Lab 2. Bastionado de sistemas:

Fecha: 14/10/2024

Elaborado por: Alvaro Rey Jimenez

- ***INSTALACIÓN DE SERVICIOS MÍNIMOS:***
  - Vamos a preparar un servidor de Ubuntu server con los servicios necesarios es decir. SSH, FTP, el servidor MySQL y el servidor Apache
  - Hay que asegurarse que este servidor este accesible para poder hacer ping y que se puedan ver ambas máquinas
  - Actualizaremos los paquetes del sistema antes de realizar todas las instaciones
  - Los comandos para instalar todos esos servicios son:

    ```
    sudo apt-get install ssh
    ```

    ```
    sudo apt-get install vsftpd
    ```

    ```
    sudo apt-get install mysql-server
    ```

    ```
    sudo apt-get install apache2
    ```

  - Una vez instalados todos los servicios necesarios, tendremos que habilitarlos para que puedan funcionar
  - Para ello, utilizaremos los siguientes comandos:

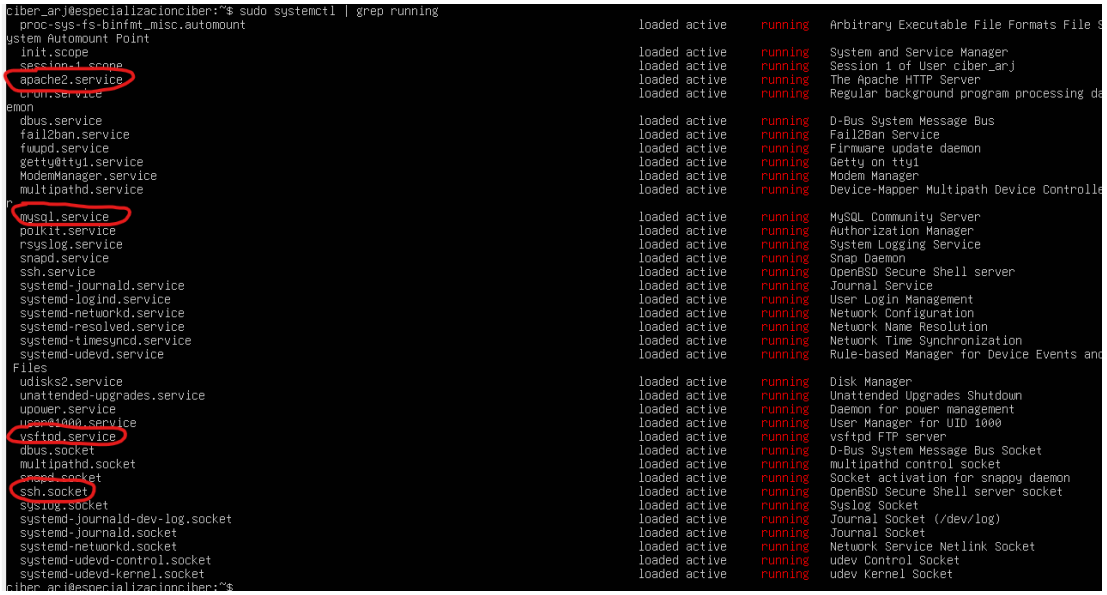
    ```
    sudo systemctl enable ssh
    ```

    ```
    sudo systemctl enable vsftpd
    ```

```
sudo systemctl enable mysql
```

```
sudo systemctl enable apache2
```

- Si utilizamos el comando que se verá en la siguiente imagen, podemos confirmar que estos servicios están habilitados



- Se puede ver q todos los servicios están activos pero hay que iniciar todos los servicios habilitados.
- Para iniciarlos, habrá que utilizar los siguientes comandos

```
service ssh start
```

