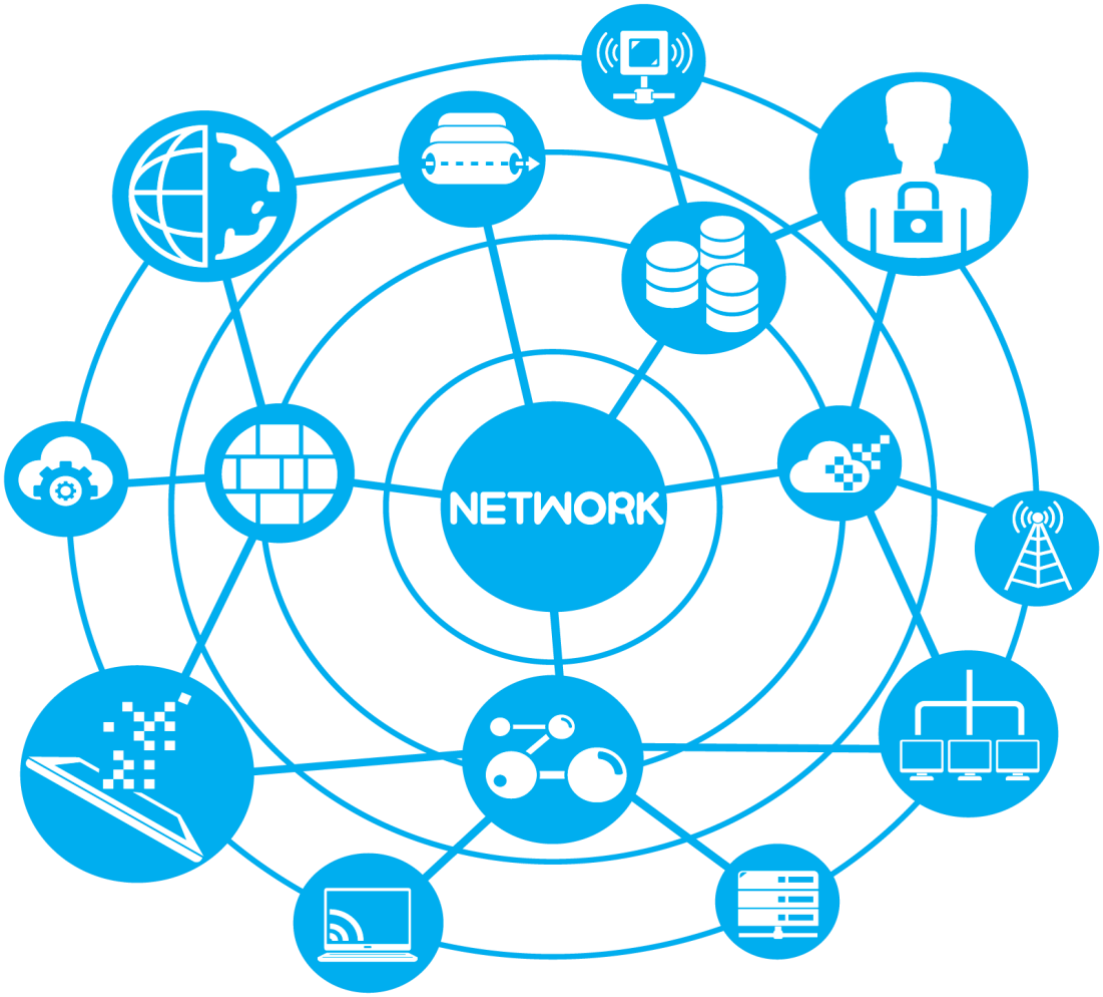
MODUL PRAKTIKUM

JARINGAN KOMPUTER LANJUT

UNIVERSITAS GUNADARMA



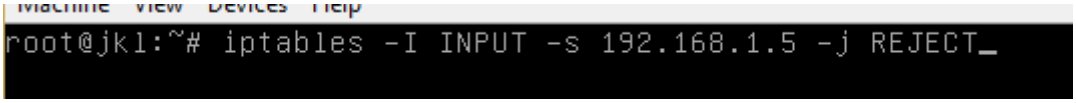
Laboratorium Sistem Komputer Lanjut
Universitas Gunadarma

