 references)
  pkts bytes target     prot opt in     out     source            destination
```

Penjelasan :

Konfigurasi iptables yang ditampilkan menunjukkan bahwa lalu lintas TCP masuk ke port 22 (SSH) sedang ditolak. Ini berarti bahwa segala upaya koneksi SSH ke server (Kali) akan diblokir oleh firewall, menyebabkan kesalahan timeout.

6. Sekarang, jalankan command berikut dan lakukan kembali koneksi ssh.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT
```

```
(user@kali)-[~]
$ sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT

(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 113 packets, 8700 bytes)
 pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT     tcp  --  any    any    anywhere          anywhere          tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-USER (0 references)
 pkts bytes target     prot opt in     out     source            destination
```

Penjelasan :

Command `sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT`:

- `sudo`: Perintah dieksekusi dengan hak superuser (root).
- `iptables`: Perintah untuk mengonfigurasi aturan penyaringan paket dalam kerangka kerja netfilter Linux.
- `-R INPUT 1`: Menunjukkan kita ingin mengganti aturan pertama (indeks 1) dalam rantai INPUT dengan aturan baru yang ditentukan. `-R` digunakan untuk mengganti aturan, INPUT adalah rantai yang dituju, dan 1 adalah indeks aturan yang ingin diganti.
- `-p tcp`: Menentukan protokol yang akan diterapkan aturan, dalam hal ini TCP.
- `--dport 22`: Menentukan port tujuan, yaitu port 22 (SSH).



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

- -j ACCEPT: Menentukan tindakan yang harus diambil jika paket cocok dengan aturan (ACCEPT) paket.

Perintah tersebut mengganti aturan pertama dalam rantai INPUT dengan aturan baru yang memungkinkan lalu lintas TCP masuk ke port 22 (SSH).

7. Melalui VM, cobalah mengakses ssh anda

```
ssh <USERNAME>@<IP LOCAL>
```

```
(user@kali)-[~]
$ sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT
(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 113 packets, 8700 bytes)
 pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT    tcp  --  any    any    anywhere          tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-USER (0 references)
 pkts bytes target     prot opt in     out     source            destination

(user@kali)-[~]
$
```

```
1 Nama : Dani Adrian
2 NIM : 225150201111009
3
```

```
PS C:\Users\USER> ssh user@192.168.100.53
The authenticity of host '192.168.100.53 (192.168.100.53)' can't be established.
ED25519 key fingerprint is SHA256:Mg96u7EPuDCr4kKcbL05SrYS5089bfYJisNid+dtHwC.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.53' (ED25519) to the list of known hosts.
user@192.168.100.53's password:
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 12 21:07:45 2024 from 10.0.2.15
(user@kali)-[~]
$
```

Penjelasan :
Koneksi SSH berhasil karena aturan iptables telah diubah untuk mengizinkan lalu lintas TCP masuk ke port 22. Sebelumnya, aturan pertama dalam rantai INPUT adalah untuk menolak lalu lintas SSH masuk. Setelah aturan diubah dengan perintah `sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT`, lalu lintas SSH masuk diizinkan dan koneksi berhasil terbentuk.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

8. Jalankan command berikut untuk menghapus semua rules.

```
sudo iptables -F
```

Sebelum :

```
(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 113 packets, 8700 bytes)
 pkts bytes target    prot opt in     out     source    destination
  0      0 ACCEPT    tcp  --  any    any    anywhere  tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-USER (0 references)
 pkts bytes target    prot opt in     out     source    destination
```

Sesudah :