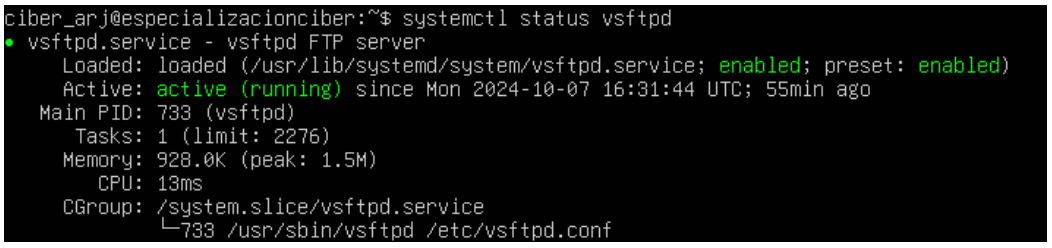
```
service vsftpd start
```

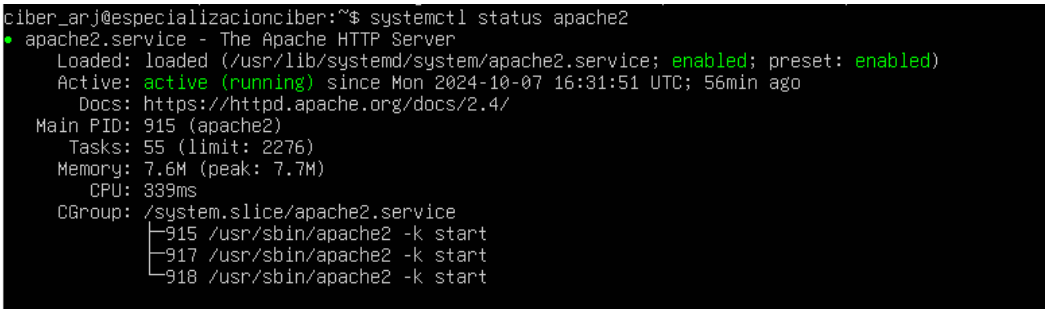
```
service mysql start
```

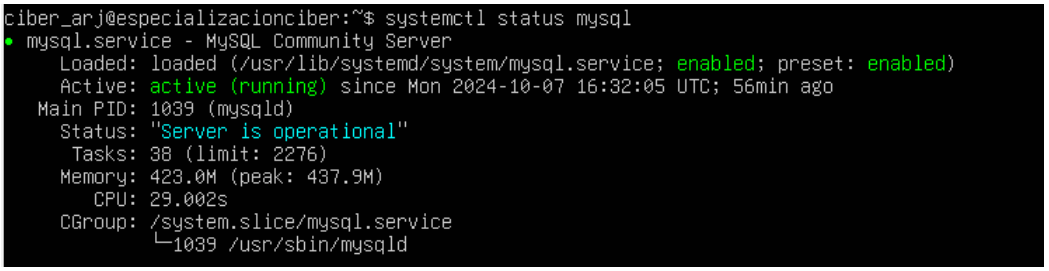
```
service apache2 start
```

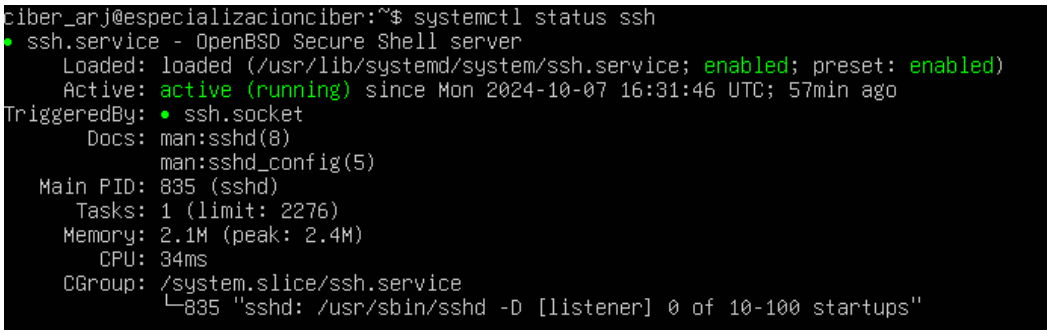
- Para confirmar que absolutamente todos los servicios están iniciados, utilizaremos los comandos que se ven en las siguientes

imagenes.





