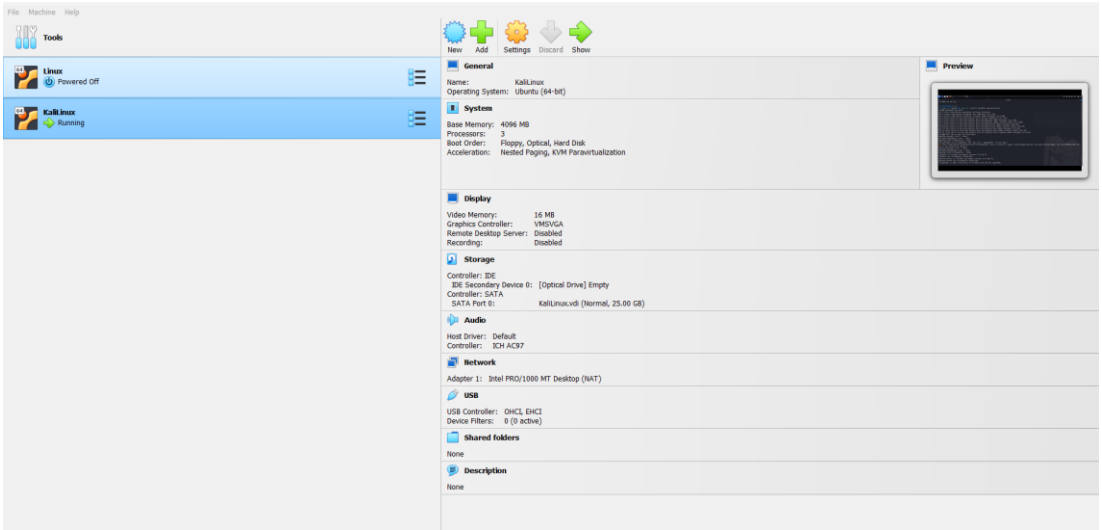
LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

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.

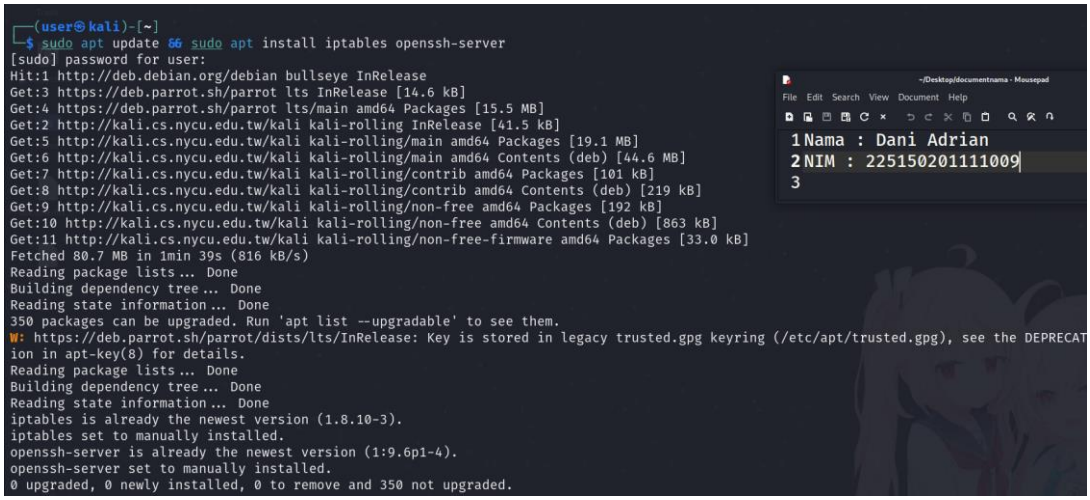


2. Jalankan command berikut pada Ubuntu VM Terminal:

```
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



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

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.

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
```

Penjelasan :

