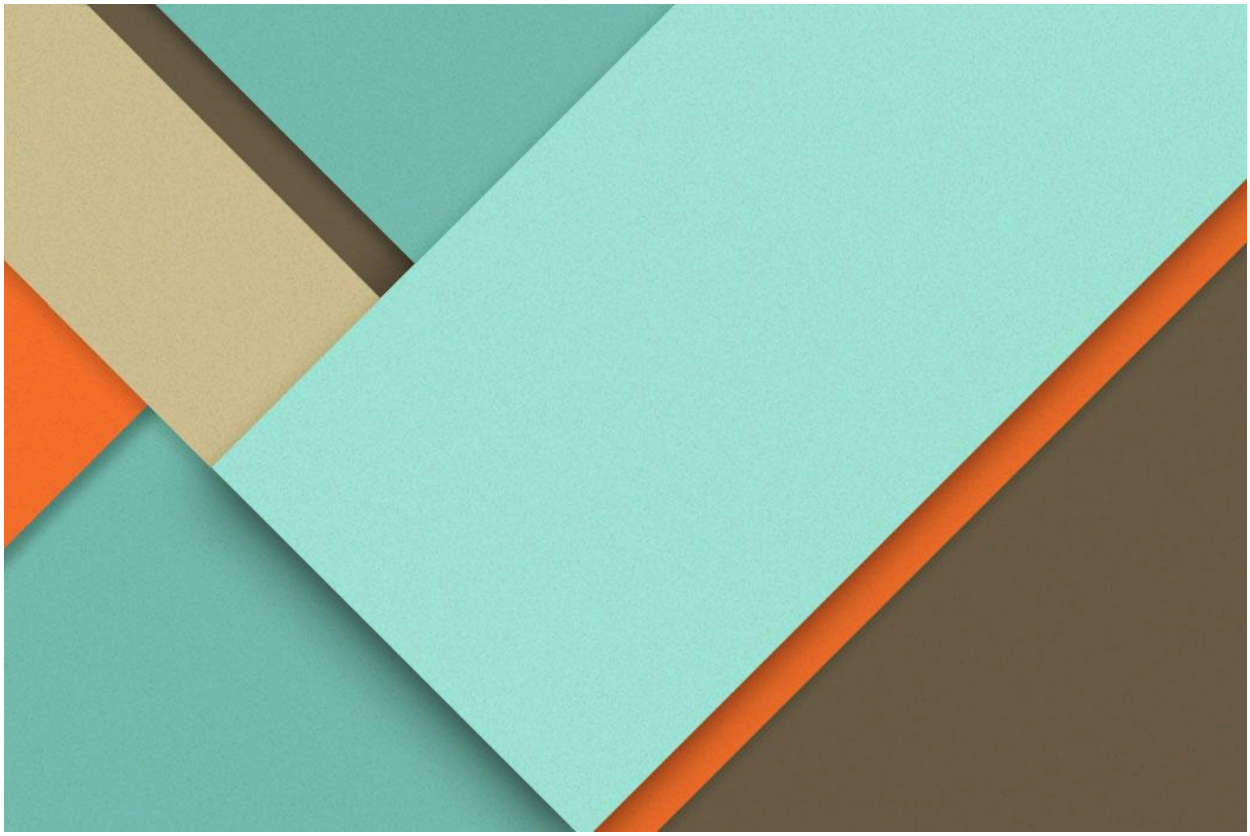


Práctica 3.1. Configuraciones de Seguridad

DESPLIEGUE DE APLICACIONES WEB

Alejandro Leo Carretero
2º DAW-A

Configuración de red

Lo primero que haremos es configurar la red

Vemos que se ha configurado sin problemas

```
usuario@usuario-VirtualBox:~/Escritorio$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::7919:2673:2721:dd8a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:50:2b:3b  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 280 (280.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49  bytes 5553 (5.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 166  bytes 13696 (13.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 166  bytes 13696 (13.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Hace ping con el cliente sin problemas

```
usuario@usuario-VirtualBox:~/Escritorio$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.313 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.227 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.250 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=0.234 ms
64 bytes from 192.168.1.3: icmp_seq=6 ttl=64 time=0.227 ms
64 bytes from 192.168.1.3: icmp_seq=7 ttl=64 time=0.271 ms
^C
--- 192.168.1.3 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6122ms
rtt min/avg/max/mdev = 0.206/0.246/0.313/0.032 ms
usuario@usuario-VirtualBox:~/Escritorio$
```

IpTables

Instalamos el programa

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo apt install iptables
```

Con este comando añadiremos una regla de firewall para que no podamos recibir ningún ping entrante

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -A INPUT -p icmp --icmp-
type 8 -j REJECT
```

Si intentamos hacer ping desde el cliente a nuestro servidor veremos que es imposible

