# Trabajos prácticos

Aquí se proponen ejercicios para implementar algunos de los puntos abordados en el capítulo. En cada uno de ellos se da un ejemplo comentado de la realización del ejercicio, que deberá adaptar a la configuración de sus sistemas.

## 1. Configuración de un firewall Linux

Decidimos implementar un firewall IPv4 en un servidor Linux Debian 10. Tendrá que filtrar todo el tráfico entrante o saliente, que no sea SSH, HTTP, HTTPS y DNS.

### Comandos y archivos utiles

- `iptables`
- `wget`
- `ping`
- `host`
- `iptables-save`
- `/etc/iptables/rules.v4`

### Etapas

1. En el servidor `debian10`, compruebe que el comando `iptables` está disponible y muestre las reglas de filtrado actuales.

2. Configure el firewall para que acepte las conexiones entrantes y salientes SSH.

3. Configure el firewall para que, por defecto, rechace cualquier tráfico de red. Compruebe que las reglas se han aplicado correctamente.

4. Configure el firewall para autorizar el tráfico entrante y saliente HTTP, HTTPS y DNS. Compruebe que las reglas se han aplicado correctamente.

5. Configure el servidor para que las reglas del firewall sean activadas automáticamente durante el inicio de la red. Compruebe que las reglas se han aplicado correctamente después del reinicio.

### Resumen de los comandos y resultado en pantalla

1. En el servidor `debian10`, compruebe que el comando `iptables` está disponible y muestre las reglas de filtrado actuales.

¿Está el paquete de software instalado?

```
root@debian10:~# apt list iptables
Listando... Hecho
iptables/stable,now 1.8.2-4 amd64  [instalado]
```

Las reglas `iptables` cargadas actualmente:

```
root@debian10:~# 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
```

No hay ninguna restricción de acceso configurada.

2. Configure el firewall para que acepte las conexiones entrantes y salientes SSH.

Se autorizan las conexiones entrantes hacia el servidor SSH local:

```
root@debian10:~# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

Se autorizan las conexiones salientes hacia un servidor SSH remoto:

```
root@debian10:~# iptables -A OUTPUT -p tcp --dport ssh -j ACCEPT
```

Se autorizan los intercambios vinculados a una conexión establecida entrante o saliente:

```
root@debian10:~# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
root@debian10:~# iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Se muestran las reglas:

```
root@debian10:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
```

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
```

3. Configure el firewall para que, por defecto, rechace cualquier tráfico de red. Compruebe que las reglas se han aplicado correctamente.

Fijamos las estrategias de las cadenas por defecto para destruir los paquetes:

```
root@debian10:~# iptables -P OUTPUT DROP
root@debian10:~# iptables -P INPUT DROP
root@debian10:~# iptables -P FORWARD DROP
```

Mostramos las reglas:

```
root@debian10:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
```

Comprobamos la conexión SSH, saliente, abriendo una sesión en el servidor `192.168.0.60` :

```
root@debian10:~# ssh 192.168.0.60
Bienvenido al servidor CentOS8.
Acceso reservado a personas autorizadas.
root@192.168.0.60's password:
Bienvenido al servidor CentOS 8
Last login: Wed Jun 24 15:32:59 2020 from 192.168.0.24
```

Desde este servidor, comprobamos la conexión entrante SSH:

```
[root@centos8 ~]# ssh 192.168.0.70
root@192.168.0.70's password:
Linux debian10 4.19.117 #2 SMP Thu Apr 23 10:04:02 CEST 2020 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Jun 24 15:55:23 2020 from 192.168.0.24
root@debian10:~#
```

4. Configure el firewall para autorizar el tráfico entrante y saliente HTTP, HTTPS y DNS. Compruebe que las reglas se han aplicado correctamente.

Se abren los puertos HTTP, HTTPS y DNS, en entrada y salida:

```
root@debian10:~# iptables -A INPUT -p tcp --dport https -j ACCEPT
root@debian10:~# iptables -A INPUT -p tcp --dport domain -j ACCEPT
root@debian10:~# iptables -A INPUT -p udp --dport domain -j ACCEPT
root@debian10:~# iptables -A OUTPUT -p tcp --dport http -j ACCEPT
root@debian10:~# iptables -A OUTPUT -p tcp --dport https -j ACCEPT
```

```
root@debian10:~# iptables -A OUTPUT -p tcp --dport domain -j ACCEPT
root@debian10:~# iptables -A OUTPUT -p udp --dport domain -j ACCEPT
```

Mostramos las reglas:

```
root@debian10:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
```

Comprobamos las conexiones entrantes desde una máquina remota.

Comprobamos que el servidor HTTP local está activo:

```
root@debian10:~# systemctl status apache2
  apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2020-06-24 16:19:24 CEST;
[...]
```

Solicitamos la página de inicio del servidor HTTP desde una máquina remota:

```
[root@centos8 ~]# wget -O - debian10 | more
--2020-06-24 16:20:31--  http://debian10/
Resolviendo debian10 (debian10)... 192.168.0.70
Conectando con debian10 (debian10)|192.168.0.70|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 10701 (10K) [text/html]
Grabando a: « STDOUT »

-           0%[                                 ]       0  --.-KB/s
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Debian Default Page: It works</title>
```

El servidor está accesible.

Nos conectamos en el servidor SMTP local, usando el comando nc:

```
root@debian10:~# nc localhost 25
220 debian10.mondns.fr ESMTP Postfix (Debian/GNU)
^C
```

Hacemos la prueba de la conexión desde una máquina remota:

```
[root@centos8 ~]# nc 192.168.0.70 25
EHLO
Ncat: Connection timed out.
```

La solicitud de conexión ha sido destruida silenciosamente por el firewall.

Comprobamos la resolución de nombres DNS:

```
root@debian10:~# host www.google.com
www.google.com has address 172.217.22.132
www.google.com has IPv6 address 2a00:1450:4007:815::2004
```

Comprobamos que se puede acceder a un servidor HTTPS remoto:

```
root@debian10:~# wget -O - https://www.centos.org | more
--2020-06-24 16:29:48--  https://www.centos.org/
Resolviendo de www.centos.org (www.centos.org)...
2a05:d01c:c6a:cc02:e4d3:88b0:60da:6fb4, 35.178.203.231
Conectando con www.centos.org (www.centos.org)|
2a05:d01c:c6a:cc02:e4d3:88b0:60da:6fb4|:443... connectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 21061 (21K) [text/html]
Guardado a: « STDOUT »

-           0%[                    ]      0  --.-KB/s            <!DOCTYPE html>
-           100%[===========================>]  20,57K  --.-KB/s    ds 0,02s

<html>
 <head>
2020-06-24 16:29:48 (1,33 MB/s) — escritos a stdout [21061/21061]

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <link href="//fonts.googleapis.com/css?family=Oxygen+Mono%7CSource+Sans+Pro:
400,300,300italic,400italic,600,600italic%7CExo:400,100
,100italic,200,200italic,300,300italic,400italic,500italic,500,600,600italic"
rel="stylesheet" type="text/css">
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <meta content="" name="description">
  <meta content="" name="author">
  <meta content="max-age=0" http-equiv="cache-control">
  <meta content="no-cache" http-equiv="pragma">
  <link href="/images/favicon.ico" rel="shortcut icon">
  <title>CentOS Project</title>
[...]
```

5. Configure el servidor para que las reglas del firewall sean activadas automáticamente durante el inicio de la red. Compruebe que las reglas se han aplicado correctamente después del reinicio.

Instalamos el paquete de software `iptables-persistent` si fuera necesario:

```
root@debian10:~# apt list iptables-persistent
Listando... Hecho
iptables-persistent/stable 1.0.11 all
root@debian10:~# apt-get install iptables-persistent
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 netfilter-persistent
Se instalarán los siguientes paquetes NUEVOS:
 iptables-persistent netfilter-persistent
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 22,0 kB de archivos.
Se utilizarán 81,9 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S

[...]
¿Hay que guardar las reglas IPv4 actuales ?                ¦
¦                                                          ¦
¦                          <Sí>
[...]
```

Guardando las reglas:

```
root@debian10:~# iptables-save -f rules.txt
root@debian10:~# vi rules.txt
# Generated by xtables-save v1.8.2 on Wed Jun 24 16:31:32 2020
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
```

```
:OUTPUT DROP [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
COMMIT
# Completed on Wed Jun 24 16:31:32 2020
```

Copiamos el archivo en el archivo de configuración de las reglas al iniciar:

```
root@debian10:~# cp rules.txt /etc/iptables/rules.v4
root@debian10:~# ls -l /etc/iptables/rules.v4
-rw-r--r-- 1 root root 735 juin  24 16:34 /etc/iptables/rules.v4
```

Después de reiniciar el sistema, mostramos las reglas cargadas:

```
root@debian10:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
```

```
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere            udp dpt:domain
```

Las reglas han sido reactivadas correctamente.