

Actividad 10 – 03: Cortafuegos



USO DEL FIREWALL UFW

- [1] Instala el paquete openssh-server, que es un servidor de SSH. Una vez instalado, asegúrate de que el servicio esté corriendo. Despues, accede por SSH (con el comando ssh, no con putty) con tu usuario a tu propia máquina desde tu propia máquina. ¿Funciona el acceso?

```
alberto@alberto-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
```

```
alberto@alberto-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2022-03-21 13:04:20 CET; 1min 30s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 12381 (sshd)
     Tasks: 1 (limit: 7044)
    Memory: 1.0M
      CGroup: /system.slice/ssh.service
              └─12381 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

mar 21 13:04:20 alberto-VirtualBox systemd[1]: Starting OpenBSD Secure Shell server...
mar 21 13:04:20 alberto-VirtualBox sshd[12381]: Server listening on 0.0.0.0 port 22.
mar 21 13:04:20 alberto-VirtualBox sshd[12381]: Server listening on :: port 22.
mar 21 13:04:20 alberto-VirtualBox systemd[1]: Started OpenBSD Secure Shell server.
```

```
alberto@alberto-VirtualBox:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:jvuSZlcCp0o1R8FF0ZibNoV6YRF0CAItbzSouYDz1Is.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
alberto@localhost's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

(Sí, funciona correctamente).

2. [2] Utiliza **ufw** para aplicar a tu ordenador la configuración típica de firewall para un Linux de Escritorio (denegar tráfico entrante y permitir tráfico saliente). Una vez aplicada la configuración muestra el estado de la configuración del firewall y comprueba que puedes navegar correctamente. Adjunta pantallazos de los comandos necesarios y de un navegador visitando una página web de tu libre elección.

```
alberto@alberto-VirtualBox:~$ sudo ufw default deny incoming
[sudo] password for alberto:
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
alberto@alberto-VirtualBox:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
alberto@alberto-VirtualBox:~$ █
```

```
alberto@alberto-VirtualBox:~$ sudo ufw status
Status: inactive
alberto@alberto-VirtualBox:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
alberto@alberto-VirtualBox:~$ sudo ufw status
Status: active
alberto@alberto-VirtualBox:~$ █
```

The screenshot shows a GitHub profile page for the user 'Kadex96'. The profile picture is a circular portrait of a man with dark hair and a beard. The user's name is listed as 'Alberto Fernández-Palacios Aquino' and their GitHub handle is 'Kadex96'. Below the profile, there are two repository cards:

- Programacion_DAW** (Public)
Todos mis ejercicios del módulo de programación del CFGS Desarrollo de Aplicaciones Web
Java Updated 6 days ago
- Entornos_DAW** (Public)
Asignatura Entornos de Desarrollo del CFGS DAW
Java Updated 25 days ago

At the bottom left, there are buttons for 'Follow' and 'Block or Report'. The top of the page shows a browser header with the URL 'github.com/Kadex96?tab=repositories'.

3. [3] Intenta acceder de nuevo a tu ordenador con ssh. ¿Porqué sigue funcionando el acceso si acabamos de configurar el cortafuegos de forma que se deniegue el tráfico entrante?

```
alberto@alberto-VirtualBox:~$ ssh localhost
alberto@localhost's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar 21 13:07:37 2022 from 127.0.0.1
alberto@alberto-VirtualBox:~$ █
```

(Funciona porque el SSH manda una operación de salida, y estas operaciones sí están permitidas. Al tratarse del mismo ordenador, se considera al completo como una operación de salida y se permite).

4. [3] Partiendo de la configuración anterior utiliza **ufw** para abrir los puertos necesarios para poder ofrecer los siguientes servicios:

4.a) DNS

```
alberto@alberto-VirtualBox:~$ sudo ufw allow 53/udp
Rule added
Rule added (v6)
alberto@alberto-VirtualBox:~$ █
```

4.b) FTP en modo activo

```
alberto@alberto-VirtualBox:~$ sudo ufw allow 21
Rule added
Rule added (v6)
alberto@alberto-VirtualBox:~$ █
```

4.c) SSH

```
alberto@alberto-VirtualBox:~$ sudo ufw allow 22
Rule added
Rule added (v6)
alberto@alberto-VirtualBox:~$ █
```

4.d) HTTP y HTTPS

```
alberto@alberto-VirtualBox:~$ sudo ufw allow http  
Rule added  
Rule added (v6)  
alberto@alberto-VirtualBox:~$ sudo ufw allow https  
Rule added  
Rule added (v6)  
alberto@alberto-VirtualBox:~$ █
```

Muestra el estado de la configuración del firewall.

```
alberto@alberto-VirtualBox:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To                         Action      From  
--                         -----      ---  
80/tcp                      ALLOW IN   Anywhere  
443/tcp                     ALLOW IN   Anywhere  
22                          ALLOW IN   Anywhere  
21                          ALLOW IN   Anywhere  
53/udp                      ALLOW IN   Anywhere  
80/tcp (v6)                  ALLOW IN   Anywhere (v6)  
443/tcp (v6)                ALLOW IN   Anywhere (v6)  
22 (v6)                     ALLOW IN   Anywhere (v6)  
21 (v6)                     ALLOW IN   Anywhere (v6)  
53/udp (v6)                 ALLOW IN   Anywhere (v6)
```

5. [4] Partiendo de la configuración anterior debes denegar (deny) los puertos asociados al servicio de FTP y DNS. Muestra el estado de configuración del firewall tras realizar los cambios.

```
alberto@alberto-VirtualBox:~$ sudo ufw deny 53/udp  
Rule updated  
Rule updated (v6)  
alberto@alberto-VirtualBox:~$ sudo ufw deny 21  
Rule updated  
Rule updated (v6)
```

```
alberto@alberto-VirtualBox:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         -----      ---
80/tcp                      ALLOW IN   Anywhere
443/tcp                     ALLOW IN   Anywhere
22                          ALLOW IN   Anywhere
21                          DENY IN   Anywhere
53/udp                      DENY IN   Anywhere
80/tcp (v6)                 ALLOW IN   Anywhere (v6)
443/tcp (v6)                ALLOW IN   Anywhere (v6)
22 (v6)                     ALLOW IN   Anywhere (v6)
21 (v6)                     DENY IN   Anywhere (v6)
53/udp (v6)                 DENY IN   Anywhere (v6)
```

6. [1] Por último, resetea el firewall para dejar el ordenador como al principio.

```
alberto@alberto-VirtualBox:~$ sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20220321_133504'
Backing up 'before.rules' to '/etc/ufw(before.rules.20220321_133504'
Backing up 'after.rules' to '/etc/ufw(after.rules.20220321_133504'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20220321_133504'
Backing up 'before6.rules' to '/etc/ufw(before6.rules.20220321_133504'
Backing up 'after6.rules' to '/etc/ufw(after6.rules.20220321_133504'
```