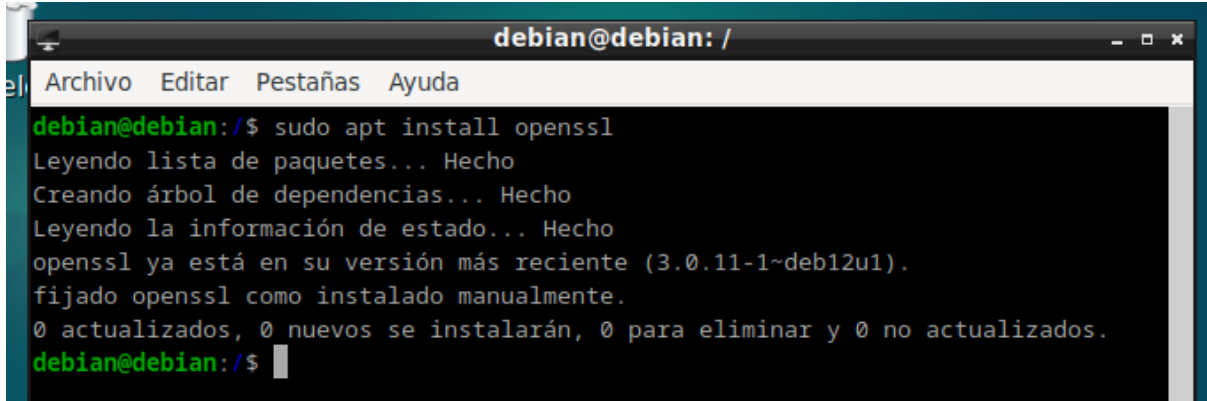


PRÁCTICA 2

Autenticación y restricciones por IP con Nginx

En esta práctica debemos instalar openssl, pues es la herramienta que vamos a emplear para la creación de contraseñas.

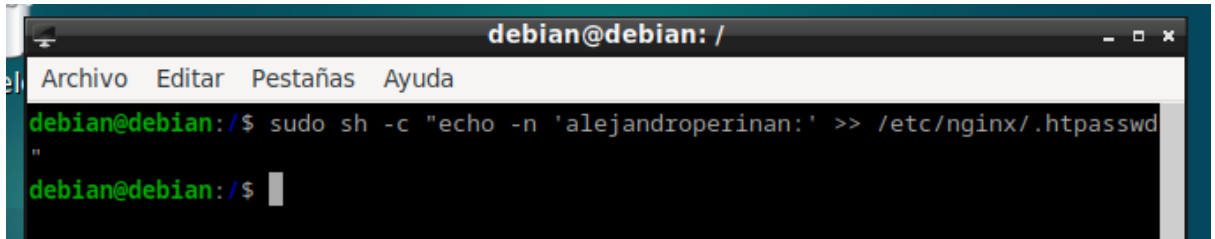
Es necesario instalar openssl: *sudo apt install openssl*



```
debian@debian: /
Archivo Editar Pestañas Ayuda
debian@debian:/$ sudo apt install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente (3.0.11-1~deb12u1).
fijado openssl como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
debian@debian:/$
```

1. Creación de un archivo “.htpasswd” donde vamos a almacenar los usuarios junto con sus contraseñas:

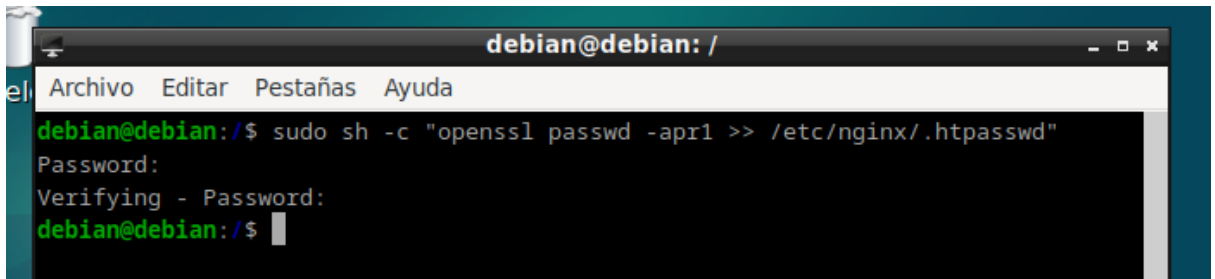
- *sudo sh -c "echo -n 'tu_nombre:' >> /etc/nginx/.htpasswd"*



```
debian@debian: /
Archivo Editar Pestañas Ayuda
debian@debian:/$ sudo sh -c "echo -n 'alejandropereira:' >> /etc/nginx/.htpasswd"
debian@debian:/$
```

