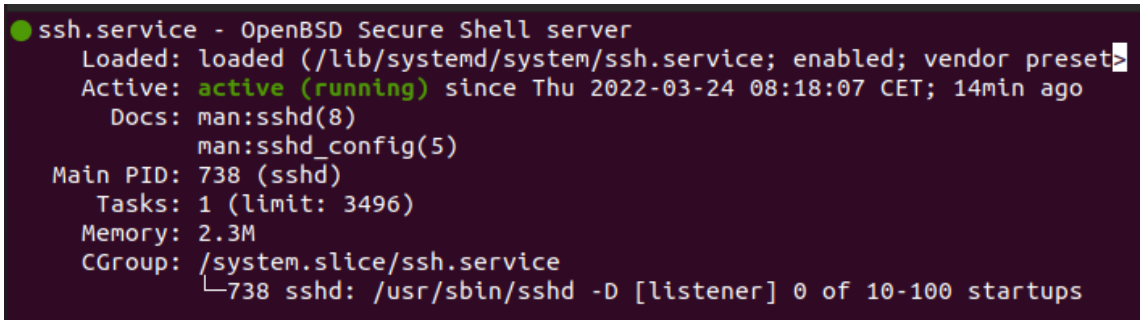
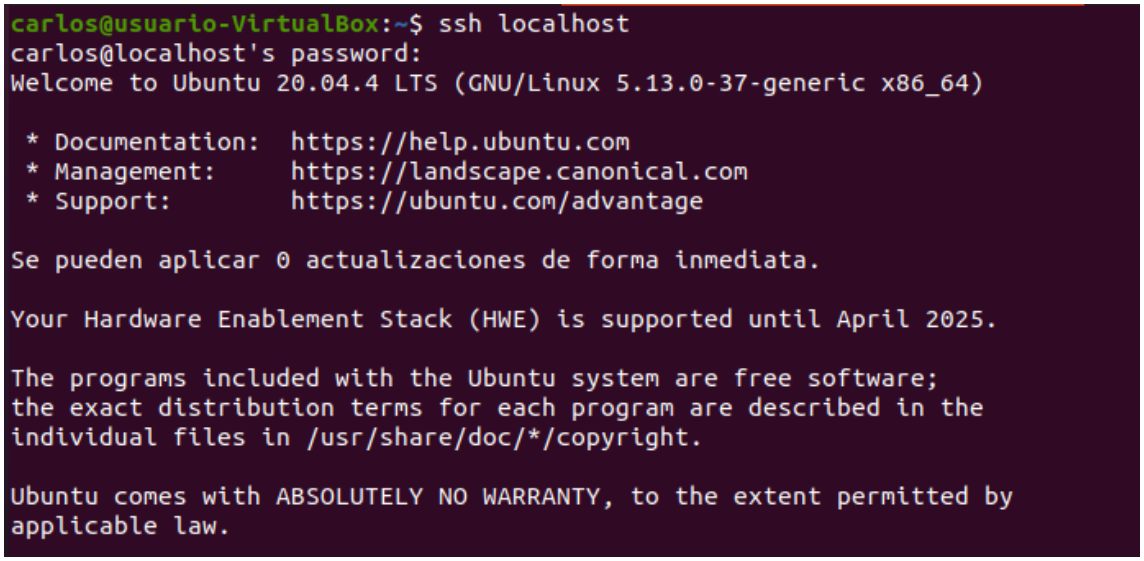
USO DEL FIREWALL UFW

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

Si, utilizamos el comando **sudo ufw allow ssh** para añadir permiso de conexión en red por ssh





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.

