Pablo Ruiz Galianez
Practica Iptables

Ejercicios Firewall con IPTABLES

1. Permitir todo el tráfico desde una dirección IP específica:

```
iptables -A INPUT -s <IP_ADDRESS> -j ACCEPT
```

2. Permitir todo el tráfico desde una subred específica:

```
iptables -A INPUT -s <subred> -j ACCEPT
```

3. Bloquear todo el tráfico entrante:

```
iptables -A INPUT -j DROP
```

4. Permitir SSH desde una dirección IP específica 122.122.122.1:

```
iptables -A INPUT -s 122.122.122.1 -p tcp --dport ssh -j ACCEPT
```

5. *Permitir HTTP desde una subred específica:*

```
iptables -A INPUT -p tcp --dport 80 -s <subred> -j ACCEPT
```

6. *Permitir HTTPS desde cualquier dirección IP:*

```
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

7. *Permitir ping desde cualquier dirección IP:*

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

8. Bloquear ping desde cualquier dirección IP:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

9. Permitir acceso FTP desde una dirección IP específica:

```
iptables -A INPUT -p tcp -s <IP_ADDRESS> --dport 21 -j ACCEPT
```

10. *Permitir acceso SSH desde cualquier dirección IP:*

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

11. Permitir acceso POP3 desde una dirección IP específica:

```
iptables -A INPUT -s <IP_ADDRESS> -p tcp --dport pop3 -j ACCEPT
```

12. Permitir acceso IMAP desde cualquier dirección IP:

```
iptables -A INPUT -p tcp --dport imap -j ACCEPT
```

13. Permitir acceso HTTP a un servidor web:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

14. Permitir el tráfico FORWARD:

```
iptables -P FORWARD ACCEPT
```

15. Permitir el tráfico FORWARD de una dirección IP específica:

```
iptables -A FORWARD -s <IP_ADDRESS> -j ACCEPT
```

16. *Permitir el tráfico FORWARD a una dirección IP específica*

```
iptables -A FORWARD -d <IP_ADDRESS> -j ACCEPT
```

17. *Permitir el tráfico FORWARD de un puerto específico*

```
iptables -A FORWARD -p tcp --dport PUERTO_ESPECIFICO -j ACCEPT
```

18. Denegar el tráfico FORWARD de una interfaz específica: Solución:

iptables `-A FORWARD -i <INTERFACE_NAME> -j DROP`

19. Denegar el tráfico FORWARD a una interfaz específica

```
iptables -A FORWARD -o <INTERFACE_NAME> -j DROP
```

20. Permitir el tráfico HTTP (puerto 80) a través de un proxy solo para una dirección IP específica: Solución:

```
iptables -t nat -A OUTPUT -p tcp --dport 80 -d ! <PROXY_IP_ADDRESS> -j
DNAT --to-destination <PROXY_IP_ADDRESS>:<PROXY_PORT>
iptables -A OUTPUT -p tcp --dport <PROXY_PORT> -d <PROXY_IP_ADDRESS> -
s <IP_ADDRESS> -j ACCEPT
```

21. Limitar la velocidad de tráfico de subida y bajada a una interfaz específica: Solución:

```
iptables -A OUTPUT -o <INTERFACE_NAME> -m limit --limit 100/s --limit-
burst 100 -j ACCEPT
iptables -A INPUT -i <INTERFACE_NAME> -m limit --limit 100/s --limit-
burst 100 -j ACCEPT
```

22. Bloquear el tráfico ICMP a excepción de la respuesta de ping (tipo 8 y código 0):

```
iptables -A INPUT -p icmp --icmp-type 8 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp -j DROP
```

23. Configura un firewall en una máquina Linux para permitir el tráfico SSH (puerto 22) desde una dirección IP específica y bloquear todo el tráfico entrante no permitido.

```
iptables -A INPUT -p tcp --dport 22 -s <IP_ADDRESS> -j ACCEPT
iptables -A INPUT -j DROP
```

24. Configura un firewall en una máquina Linux para permitir el tráfico SSH (puerto 22) desde una dirección IP específica y permitir el tráfico HTTPS (puerto 443) desde cualquier dirección IP, pero solo después de una conexión exitosa SSH. Solución:

```
iptables -P INPUT DROP
iptables -A INPUT -p tcp --dport 22 -s <IP_ADDRESS> -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED
-m recent --set --name HTTPS --rsource
iptables -A INPUT -p tcp --dport 443 -m state --state ESTABLISHED -m
recent --name HTTPS --rsource --remove -j ACCEPT
```

25. Configura un firewall en una máquina Linux para permitir el tráfico SSH (puerto 22) desde una dirección IP específica y permitir el tráfico HTTP (puerto 80) desde cualquier dirección IP, pero solo después de una conexión exitosa SSH. Solución:

```
iptables -P INPUT DROP
iptables -A INPUT -p tcp --dport 22 -s <IP_ADDRESS> -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -
m recent --set --name HTTP --rsource
iptables -A INPUT -p tcp --dport 80 -m state --state ESTABLISHED -m
recent --name HTTP --rsource --remove -j ACCEPT
```

26. *Configura un firewall en una máquina Linux para permitir el tráfico HTTP (puerto 80) y HTTPS (puerto 443) desde cualquier dirección IP y registrar todoslos paquetes que superen una determinada tasa de transferencia.*

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -m limit --limit (transfer rate)kb/s -j LOG --log-
prefix "tasa de transferencia superada en el paquete: "
iptables -A INPUT -j DROP
```

Extra para guardar la configuración:

```
iptables-save > <ruta>
```

Y para listar:

```
iptables -L -n
```