2. Creación de la contraseña correspondiente al usuario anterior:

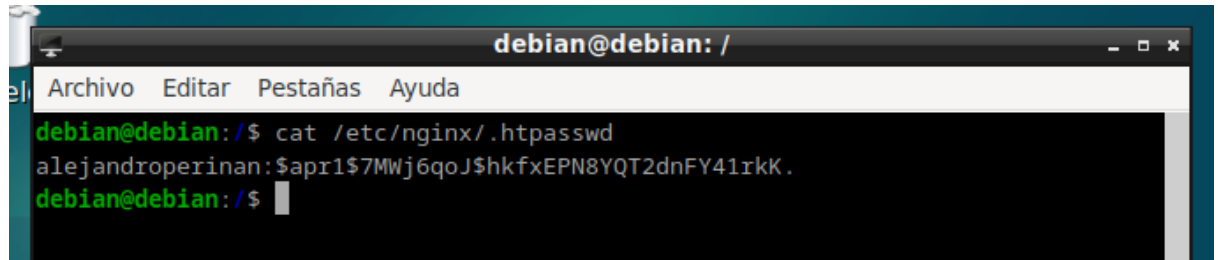
- *sudo sh -c "openssl passwd -apr1 >> /etc/nginx/.htpasswd"*



```
debian@debian: /
Archivo Editar Pestañas Ayuda
debian@debian:/$ sudo sh -c "openssl passwd -apr1 >> /etc/nginx/.htpasswd"
Password:
Verifying - Password:
debian@debian:/$
```

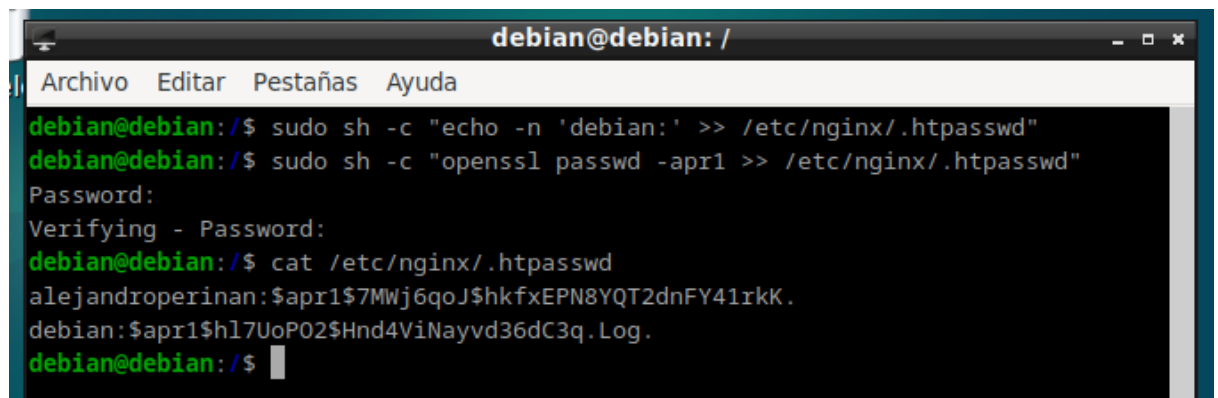
3. Vamos a comprobar que aparece el nombre del usuario anterior junto con su contraseña cifrada cifrados en el fichero `.htpasswd`

- `cat /etc/nginx/.htpasswd`



```
debian@debian: /
Archivo Editar Pestañas Ayuda
debian@debian:/$ cat /etc/nginx/.htpasswd
alejandroperinan:$apr1$7MWj6qoJ$hkfxEPN8YQT2dnFY41rkK.
debian@debian:/$
```

4. Añade un usuario más con su correspondiente contraseña y haz una captura con el contenido del archivo `.htpasswd` visto en la consola.



```
debian@debian: /
Archivo Editar Pestañas Ayuda
debian@debian:/$ sudo sh -c "echo -n 'debian:' >> /etc/nginx/.htpasswd"
debian@debian:/$ sudo sh -c "openssl passwd -apr1 >> /etc/nginx/.htpasswd"
Password:
Verifying - Password:
debian@debian:/$ cat /etc/nginx/.htpasswd
alejandroperinan:$apr1$7MWj6qoJ$hkfxEPN8YQT2dnFY41rkK.
debian:$apr1$h17UoPO2$Hnd4ViNayvd36dC3q.Log.
debian@debian:/$
```