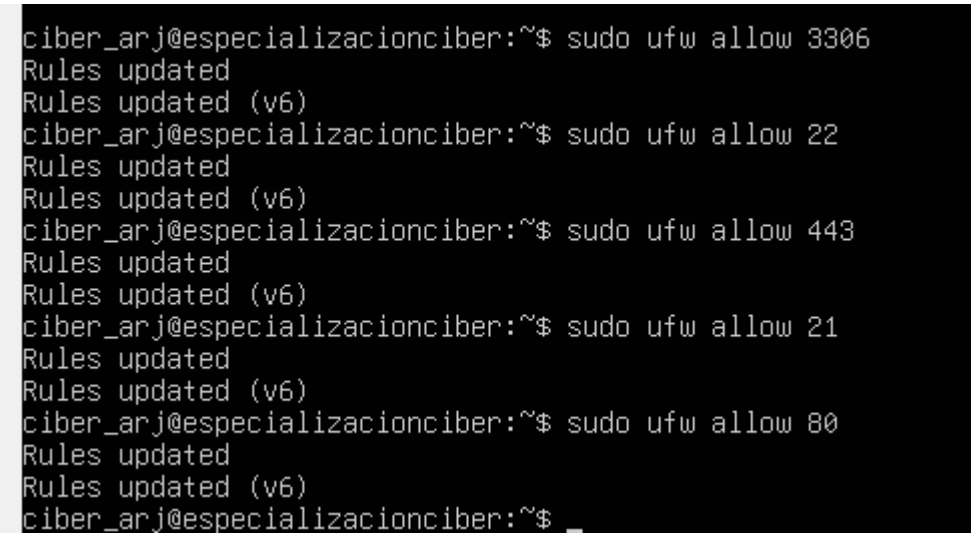




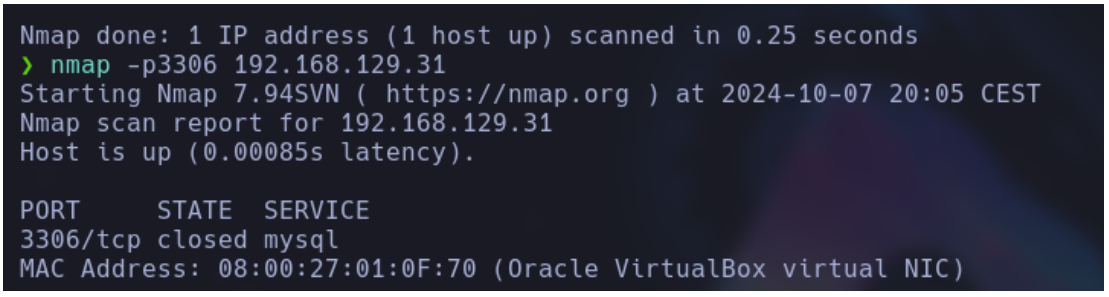
- Ahora hay que configurar el firewall de tal manera que pueda permitir solamente los puertos que se habiliten. Para ello, hay que ver en que puerto están los servicios activos. En mi caso al instala MySQL, el puerto por defecto de este es el 3306, el del SSH es el puerto 22, el de FTP en el puerto 21 y el Apache en el 80.
- Estos puertos se pueden ver con el comando:

```
nano /etc/services
```