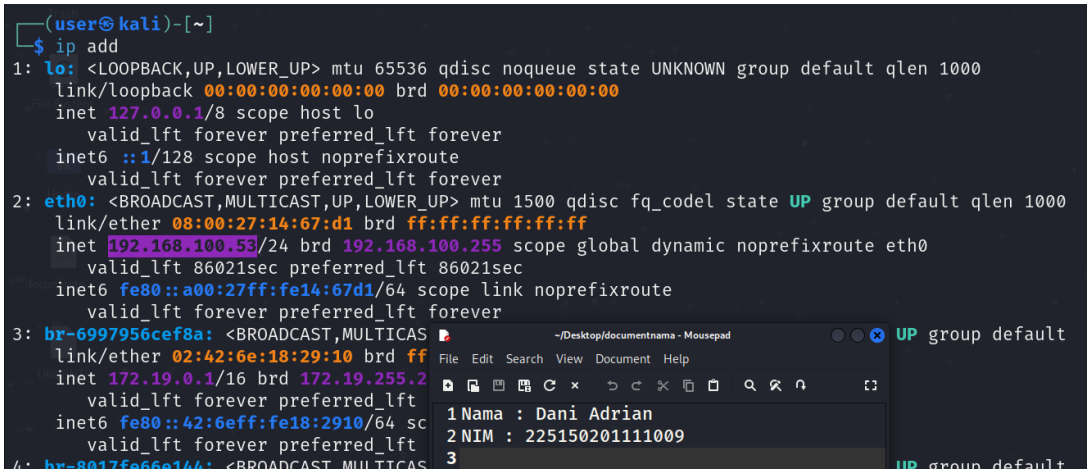
Command `sudo iptables -L -v`:

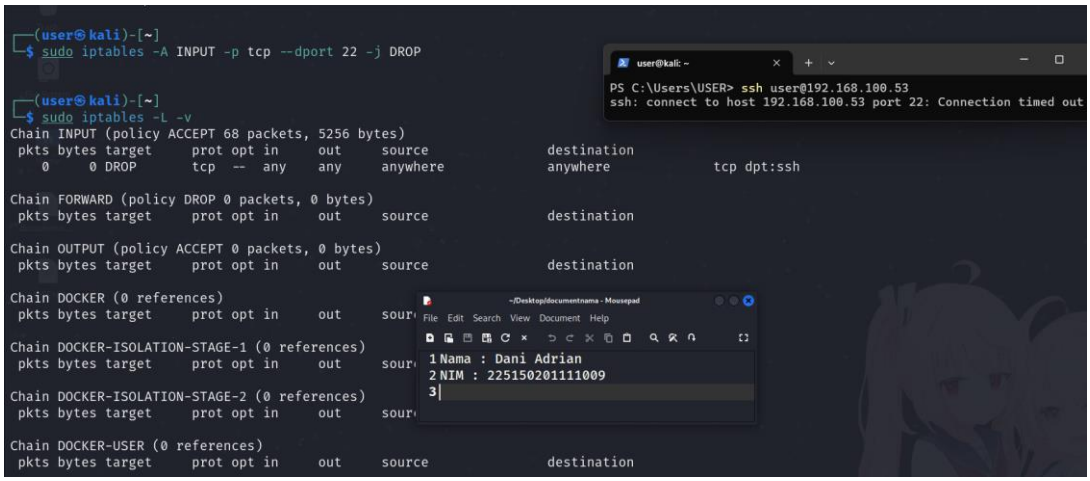
- `sudo`: perintah dieksekusi dengan hak superuser (root).
- `iptables`: Perintah untuk mengonfigurasi aturan penyaringan paket dalam kerangka kerja netfilter Linux.
- `-L`: "`list`" untuk menampilkan semua aturan dalam suatu rantai atau semua rantai.
- `-v`: "`verbose`" untuk menampilkan informasi detail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

5. Melalui VM, cobalah mengakses ssh anda

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

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





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
```

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).

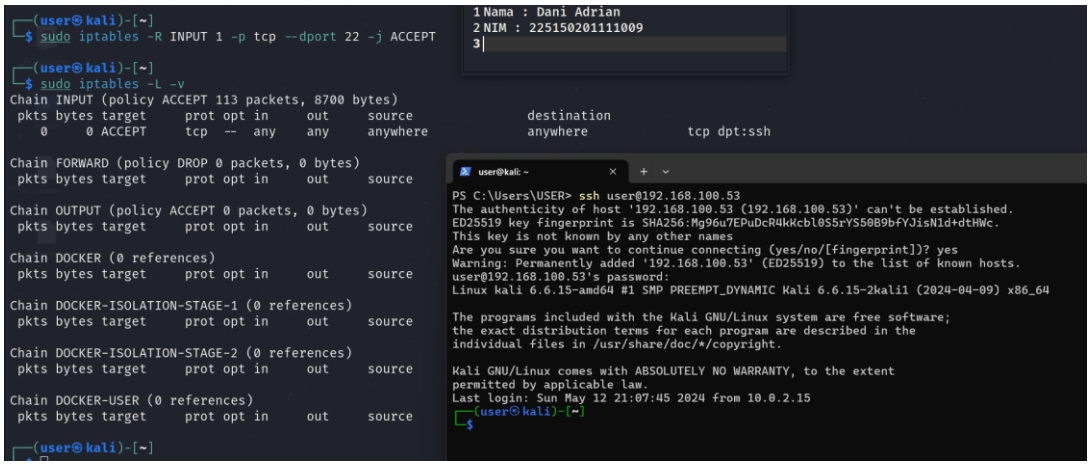
BAB	: KEAMANAN JARINGAN
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 09/05/2024
ASISTEN	: Bernas Cakra Sakti Harisna Mohammad Seto Aji Pamungkas

- `-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>
```



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.