5. Ahora debemos modificar la configuración de nuestro archivo localizado en el directorio `sites-available` para que tenga en cuenta los credenciales anteriores:

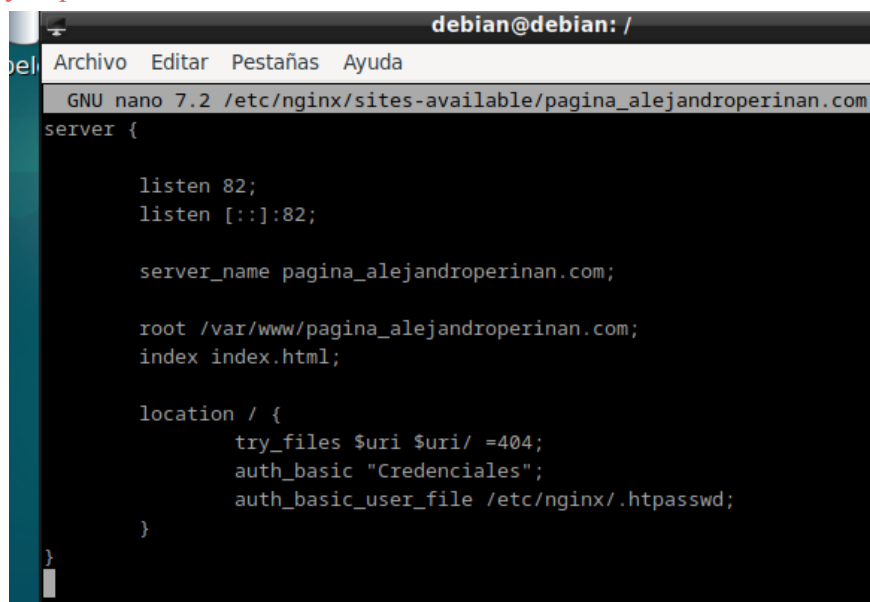
- `sudo nano /etc/nginx/sites-available/pagina_tunombre.com`

Hay que añadir las siguientes líneas dentro del área de `location`:

- `auth_basic "Credenciales";`

- `auth_basic_user_file /etc/nginx/.htpasswd;`

Haz una captura donde se muestre el nuevo aspecto del archivo `pagina_tunombre.com` y explica cuál es la función de estas 2 nuevas líneas.



```
debian@debian: /
Archivo Editar Pestañas Ayuda
GNU nano 7.2 /etc/nginx/sites-available/pagina_alejandroperinan.com
server {

    listen 82;
    listen [::]:82;

    server_name pagina_alejandroperinan.com;

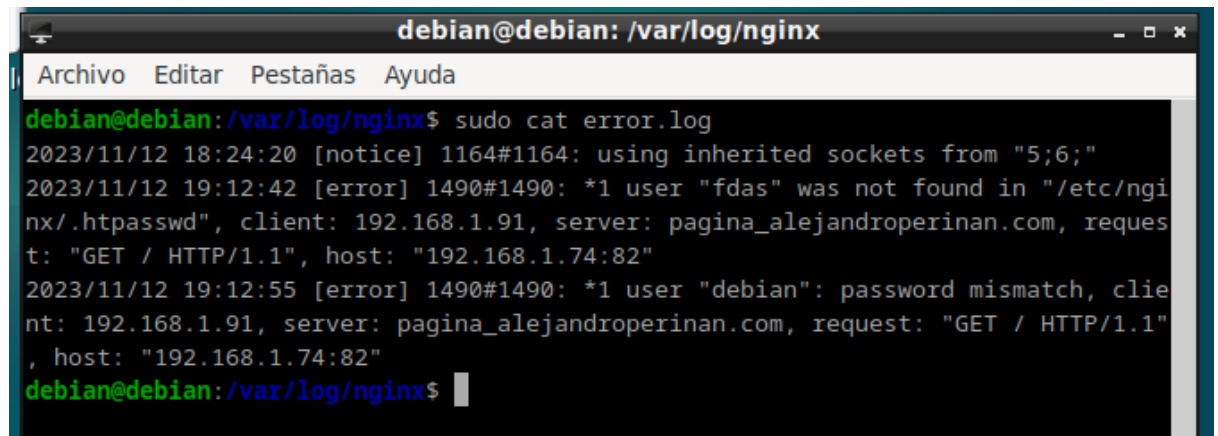
    root /var/www/pagina_alejandroperinan.com;
    index index.html;

    location / {
        try_files $uri $uri/ =404;
        auth_basic "Credenciales";
        auth_basic_user_file /etc/nginx/.htpasswd;
    }

}
```