BAB 5 FIREWALL

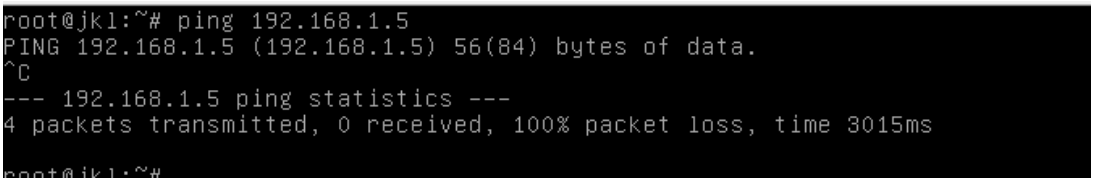
5.1 Konfigurasi IP TABLES

1. Buka virtual box yang telah terinstall operating sistem Debian 8
2. Login masukan ID dan Password yang telah dibuat

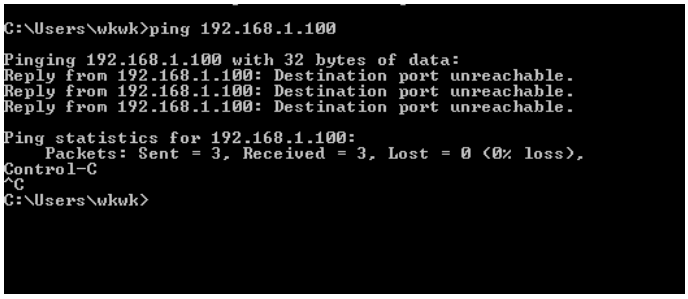
3. Coba lakukan test ping dari debian ke ip client, begitu juga sebaliknya dari client ke ip debian.
4. Percobaan iptables ini akan mencoba memblock IP dengan menjalankan perintah **DROP** dan **REJECT**.Pertama kita gunakan **REJECT**, ketikan perintah **iptables –I INPUT –s 192.168.1.5 –j REJECT**.
   *IP disesuaikan PC masing-masing



5. Setelah memberikan perintah, cek apakah perintah yang ditambahkan sudah tersedia di rules iptables, dengan mengetikan perintah iptables –L
6. Untuk melihat apakah IP yang telah di REJECT menggunakan metode iptables ini berjalan, lakukan perintah ping ke IP yang telah didaftarkan ke iptables.
   a. Ping dari debian ke client



   b. ping dari client ke debian



7. Setelah berhasil hapus rules yang tersedia pada iptables dengan menggunakan perintah **iptables –F** dan lihat hasilnya dengan menggunakan perintah **iptables -L**.

```
root@jkl:~# iptables -F
```

```
root@jkl:~# 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@jkl:~# _
```

8. Selanjutnya, mencoba untuk men DROP IP. Ketikka iptables –I OUTPUT –d 192.168.1.5 –j DROP

```
root@jkl:~# iptables -I OUTPUT -d 192.168.1.5 -j DROP
root@jkl:~# _
```

9. Untuk melihat apakah IP yang telah di DROP menggunakan metode iptables ini berjalan, lakukan perintah ping ke IP yang telah didaftarkan ke iptables.
   a. Ping dari debian ke ip client

```
root@jkl:~# ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.1.5 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3000ms
```

   b. Ping dari windows ke ip debian

```
Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
```

10. Langkah selanjutnya adalah memblock port dengan menggunakan metode iptables, port yang akan di block adalah port 22 yaitu port SSH dengan menggunakan perintah **iptables –A INPUT –p tcp --dport 22 –j REJECT**.

```
root@acsldebian:~# iptables -A INPUT -p tcp --dport 22 -j REJECT
root@acsldebian:~# _
```