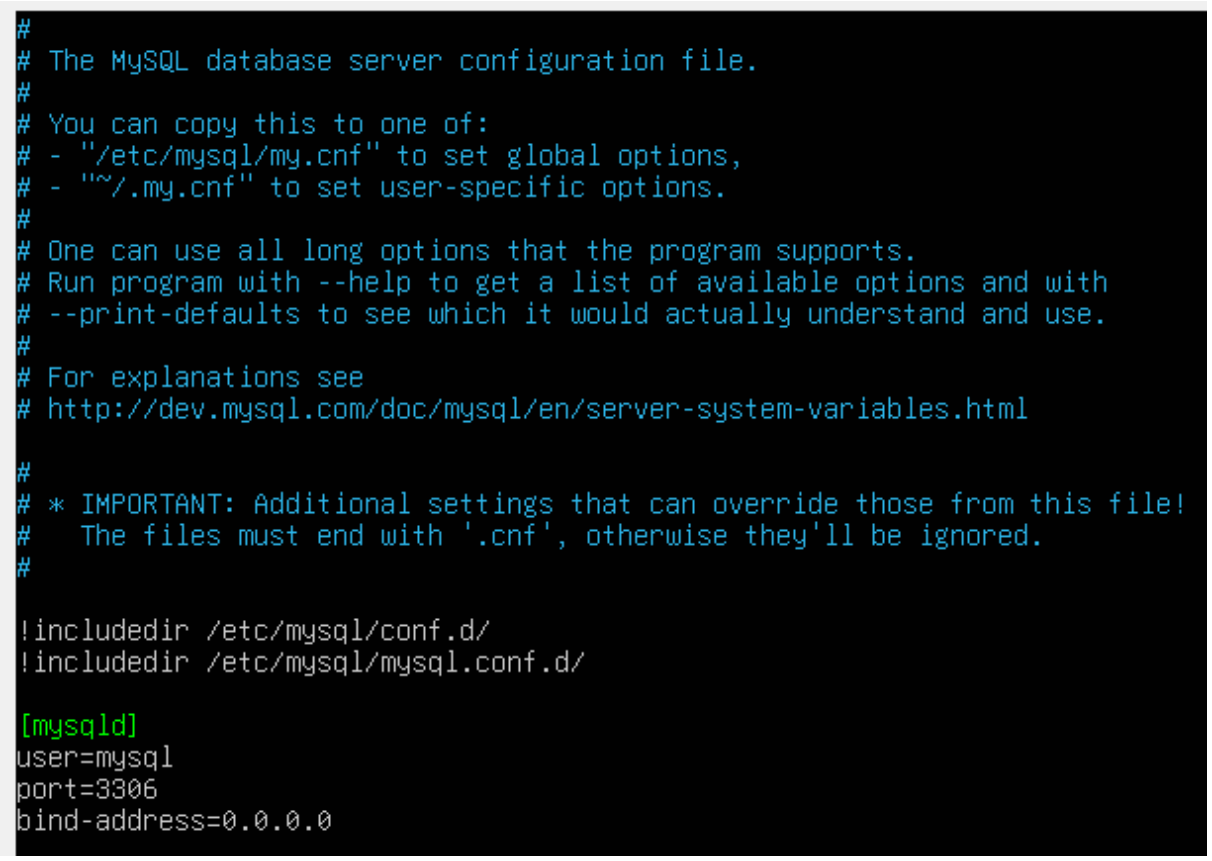
- Para habilitar el firewall, habrá que utilizar los comandos de la siguiente imagen:



- Si hacemos un escaneo de nmap, podremos ver que no nos sale nuestro servicio mysql. Ya que por defecto el puerto sale cerrado



- Por lo cual habrá que modificarlo con los parámetros de la siguiente imagen:

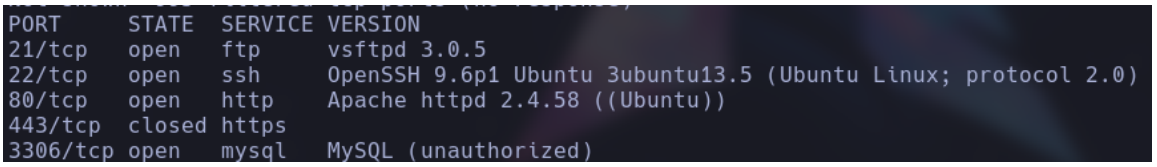


- ***ESCANEO DE PUERTOS ABIERTOS:***
  - Ahora que ya hemos configurado absolutamente todo en nuestro Ubuntu server, llega la hora de realizar un escaneo en Nmap para encontrar vulnerabilidades. Para ello utilizaremos el siguiente comando:

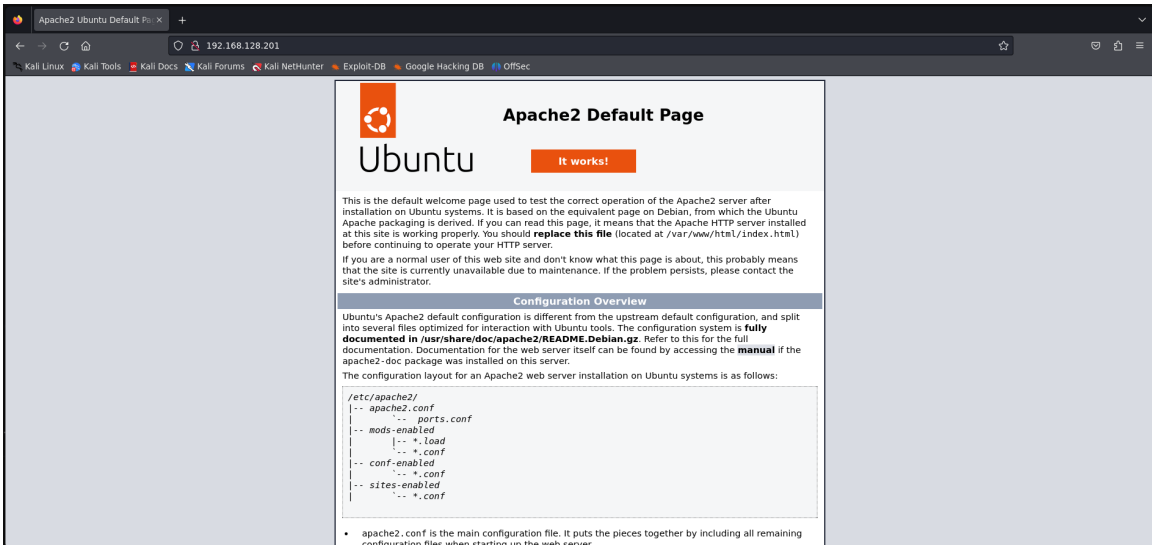
```
nmap -sS -sV -v -O 192.168.128.201
```