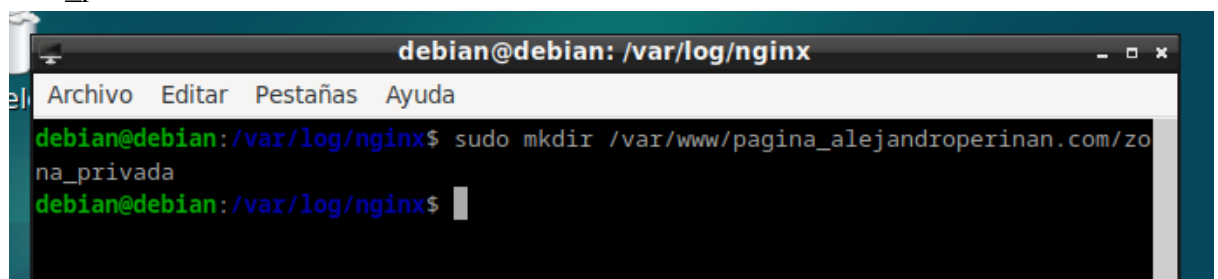
6. Reiniciamos Nginx para que se aplique la nueva configuración. Intenta acceder a la web desde el cliente. Hazlo utilizando un usuario correcto y otro incorrecto. Di los errores que aparecen y revisa el fichero de logs. Intenta acceder cancelando la autenticación. ¿Qué mensaje de error aparece? ¿Qué sucede cuando intentas acceder a la misma página por segunda vez? **Describe esto en la memoria de la práctica.**

Al entrar, se solicita al usuario que introduzca sus datos, si los datos no se encuentran en el archivo configurado anteriormente se recarga el procedimiento, en caso contrario extremos con éxito en la página.



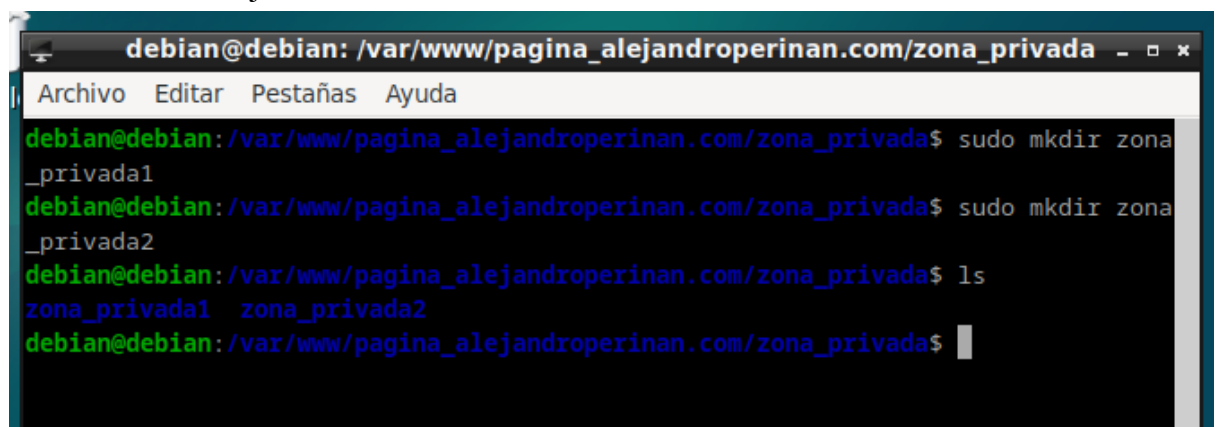
```
debian@debian: /var/log/nginx
Archivo Editar Pestañas Ayuda
debian@debian:/var/log/nginx$ sudo cat error.log
2023/11/12 18:24:20 [notice] 1164#1164: using inherited sockets from "5;6;"
2023/11/12 19:12:42 [error] 1490#1490: *1 user "fdas" was not found in "/etc/nginx/.htpasswd", client: 192.168.1.91, server: pagina_alejandroperinan.com, request: "GET / HTTP/1.1", host: "192.168.1.74:82"
2023/11/12 19:12:55 [error] 1490#1490: *1 user "debian": password mismatch, client: 192.168.1.91, server: pagina_alejandroperinan.com, request: "GET / HTTP/1.1", host: "192.168.1.74:82"
debian@debian:/var/log/nginx$
```