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ sudo iptables -F

(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 254 packets, 20580 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain DOCKER (0 references)
 pkts bytes target    prot opt in     out     source            destination
Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target    prot opt in     out     source            destination
Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target    prot opt in     out     source            destination
Chain DOCKER-USER (0 references)
 pkts bytes target    prot opt in     out     source            destination
```

Penjelasan :

-F: Berarti "flush" dan digunakan untuk menghapus semua aturan dalam semua rantai iptables.

Kesimpulan

Langkah pertama adalah menginstal paket iptables dan OpenSSH server. Hal ini untuk mengatur aturan firewall menggunakan iptables dan untuk memungkinkan akses SSH ke sistem agar dapat diuji. iptables dilakukan dengan menjalankan perintah `sudo iptables -L -v`, memberikan gambaran tentang aturan-aturan yang ada dalam konfigurasi firewall iptables. Aturan iptables kemudian ditambahkan untuk menolak koneksi SSH masuk dengan menutup port 22 menggunakan perintah `sudo iptables -A INPUT -p tcp --dport 22 -j DROP`, tujuannya untuk menguji kemampuan iptables dalam memblokir jenis koneksi tertentu. Selanjutnya, percobaan praktikum dilakukan untuk mengakses SSH



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

setelah aturan baru diterapkan, menguji efektivitas pemblokiran. Terakhir, aturan iptables diubah kembali untuk mengizinkan koneksi SSH masuk dengan membuka port 22 menggunakan perintah `sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT`, dan percobaan praktikum koneksi SSH kembali dilakukan untuk memastikan perubahan berhasil. Setelah semua percobaan selesai, semua aturan iptables dihapus menggunakan perintah `sudo iptables -F` untuk membersihkan konfigurasi iptables.

Evaluasi

1. Jelaskan apa yang dimaksud dengan **chain** pada firewall, dan berikan contoh masing-masing implementasinya menggunakan iptables.

Chain dalam firewall adalah serangkaian aturan yang diterapkan secara berurutan pada paket data yang melewati titik tertentu dalam sistem. Setiap chain memiliki tujuan dan fungsi spesifik dalam mengelola lalu lintas jaringan. Dalam konteks iptables, ada tiga chain utama yang biasanya digunakan:

- a. INPUT Chain: Chain ini bertanggung jawab untuk mengelola paket data yang ditujukan untuk sistem lokal atau server. Paket data yang masuk dari luar jaringan dan ditujukan langsung ke sistem akan diperiksa oleh aturan-aturan dalam chain INPUT.

Contoh Implementasi dengan iptables:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 4329 packets, 337K bytes)
 pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT     tcp  --  any    any    anywhere          tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 238 packets, 38739 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target     prot opt in     out     source            destination

Chain DOCKER-USER (0 references)
 pkts bytes target     prot opt in     out     source            destination

(user@kali)-[~]
$
```

~/Desktop/documentnama - Mo
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3

Aturan di atas mengizinkan koneksi SSH masuk ke sistem dengan membuka port 22 dalam chain INPUT.

- b. FORWARD Chain: Chain ini mengelola paket data yang melewati sistem dan diarahkan ke tujuan lain. Biasanya digunakan dalam konfigurasi routing atau sebagai gateway.

Contoh Implementasi dengan iptables:

```
sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 4334 packets, 338K bytes)
 pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    tcp  --  any    any     anywhere  anywhere    tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    all  --  eth0   eth1    anywhere  anywhere

Chain OUTPUT (policy ACCEPT 238 packets, 38739 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target    prot opt in     out     source    destination

Chain DOCKER-USER (0 references)
 pkts bytes target    prot opt in     out     source    destination

(user@kali)-[~]
```

~/Desktop/documentnama - Mo
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3|

Aturan di atas mengizinkan paket data yang masuk dari antarmuka eth0 dan keluar dari antarmuka eth1 untuk melalui sistem dalam chain FORWARD.

- c. **OUTPUT Chain:** Chain ini mengelola paket data yang dibuat oleh sistem lokal dan dikirimkan ke luar jaringan. Ini berarti paket data yang keluar dari sistem akan diperiksa oleh aturan-aturan dalam chain OUTPUT.

Contoh Implementasi dengan iptables:

```
sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 4339 packets, 338K bytes)
pkts bytes target      prot opt in     out     source            destination
0      0 ACCEPT      tcp  --  any    any     anywhere          anywhere          tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
0      0 ACCEPT      all  --  eth0   eth1    anywhere          anywhere

Chain OUTPUT (policy ACCEPT 238 packets, 38739 bytes)
pkts bytes target      prot opt in     out     source            destination
0      0 ACCEPT      udp  --  any    any     anywhere          anywhere          udp dpt:domain

Chain DOCKER (0 references)
pkts bytes target      prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
pkts bytes target      prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
pkts bytes target      prot opt in     out     source            destination

Chain DOCKER-USER (0 references)
pkts bytes target      prot opt in     out     source            destination

(user@kali)-[~]
```

Aturan di atas mengizinkan koneksi DNS keluar dari sistem dengan membuka port 53 dalam chain OUTPUT.