```
usuario@usuario-VirtualBox:~/Escritorio$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.1.2 icmp_seq=1 Destination Port Unreachable
From 192.168.1.2 icmp_seq=2 Destination Port Unreachable
From 192.168.1.2 icmp_seq=3 Destination Port Unreachable
From 192.168.1.2 icmp_seq=4 Destination Port Unreachable
From 192.168.1.2 icmp_seq=5 Destination Port Unreachable
^C
--- 192.168.1.2 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4096ms

usuario@usuario-VirtualBox:~/Escritorio$
```

Ahora con este comando eliminamos la regla anterior

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -D INPUT -p icmp --icmp-
type 8 -j REJECT
```

Si volvemos otra vez al cliente veremos que la conexión entre ambas maquinas se ha restablecido

```
usuario@usuario-VirtualBox:~/Escritorio$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.212 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.220 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.360 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=0.367 ms
^C
--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.212/0.294/0.367/0.066 ms
```

Ahora pondremos las siguientes reglas

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P INPUT DROP
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P OUTPUT DROP
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P FORWARD DROP
usuario@usuario-VirtualBox:~/Escritorio$
```

Y vemos que no tenemos conexión ya que el firewall está cortando el acceso

Hmm. We're having trouble finding that site.

We can't connect to the server at www.google.com.

If you entered the right address, you can:

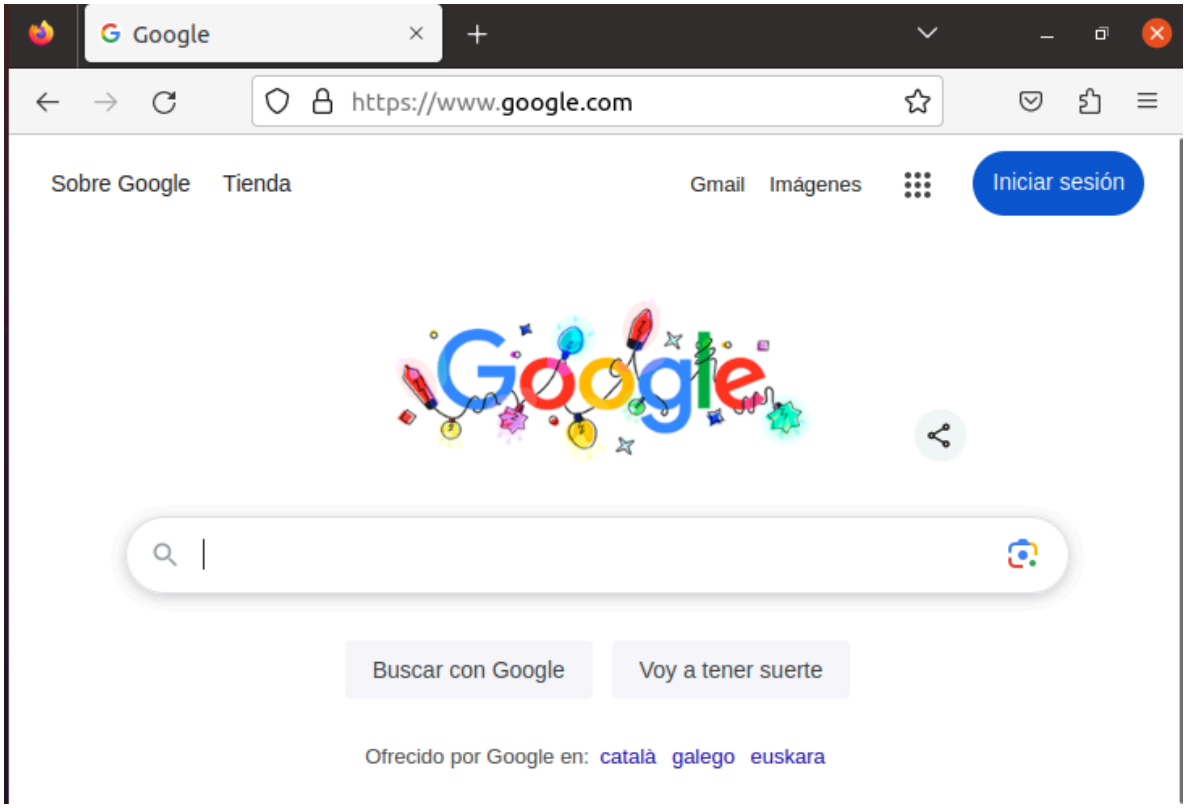
- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

Ahora para volver a tener conexión pondremos los siguientes comandos

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P INPUT ACCEPT
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P OUTPUT ACCEPT
usuario@usuario-VirtualBox:~/Escritorio$ sudo iptables -P FORWARD ACCEPT
usuario@usuario-VirtualBox:~/Escritorio$
```

Vemos que volvemos a tener conexión a internet



Si queremos que las configuraciones despues de reiniciar el sistema sigan estando instalaremos el siguiente comando

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo apt install iptables-persistent
```

Para que se termine de configurar utilizaremos el siguiente comando

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables sav
e
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables sav
e
```

Y este comando para actualizar cada vez que añadamos una nueva regla

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo netfilter-persistent reload
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables sta
rt
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables sta
rt
```

Con este comando veremos todas las reglas que hemos añadido

```
usuario@usuario-VirtualBox:~/Escritorio$ sudo 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
usuario@usuario-VirtualBox:~/Escritorio$
```