Hasta ahora estamos aplicando autenticación a toda nuestra página. Vamos a ver cómo hacerlo solo a ciertas partes. Para ello, dentro del directorio en el que estamos incluyendo los distintos archivos de nuestra página (/var/www/pagina_tunombre.com), debemos crear otro directorio. Por ejemplo, zona_privada.



```
debian@debian: /var/log/nginx
Archivo Editar Pestañas Ayuda
debian@debian:/var/log/nginx$ sudo mkdir /var/www/pagina_alejandroperinan.com/zona_privada
debian@debian:/var/log/nginx$
```

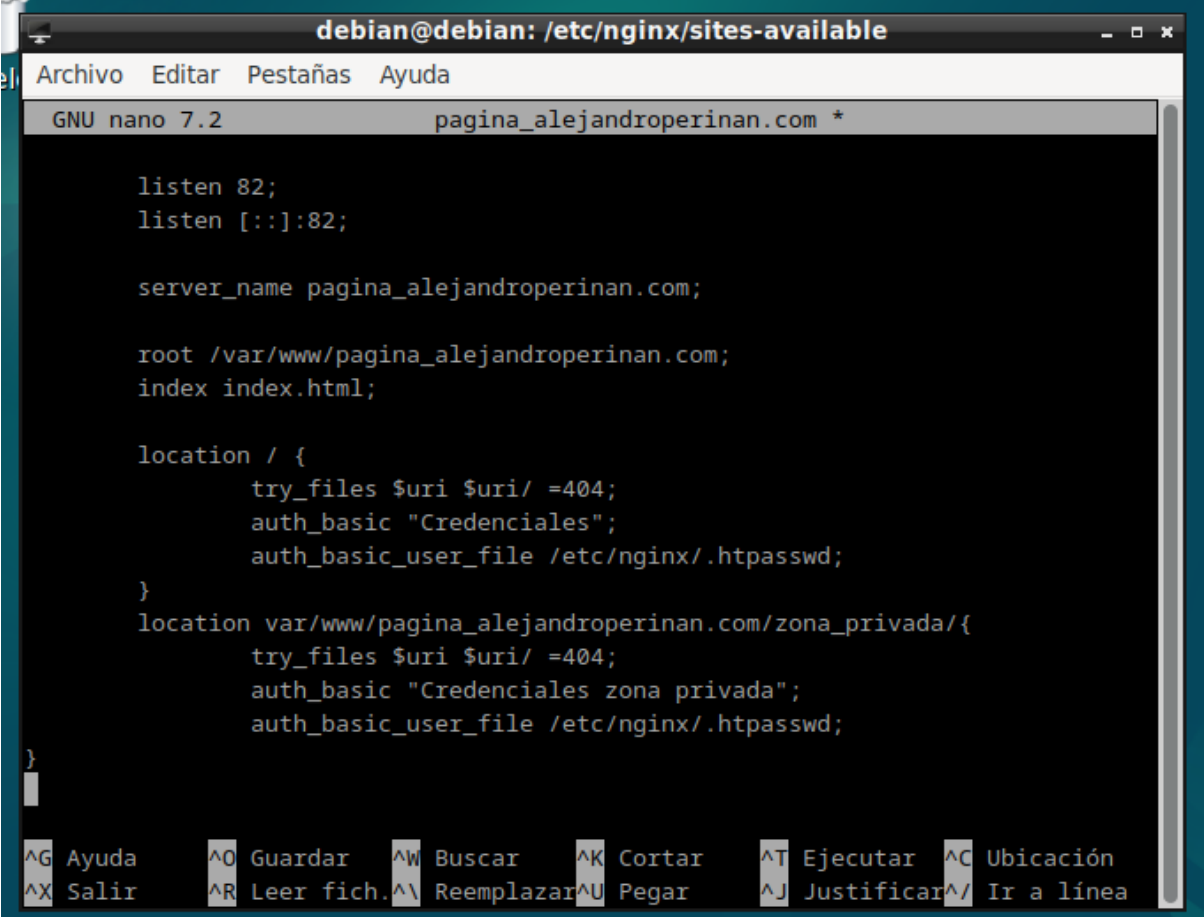
7. Dentro de este nuevo directorio, crea dos nuevas páginas html. Por ejemplo: zona_privada1 y zona_privada2. Configura cada una para que al acceder a ellas muestren un mensaje diferente.



```
debian@debian: /var/www/pagina_alejandroperinan.com/zona_privada
Archivo Editar Pestañas Ayuda
debian@debian:/var/www/pagina_alejandroperinan.com/zona_privada$ sudo mkdir zona_privada1
debian@debian:/var/www/pagina_alejandroperinan.com/zona_privada$ sudo mkdir zona_privada2
debian@debian:/var/www/pagina_alejandroperinan.com/zona_privada$ ls
zona_privada1 zona_privada2
debian@debian:/var/www/pagina_alejandroperinan.com/zona_privada$
```