11. Untuk memeriksa port yang telah di block apakah berhasil, gunakan aplikasi putty dan masukan ip Debian 8pada putty.

12. Dapat pula memblock port 22 atau SSH pada IP tertentu dengan menggunakan perintah **iptables –A INPUT –s 192.168.1.5 –p tcp --dport 22 –j REJECT**.
    *IP disesuaikan PC masing-masing

```
root@jkl:~# iptables -A INPUT -s 192.168.1.5 -p tcp --dport 22 -j REJECT
root@jkl:~#
root@jkl:~# _
```

13. Hasil pada PC yang di block port 22 atau SSH saat membuka Putty dengan IP Debian 8.

5.2 Konfigurasi UFW (UncomplicatedFirewall)

1. Instal UFW terlebih dahulu dengan menggunakan perintah **apt-get install ufw**.

```
root@acsldebian:~# apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 399 not upgraded.
root@acsldebian:~# _
```

2. Untuk mengecek status pada UFW gunakan perintah **ufw status**, jika status inactive maka status ufw belumberjalan / belum aktif.

```
root@jkl:~# ufw status
Status: inactive
root@jkl:~# _
```

3. Untuk membuat status pada UFW berjalan / aktif ketikan perintah **ufw enable** dan untuk menonaktifkan ketikan perintah **ufw disable**.

```
root@acsldebian:~# ufw enable
Firewall is active and enabled on system startup
root@acsldebian:~# ufw disable
Firewall stopped and disabled on system startup
root@acsldebian:~# _
```

4. Untuk membuat *rules* gunakan perintah *allow* untuk mengijinkan akses dan perintah deny untuk memblok akses pada suatu jaringan komputer. Untuk contoh digunakan IP 192.168.125.112 yang akan diijinkan untuk mengakses sebuah jaringan pada semua port dengan menggunakan perintah **ufw allow 192.168.125.112.**

```
root@acsldebian:~# ufw allow from 192.168.125.112
Rule added
```

5. Selain *allow* terdapat pula deny yang akan memblok akses pada suatu jaringan, dengan menggunakan perintah **ufw deny 192.168.125.112**.

```
root@acsldebian:~# ufw deny from 192.168.125.112
Rule updated
```

*Untuk mengecek hasil perintah 4 dan 5 gunakan akses PC terhadap port dan internet atau menggunakan ping melalui cmd.

6. Untuk mengecek status pada ufw dan melihat rules yang telah dibuat, gunakan perintah **ufw status.**

```
root@acsldebian:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        192.168.125.112
```

7.Selanjutnya adalah memblock dan mengijinkan port-port tertentu, contohnya untuk mengijinkan pot 80 (HTTP) gunakan perintah **ufw allow http**. Sedangkan untuk memblock port 22 (SSH) gunakan perintah **ufw deny ssh**.

```
root@acsldebian:~# ufw allow http
Rule added
Rule added (v6)
root@acsldebian:~# ufw deny ssh
Rule added
Rule added (v6)
```

8. Untuk mengecek status pada ufw dan melihat rules yang telah dibuat, gunakan perintah **ufw status**.

```
root@acsldebian:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        192.168.125.112
80                         ALLOW       Anywhere
22                         DENY        Anywhere
80 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)

root@acsldebian:~# _
```

9. untuk hasilnya sebagai berikut.

a. Allow HTTP

```
root@acsldebian:~# ping google.com
PING google.com (172.217.24.110) 56(84) bytes of data.
64 bytes from sin10s07-in-f14.1e100.net (172.217.24.110): icmp_seq=1 ttl=50 time
=21.4 ms
64 bytes from sin10s07-in-f14.1e100.net (172.217.24.110): icmp_seq=2 ttl=50 time
=21.8 ms
64 bytes from sin10s07-in-f14.1e100.net (172.217.24.110): icmp_seq=3 ttl=50 time
=22.5 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 21.401/21.939/22.595/0.509 ms
root@acsldebian:~# _
```

b. Deny SSH