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.

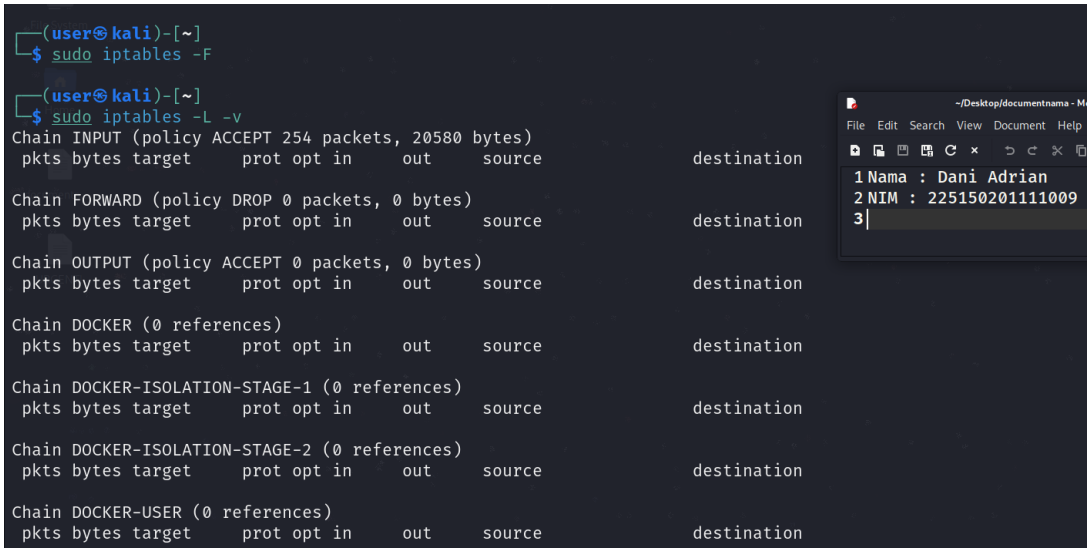
```
sudo iptables -F
```

Sebelum :

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



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

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
```

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

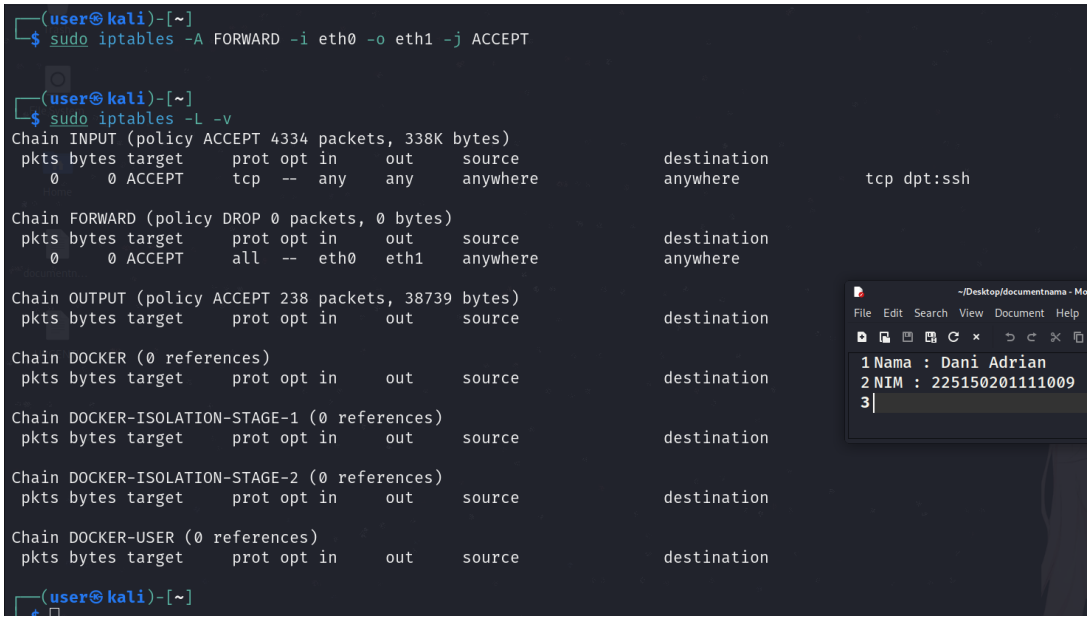
Aturan di atas mengizinkan koneksi SSH masuk ke sistem dengan membuka port 22 dalam chain INPUT.

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
```