2. Buatlah firewall rules untuk memblokir masuknya data dari port 20, 21, 1337, dan 3306 oleh local ip address 192.168.17.5 dalam satu rule (satu perintah command line) iptables. (hint: gunakan perintah berikut sebagai dasarnya: **sudo iptables -A OUTPUT -s <IP address> -j DROP**)

```
(user@kali)-[~]
$ sudo iptables -A OUTPUT -s 192.168.17.5 -p tcp --match multiport --dports 20,21,1337,3306 -j DROP

(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1317 packets, 104K bytes)
pkts bytes target      prot opt in     out     source            destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
0      0 DROP       tcp  --  any    any     192.168.17.5      anywhere          multiport dports ftp-data,ftp,1337,mysql
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Penjelasan :

Perintah ini menambahkan aturan ke chain OUTPUT pada firewall menggunakan iptables. Aturan ini bertujuan untuk menolak semua paket TCP yang berasal dari alamat sumber 192.168.17.5 dan menuju ke beberapa port tertentu yang ditentukan. Port-port yang ditentukan adalah 20 (FTP data), 21 (FTP), 1337, dan 3306 (MySQL). Aturan ini akan menolak semua paket TCP yang berasal dari 192.168.17.5 dan menuju salah satu dari port-port yang telah ditentukan.

3. Buatlah firewall rules untuk mem-forward dan menerima input dari port 443 dan menolak input dari port 80 (boleh dibuat dalam multiple rules).

```
(user@kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
(user@kali)-[~]
$ sudo iptables -A FORWARD -p tcp --dport 443 -j ACCEPT
(user@kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 80 -j REJECT
(user@kali)-[~]
$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1384 packets, 109K bytes)
 pkts bytes target     prot opt in     out     source            destination
    0      0 ACCEPT     tcp  --  any    any    anywhere          anywhere
    0      0 REJECT     tcp  --  any    any    anywhere          anywhere          tcp dpt:https
                                tcp dpt:http reject-with icmp-port-unreachable

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination
    0      0 ACCEPT     tcp  --  any    any    anywhere          anywhere          tcp dpt:https

Chain OUTPUT (policy ACCEPT 1 packets, 71 bytes)
 pkts bytes target     prot opt in     out     source            destination
```

Penjelasan :

Chain INPUT:

- Aturan pertama (ACCEPT): Mengizinkan koneksi TCP ke port 443 (HTTPS) dari mana pun.



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

- Aturan kedua (REJECT): Menolak koneksi TCP ke port 80 (HTTP) dari mana pun dan memberikan respons ICMP "port unreachable" sebagai tanggapan atas penolakan tersebut.

Chain FORWARD:

- Aturan mengizinkan koneksi TCP ke port 443 (HTTPS) dari mana pun.

Chain OUTPUT:

- Kebijakan defaultnya adalah menerima semua paket keluar.

Dengan konfigurasi ini, firewall akan mengizinkan koneksi HTTP (port 80) hanya jika tujuan akhirnya adalah untuk HTTPS (port 443). Selain itu, semua koneksi HTTPS (port 443) diizinkan, baik itu untuk lalu lintas INPUT maupun FORWARD. Tidak ada pembatasan pada lalu lintas OUTPUT, yang berarti sistem dapat mengirimkan paket ke mana pun tanpa hambatan dari firewall.

Kesimpulan

Pada langkah-langkah percobaan tersebut, dilakukan konfigurasi dan uji coba pengaturan iptables pada sebuah Ubuntu Virtual Machine (VM). Instalasi paket iptables dan openssh-server dilakukan untuk mengatur aturan firewall dan mengaktifkan layanan SSH. Melalui perintah `sudo iptables -L -v`, konfigurasi iptables saat ini diperiksa untuk melihat aturan-aturan yang ada. Pemblokiran koneksi SSH dilakukan dengan menambahkan aturan pada chain INPUT menggunakan perintah `sudo iptables -A INPUT -p tcp --dport 22 -j DROP`, yang diharapkan mengakibatkan kegagalan akses SSH. Setelahnya, koneksi SSH diizinkan kembali dengan mengubah aturan pada chain INPUT menggunakan perintah `sudo iptables -R INPUT 1 -p tcp --dport 22 -j ACCEPT`, dan



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : KEAMANAN JARINGAN
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 09/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

dilakukan uji coba koneksi SSH kembali yang diharapkan berhasil. Seluruh aturan iptables kemudian dihapus dengan perintah `sudo iptables -F` untuk membersihkan konfigurasi iptables. Chain pada firewall merupakan serangkaian aturan yang diterapkan pada paket data yang melewati titik tertentu dalam sistem firewall, dengan contoh implementasinya menggunakan iptables pada chain INPUT, FORWARD, dan OUTPUT. Selanjutnya, untuk memblokir masuknya data dari port 20, 21, 1337, dan 3306 oleh local IP address 192.168.17.5, sebuah rule dapat dibuat dengan perintah `sudo iptables -A OUTPUT -s 192.168.17.5 -p tcp --match multiport --dports 20,21,1337,3306 -j DROP`. Terakhir, aturan-aturan untuk mem-forward dan menerima input dari port 443 serta menolak input juga dijelaskan dalam konteks penggunaan iptables.

Evaluasi

Rangkaian praktikum Keamanan Jaringan telah berhasil dijalankan dengan baik