  - -sS: Esto significa SYN Scan. Es una opción que te permite escanear puertos de una manera rápida y efectiva en servidores que no tenga un firewall con políticas estrictas
  - -sV: Este comando te detecta la versión que esta utilizando el servicio que corre en el puerto abierto detectado
  - -O: Este comando te detecta el tipo de sistema operativo que esta corriendo en ese puerto abierto
  - -v: Este comando lo que hace es ir dando resultados a medida que los va encontrando para poder ir tocando herramientas incluso cuando no

haya acabado el escaneo.



- Esto es lo que nos ha salido con los parámetros utilizados. Como se puede ver tenemos el servicio ftp, ssh, http y mysql abiertos. Si entramos en la IP de Ubuntu Server, podremos ver que tenemos el servicio apache corriendo.



- ***DESHABILITAR SERVICIOS INNECESARIOS:***
  - Sabiendo los resultados que nos ha dado Nmap, podemos ver que tenemos el servicio ftp y ssh habilitados y corriendo. En este caso al tener ssh, el servicio ftp no nos servirá para nada ya que es un servicio mucho menos seguro y contiene mas vulnerabilidades por lo cual lo deshabilitaremos.
  - Una vez deshabilitado, tendremos que configurar ssh para que el atacante no pueda acceder al servidor con autenticación root.
  - En cuanto a MySQL, limitaremos el acceso solo a IPS de confianza
  - Y en apache intentaremos que solo se tenga acceso a información limitada de tal manera que no se pueda ver información importante
- DESHABILITAR FTP

- Para deshabilitar ftp utilizaremos el siguiente comando:

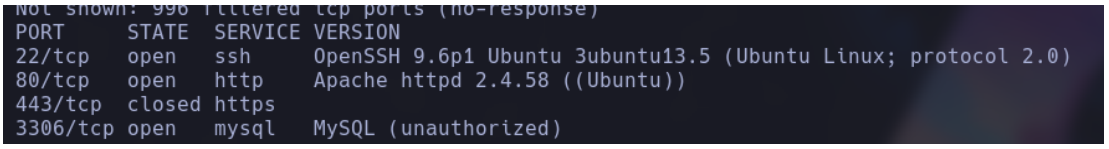
```
sudo systemctl disable vsftpd
```

- Cuando este deshabilitado, tendremos que establecer las reglas del firewall. Ya que aunq el servicio este deshabilitado, el puerto sigue abierto por lo cual utilizaremos estos comandos:

```
sudo ufw deny 21/tcp
```

```
sudo ufw deny 21
```

- Estos comandos nos cerraran los puertos por los que ftp pueda ser visible. Pra comprobar que estan cerrados, yo he reiniciado el Ubuntu server y he hecho un escaneo de nmap rápido para que me detecte solo los puertos abiertos