8. Volvemos al archivo de la carpeta sites-available. Y lo vamos a modificar para que solo se realice el acceso previa autenticación en las páginas que acabamos de crear. Debemos crearnos un nuevo bloque location y especificar la ruta que deseamos restringir, en este caso: /zona_privada/

Realiza una captura donde se muestren los cambios realizados en el archivo de configuración.



```
debian@debian: /etc/nginx/sites-available
GNU nano 7.2 pagina_alejandroperinan.com *

listen 82;
listen [::]:82;

server_name pagina_alejandroperinan.com;

root /var/www/pagina_alejandroperinan.com;
index index.html;

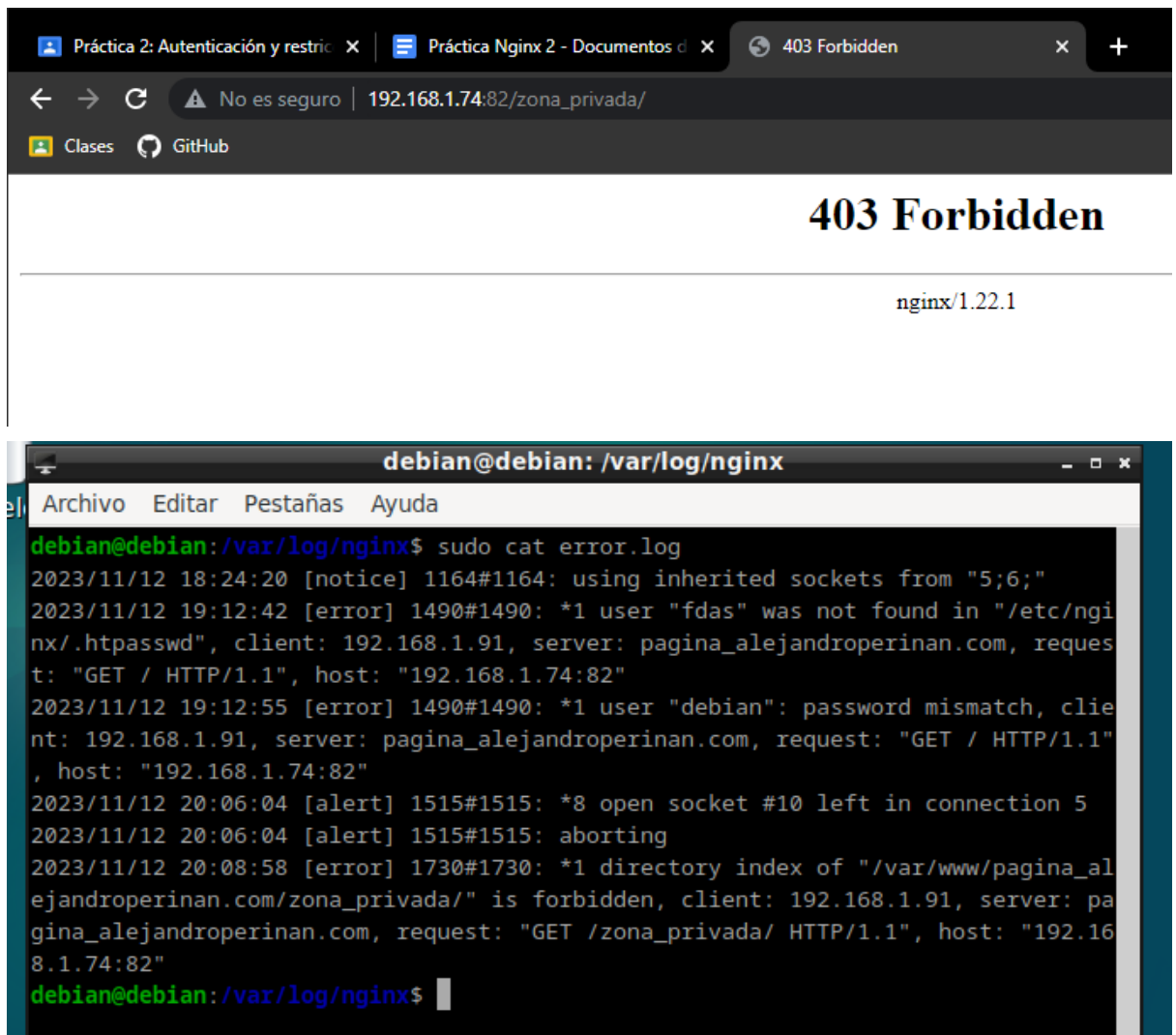
location / {
    try_files $uri $uri/ =404;
    auth_basic "Credenciales";
    auth_basic_user_file /etc/nginx/.htpasswd;
}
location var/www/pagina_alejandroperinan.com/zona_privada/{
    try_files $uri $uri/ =404;
    auth_basic "Credenciales zona privada";
    auth_basic_user_file /etc/nginx/.htpasswd;
}

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea
```

Ahora, además de la autenticación mediante usuario y contraseña, vamos a aplicar restricciones de acceso a la página mediante IP.