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



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

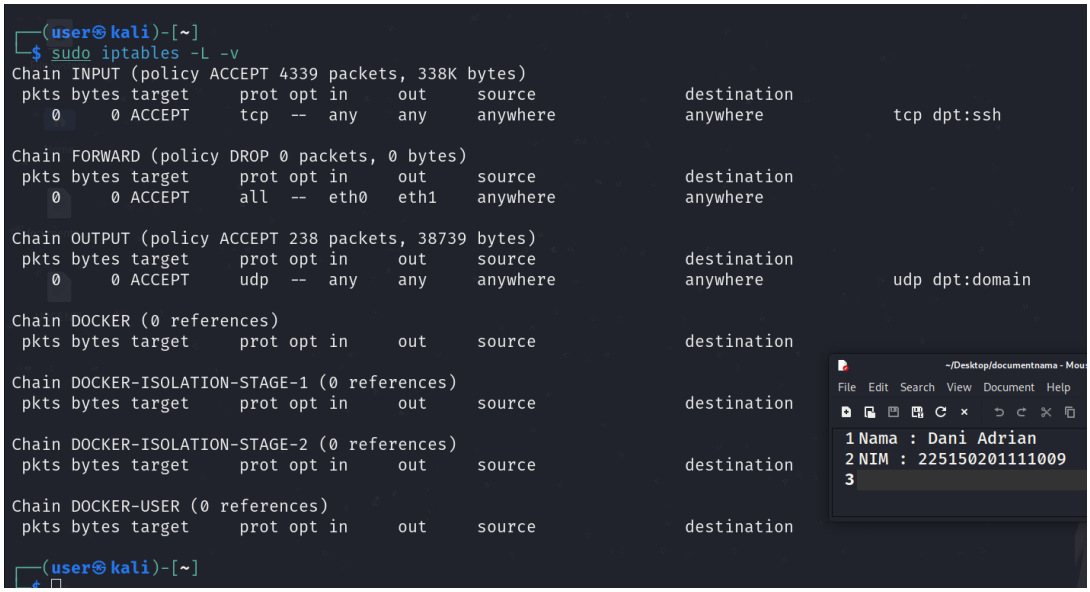
c. OUTPUT Chain: Chain ini mengelola paket data yang dibuat oleh sistem lokal dan dikirimkan ke luar jaringan. Ini berarti paket data yang keluar dari sistem akan diperiksa oleh aturan-aturan dalam chain OUTPUT.

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



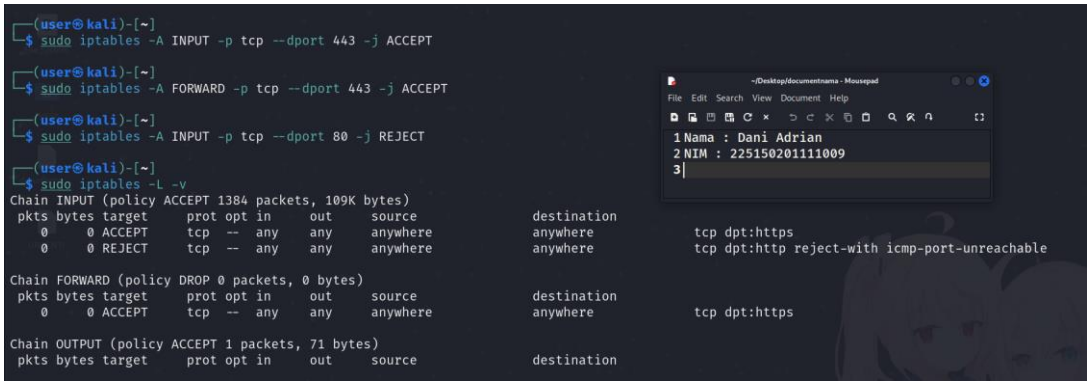
Aturan di atas mengizinkan koneksi DNS keluar dari sistem dengan membuka port 53 dalam chain OUTPUT.

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**)

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).



Penjelasan :

Chain INPUT:

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

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

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