KEAMANAN JARINGAN

8.1. DASAR TEORI

Pertahanan terhadap risiko-risiko serangan pada suatu jaringan dapat diupayakan menggunakan peralatan dasar seperti Firewall. Firewall dapat melakukan pengendalian atas trafik yang melewatinya, dengan cara mengizinkan/menolak trafik-trafik jaringan tersebut. Perangkat Firewall biasa diletakkan di antara jaringan internal (jaringan lokal) dan jaringan luar (misalnya internet), ataupun antar jaringan internal (Kim & Solomon, 2021). Firewall berperan penting dalam pertahanan jaringan, meski bukan satu-satunya mekanisme yang perlu diterapkan untuk mengupayakan keamanan.

Terminologi “firewall” dapat berarti perangkat keras maupun perangkat lunak tertentu yang menjalankan fungsionalitas sebagai filter terhadap traffic,

afik yang tidak diizinkan melewati titik tertentu di jaringan. Firewall sering diimplementasikan menggunakan **iptables**, sebuah program dalam ranah user space untuk Linux 2.4.x dst. yang memungkinkan pengaturan penyaringan trafik menggunakan sekumpulan aturan (ruleset). Dalam iptables, aturan-aturan yang didefinisikan pada firewall ditulis dalam “**tables**”, dan tiap kombinasi aturannya disebut sebagai “**chains**”, yang akan memfilter paket data dari trafik yang masuk maupun keluar ke/dari suatu jaringan tempat firewall diimplementasikan.

Ketika suatu paket data cocok dengan aturan/rules yang tertera, ia akan diperlakukan dengan beberapa opsi “**target**” berupa:

- **ACCEPT** : mengizinkan paket data melewati firewall
- **DROP** : menjatuhkan (membuang) paket data
- **RETURN** : menghentikan paket data melintasi chain dan memberitahukannya untuk kembali ke chain sebelumnya
- Atau mengarahkannya pada chain lain.

Pada praktikum ini digunakan tables sederhana yang disebut filter dengan tiga chain, yaitu:

- **INPUT** : mengatur paket data yang datang ke server
- **FORWARD** : menyaring paket data masuk yang akan di-forward-kan ke tempat lain
- **OUTPUT** : memfilter paket data yang akan keluar dari server

8.2. TUJUAN PERCOBAAN

1. Memahami cara kerja iptables firewall
2. Memahami cara kerja komponen-komponen iptables firewall
3. Menerapkan iptables firewall rules set untuk tujuan-tujuan keamanan jaringan

8.3. ALAT DAN BAHAN

Dalam rangka melaksanakan langkah-langkah praktikum yang terdapat pada bab ini, peserta praktikum perlu menyiapkan beberapa perangkat berikut:

- Perangkat komputer Desktop/Laptop dengan kapasitas RAM minimum 8 GB
- Perangkat lunak virtualisasi (Oracle VM VirtualBox/VMWare Workstation)
- Koneksi internet
- Beberapa tools yang dibutuhkan dalam praktikum

8.4. PROSEDUR PERCOBAAN

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 # Debian
sudo pacman -Syu iptables openssh # ArchLinux
```

3. Jalankan command iptables pada Ubuntu VM Terminal:

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

Lakukan screenshot dan berikan penjelasan mengenai maksud dari tiap chain yang ditampilkan.

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

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

Lakukan screenshot dan berikan penjelasan atas tiap param/flag pada command.

5. Melalui VM, cobalah mengakses ssh anda

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

Lakukan screenshot dan berikan penjelasan.

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

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

Lakukan screenshot dan berikan penjelasan atas tiap param/flag pada command.

7. Melalui VM, cobalah mengakses ssh anda

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

Lakukan screenshot dan berikan penjelasan.

8. Jalankan command berikut untuk menghapus semua rules.

```
sudo iptables -F
```

Tulislah daftar/listing pada iptables dengan menggunakan iptables -L -v sebelum dan sesudah dijalankannya command di atas, serta tulis penjelasan tentang flag/param -F

8.5. KESIMPULAN

8.6. EVALUASI

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

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`)

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