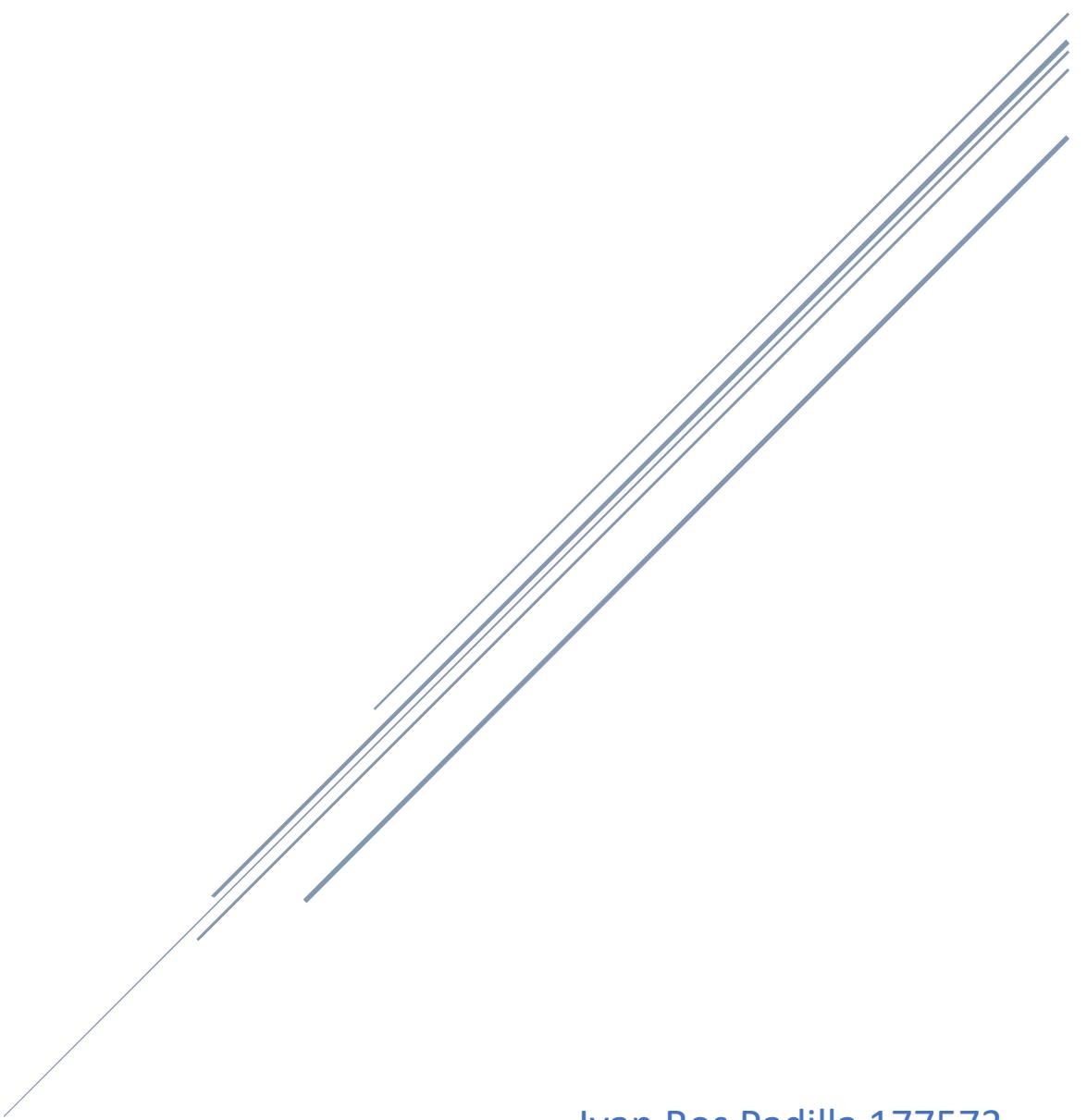


ACT4



Ivan Ros Padilla 177573

1. Establecer una política restrictiva.

```
iptables -p INPUT -j DROP
```

```
iptables -p OUTPUT -j DROP
```

2. Permitir el tráfico de conexiones ya establecidas.

```
iptables -a INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

3. Aceptar tráfico DNS (TCP) saliente de la red local.

```
iptables -a OUTPUT -i 192.1.2.* -p tcp --dport 53 -j ACCEPT
```

4. Aceptar correo entrante proveniente de Internet en el servidor de correo.

```
iptables -a INPUT -i 0.0.0.0 -d 192.1.2.10 -p tcp --dport 25 -j ACCEPT
```

5. Permitir correo saliente a Internet desde el servidor de correo.

```
Iptables -a OUTPUT -i 192.1.2.10 -d 0.0.0.0 -p tcp --dport 25 -j ACCEPT
```

6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.

```
Iptables -a INPUT -i 0.0.0.0 -d 192.1.2.11 -p tcp --dport 80 -j ACCEPT
```

7. Permitir tráfico HTTP desde la red local a Internet.

```
Iptables -a INPUT -i 192.1.2.* -d 0.0.0.0 -p tcp -dport 80 -j ACCEPT
```