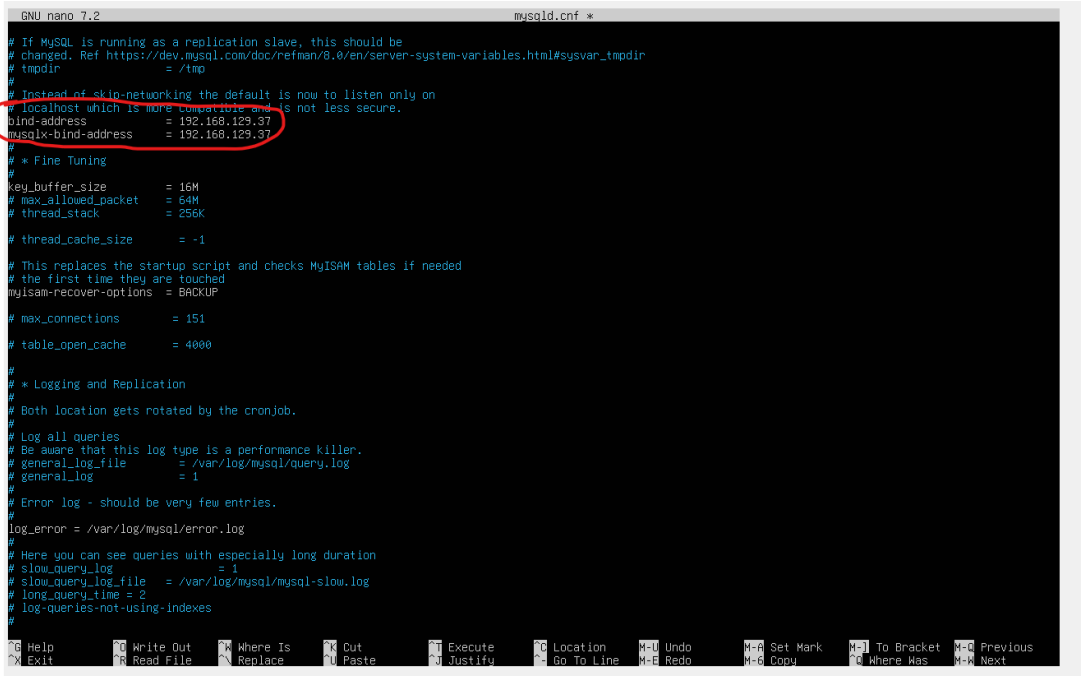


- Como se puede ver, ya no sale el servicio FTP en la máquina

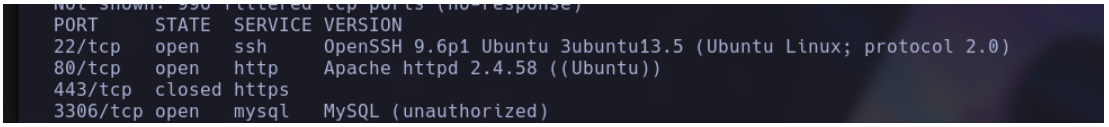
- LIMITAR ACCESO MYSQL
  - En cuanto a MySQL, no nos interesa que se tenga acceso desde todas las IPS por lo cual configuraremos desde un archivo especifico que solo tenga acceso mi maquina Kali Linux. Además queremos que funcione por lo cual no voy a deshabilitar el servicio de MySQL pero si voy a cerrar los puertos.
  - Este archivo se encuentra en el siguiente directorio

```
/etc/mysql/mysql.conf.d/mysqld.cnf
```

  - Lo editaremos como nano:



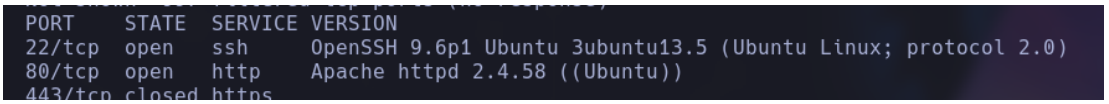
- Lo que esta recuadrado, lo cambiaremos por la IP que queramos. En mi caso la IP de Kali linux
- Como se puede ver en la siguiente imagen, nuestro kali linux detecta el mysql abierto



- Ahora cerraremos el puerto de mysql. Para ello miraremos el status de nuestro firewall con los mismos comandos anteriores