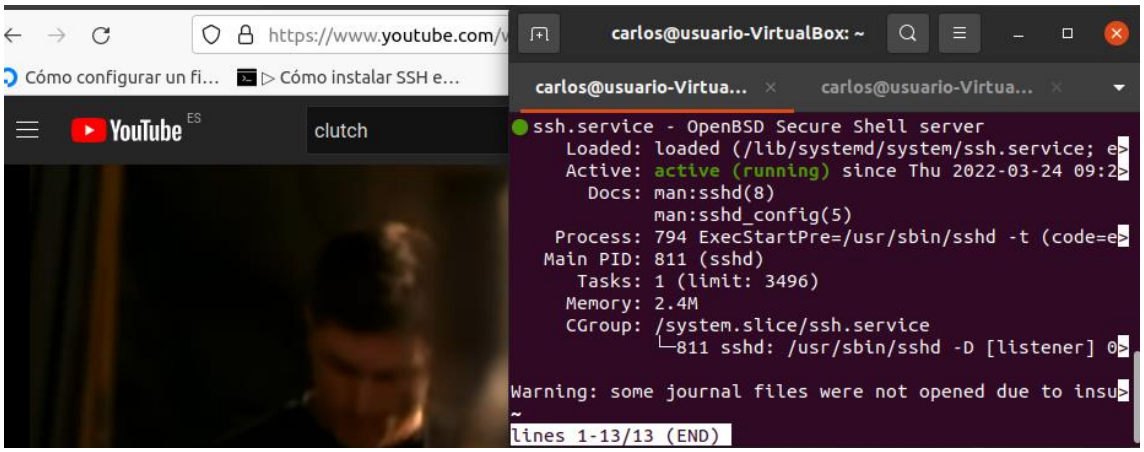
```
carlos@usuario-VirtualBox:~$ sudo ufw default deny incoming
[sudo] contraseña para carlos:
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
carlos@usuario-VirtualBox:~$ sudo ufw default allow outgoing
La política outgoing predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
carlos@usuario-VirtualBox:~$
```

```
carlos@usuario-VirtualBox:~$ sudo ufw enable
El comando puede interrumpir las conexiones ssh existentes. ¿Continuar con la operación (s|n)? s
El cortafuegos está activo y habilitado en el arranque del sistema
carlos@usuario-VirtualBox:~$
```

```
carlos@usuario-VirtualBox:~$ sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

Hasta                      Acción      Desde
-----                      ------      -----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)

carlos@usuario-VirtualBox:~$
```



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?

Previamente le he dado permisos a ssh pero supongo que es porque esta trabajando en local.

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

4.a) DNS

```
carlos@usuario-VirtualBox:~$ sudo ufw allow 53/tcp
Regla añadida
Regla añadida (v6)
carlos@usuario-VirtualBox:~$ sudo ufw allow 53/udp
Regla añadida
Regla añadida (v6)
carlos@usuario-VirtualBox:~$
```

4.b) FTP en modo activo

```
carlos@usuario-VirtualBox:~$ sudo ufw allow ftp-data
Regla añadida
Regla añadida (v6)
carlos@usuario-VirtualBox:~$
```

4.c) SSH

```
carlos@usuario-VirtualBox:~$ sudo ufw allow ssh
Omitiendo adición de regla ya existente
Omitiendo adición de regla ya existente (v6)
carlos@usuario-VirtualBox:~$
```

4.d) HTTP y HTTPS

```
carlos@usuario-VirtualBox:~$ sudo ufw allow http
Regla añadida
Regla añadida (v6)
carlos@usuario-VirtualBox:~$ sudo ufw allow https
Regla añadida
Regla añadida (v6)
carlos@usuario-VirtualBox:~$
```

Muestra el estado de la configuración del firewall.

```
carlos@usuario-VirtualBox:~$ sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

Hasta                      Acción      Desde
-----                      ------      -----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
53/tcp                     ALLOW IN    Anywhere
53/udp                     ALLOW IN    Anywhere
20/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
53/tcp (v6)                ALLOW IN    Anywhere (v6)
53/udp (v6)                ALLOW IN    Anywhere (v6)
20/tcp (v6)                ALLOW IN    Anywhere (v6)

carlos@usuario-VirtualBox:~$
```

5. 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.

```
carlos@usuario-VirtualBox:~$ sudo ufw deny ftp
Regla añadida
Regla añadida (v6)
```

```
carlos@usuario-VirtualBox:~$ sudo ufw deny 53/udp
Regla actualizada
Regla actualizada (v6)
carlos@usuario-VirtualBox:~$ sudo ufw deny 53/tcp
Regla actualizada
Regla actualizada (v6)
carlos@usuario-VirtualBox:~$
```

```
carlos@usuario-VirtualBox:~$ sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

Hasta                      Acción      Desde
-----                      ------      -----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
53/tcp                     DENY IN     Anywhere
53/udp                     DENY IN     Anywhere
20/tcp                     ALLOW IN    Anywhere
21/tcp                     DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
53/tcp (v6)                DENY IN     Anywhere (v6)
53/udp (v6)                DENY IN     Anywhere (v6)
20/tcp (v6)                ALLOW IN    Anywhere (v6)
21/tcp (v6)                DENY IN     Anywhere (v6)

carlos@usuario-VirtualBox:~$
```

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