9. Explica cómo se deben emplear las directivas deny y allow. Configura el archivo localizado en sites available de forma que se deniegue el acceso a la máquina anfitriona (nuestro cliente). ¿Cuál es el error que nos aparece en el navegador? Revisa también el archivo error.log. Incluye estas capturas y explicación en la memoria de la práctica.

Estas directivas permiten controlar qué usuarios o direcciones IP tienen permiso para acceder a recursos específicos en el servidor.



10. ¿En qué se diferencian las directivas `satisfy all` y `satisfy any`? Sigue realizando modificaciones en la configuración del archivo de `sites-available`. En primer lugar, modifícalo para que sea necesaria autenticación o tener una cierta IP para poder acceder a la web. En segundo lugar, modifícalo para que, si queremos acceder a la `zona_privada`, sea necesario tanto tener una IP determinada como estar autenticado. Realiza una captura del archivo de configuración resultante en ambos casos, y explica qué has hecho.

Las directivas `satisfy all` y `satisfy any` son configuraciones utilizadas para especificar los requisitos de autorización que deben cumplirse para permitir el acceso a un recurso.

```
debian@debian: /etc/nginx/sites-available
Archivo  Editar  Pestañas  Ayuda
GNU nano 7.2  pagina_alejandroperinan.com *
server {

    listen 82;
    listen [::]:82;

    server_name pagina_alejandroperinan.com;

    root /var/www/pagina_alejandroperinan.com;
    index index.html;

    location / {
        try_files $uri $uri/ =404;
        satisfy all;
        allow 192.168.1.91;
        deny all;
        auth_basic "Credenciales";
        auth_basic_user_file /etc/nginx/.htpasswd;
    }
    location var/www/pagina_alejandroperinan.com/zona_privada/{
        try_files $uri $uri/ =404;
    }
}

^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich. ^\ Reemplazar ^U Pegar  ^J Justificar ^/ Ir a línea
```

```
debian@debian: /etc/nginx/sites-available
Archivo  Editar  Pestañas  Ayuda
GNU nano 7.2  pagina_alejandroperinan.com *
server {

    listen 82;
    listen [::]:82;

    server_name pagina_alejandroperinan.com;

    root /var/www/pagina_alejandroperinan.com;
    index index.html;

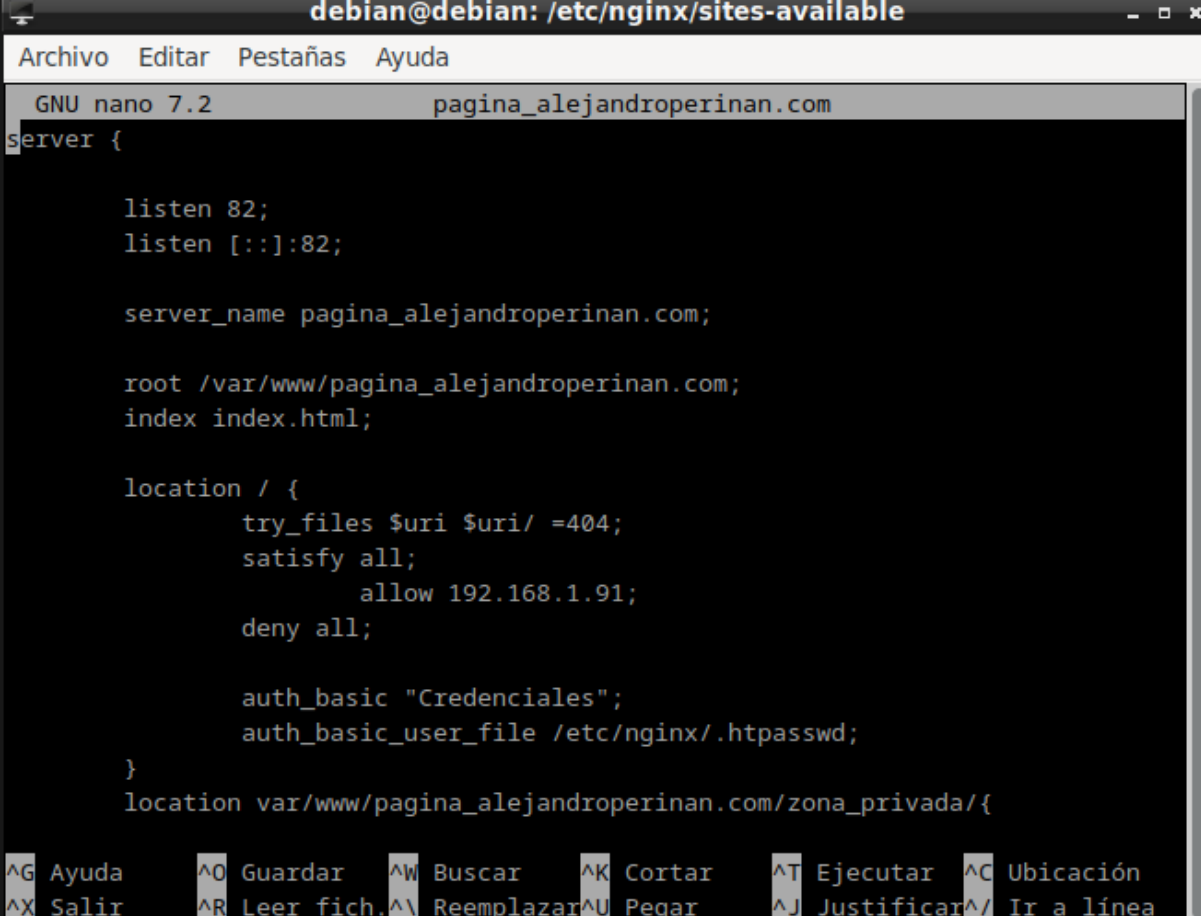
    location / {
        try_files $uri $uri/ =404;
        satisfy all;
        deny all;
        deny 192.168.1.91;
        auth_basic "Credenciales";
        auth_basic_user_file /etc/nginx/.htpasswd;
    }
    location var/www/pagina_alejandroperinan.com/zona_privada/{
        try_files $uri $uri/ =404;
    }
}

^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich. ^\ Reemplazar ^U Pegar  ^J Justificar ^/ Ir a línea
```