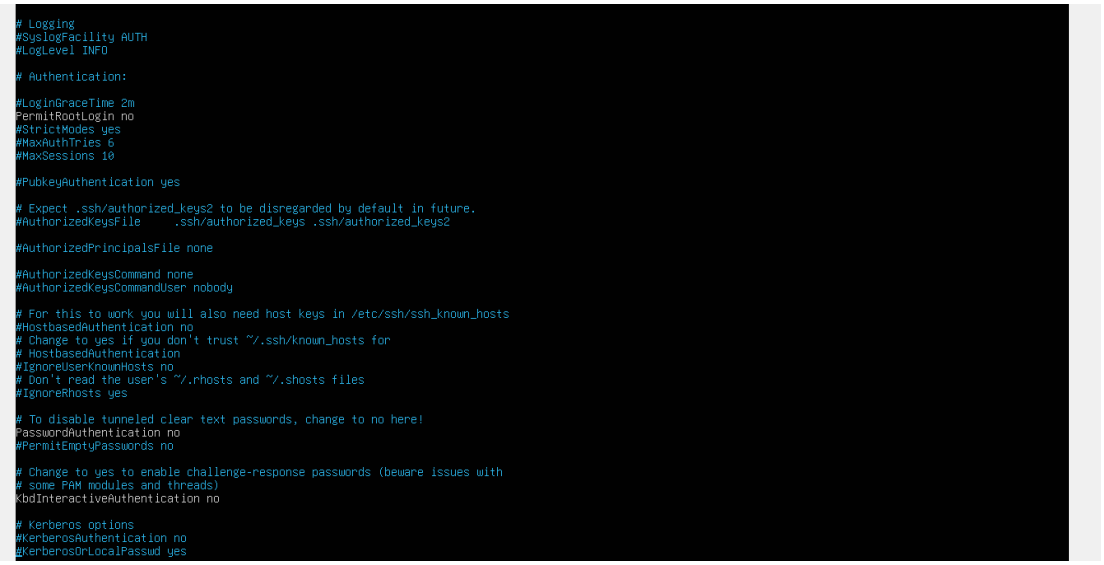
```
sudo ufw deny 3306/tcp
```

```
sudo ufw deny 3306
```



- Ya no tendremos MYSQL en los puertos abiertos. Lo tenemos totalmente seguro

- CONFIGURACIÓN SSH
  - SSH necesita los puertos abiertos ya que sin el, no podremos tener conexión remota para transferencia de archivos. Por lo cual necesitaremos aplicar una serie de reglas para que no pueda entrar cualquier equipo.
  - Hay un programa que se llama fail2ban, que lo utilizaremos para estblecer una serie de politicas pero el archivo de SSH también se podrá configurar.



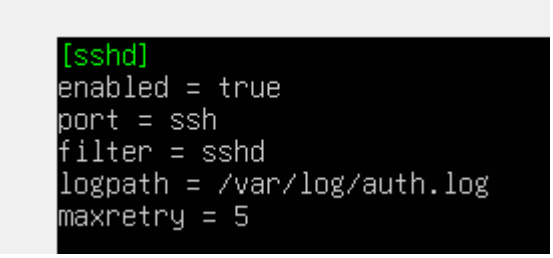
  - En esta imagen, hemos cambiado dos parámetros que son necesarios para que no entre cualquiera. Este archivo se encuentra en el directorio:

```
/etc/ssh/sshd_config
```

  - Ahora utilizaremos la herramienta fail2ban para establecer politicas de ssh. Si no se tiene instalada la herramienta, se instalara con el siguiente comando:

```
sudo apt-get install fali2ban
```

  - Crearemos un nuevo archivo con nano de tal manera que podramos escribir todas las políticas de seguridad. En ese archivo (que lo llamé jail.local) pondremos estos parámetros:



    - Una vez hecho esto, reiniciaremos el servicio con el comando de siempre

```
sudo systemctl restart fail2ban
```

- CONFIGURACIÓN APACHE
    - Apache es un servicio bastante seguro. No obstante, instalaremos una herramienta la cual nos lo proteja mas. Esta herramienta se llama “mod security”
    - La instalaremos con este comando:

```
sudo apt-get install libapache2-mod-security2
```

    - Una vez instalado, lo ejecutaremos y reiniciaremos el sistema

```
sudo a2enmod security2
```

    - Por ultimo reiniciaremos el servicio como todos con el siguiente comando:

```
sudo systemctl restart apache2
```

- CONCLUSION
    - Para el servicio FTP, lo he deshabilitado porque ya tenemos otra herramienta mucho mas segura para permitir la conexión remota
    - En cuanto a MYSQL he limitado el acceso a solo la IP que he configurado en el archivo de configuración además de cerrar los puertos para que no se vea que esta corriendo este servicio
    - SSH es un servicio que necesita tener los puertos abiertos para utilizar la conexión remota por lo cual, he actualizado las politicas de

seguridad tanto en fail2ban como en la propia configuración de SSH

- En Apache he instalado un servicio de las propias librerias de Apache para mantener el servicio https seguro
- En el firewall he deshabilitado los puertos innecesarios es decir el de mysql y el de ftp