11. ¿Qué líneas añadirías en caso de que quieras que tu página sea accesible a las direcciones del grupo 192.168.59.1/24 y 192.168.80.1/24, exceptuando la dirección 192.168.59.20? No queremos que ninguna otra dirección IP pueda acceder a nuestro sitio.

```
allow 192.168.59.0/24;  
allow 192.168.80.0/24;  
deny 192.168.59.20;  
deny all;
```

12. Configura el archivo para que puedas acceder con la IP del cliente y además también se necesite realizar la autenticación. **Añade una captura del archivo de configuración.**



The screenshot shows a terminal window titled "debian@debian: /etc/nginx/sites-available". The window contains the nano 7.2 text editor editing the file "pagina_alejandroperinan.com". The configuration is as follows:

```
server {  
  
    listen 82;  
    listen [::]:82;  
  
    server_name pagina_alejandroperinan.com;  
  
    root /var/www/pagina_alejandroperinan.com;  
    index index.html;  
  
    location / {  
        try_files $uri $uri/ =404;  
        satisfy all;  
        allow 192.168.1.91;  
        deny all;  
  
        auth_basic "Credenciales";  
        auth_basic_user_file /etc/nginx/.htpasswd;  
    }  
    location var/www/pagina_alejandroperinan.com/zona_privada/{
```

At the bottom of the terminal, there is a row of keyboard shortcuts for nano:

^G	Ayuda	^O	Guardar	^W	Buscar	^K	Cortar	^T	Ejecutar	^C	Ubicación
^X	Salir	^R	Leer fich.	^\\	Reemplazar	^U	Pegar	^J	Justificar	^/	Ir a línea

13. Imagina que mi IP es 192.168.20.24, y quiero acceder al directorio “series” de una página web que tiene la configuración de la imagen adjunta. ¿Podré acceder a esa sección? ¿Por qué?

```
location /series/ {  
  
    satisfy all;  
    allow 192.168.20.22;  
    deny all;  
    allow 192.168.20.1/24;  
  
    auth_basic "Esta zona está restringida";  
    auth_basic_user_file /.htpasswd;  
  
    try_files $uri $uri/ =404;  
}
```

No podrá, ya que del grupo de IPs 192.168.20.1/24 solo esta admitida la IP 192.168.20.22.