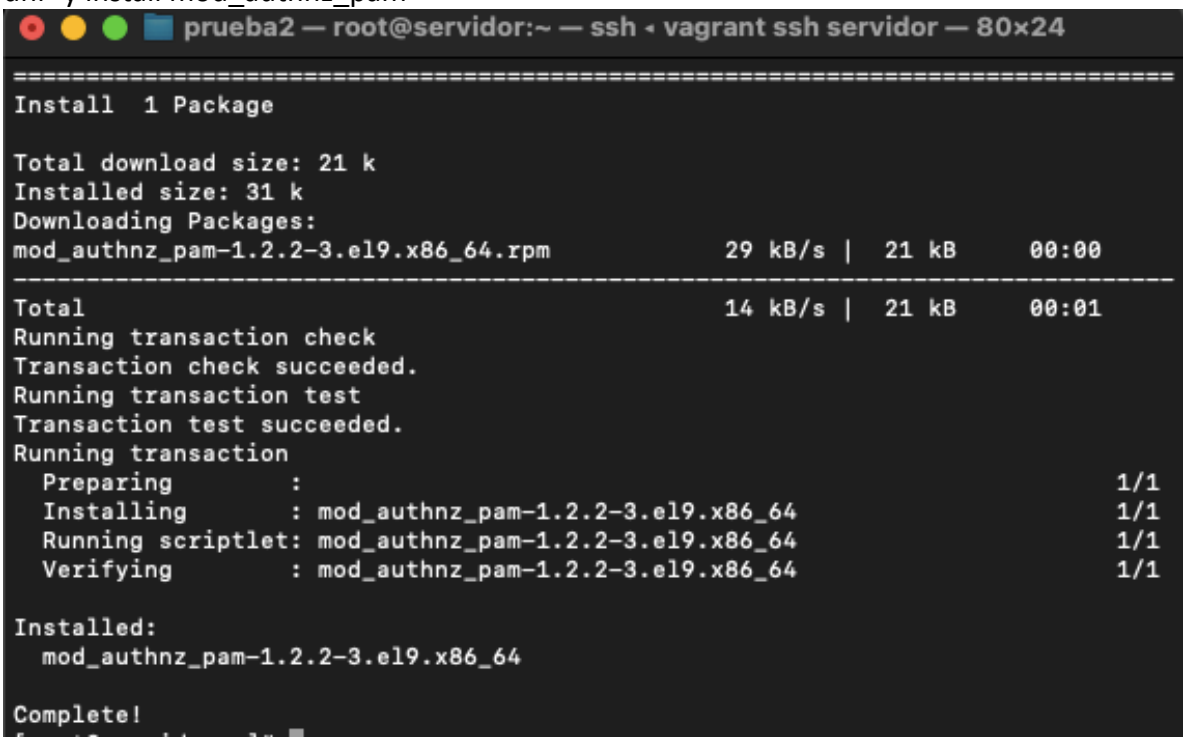
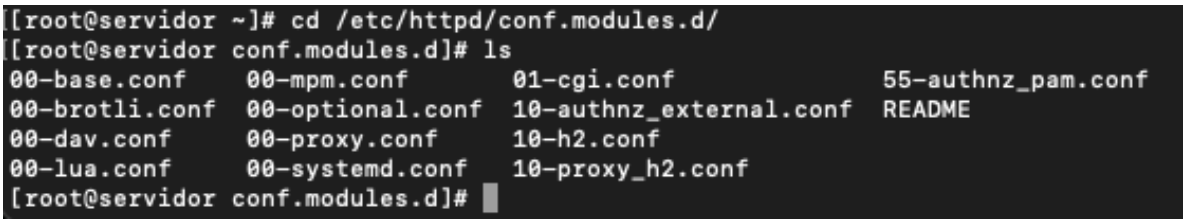
Ingresamos a nuestra máquina virtual servidor

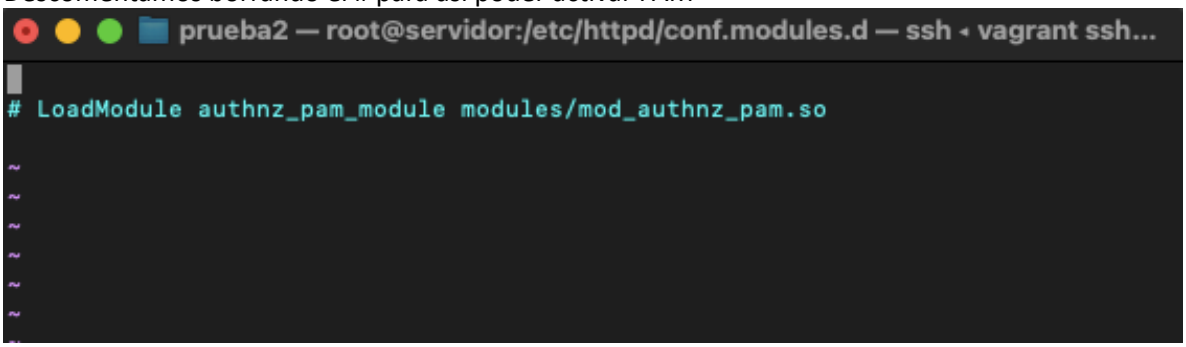
Instalamos PAM:
dnf -y install mod_authnz_pam



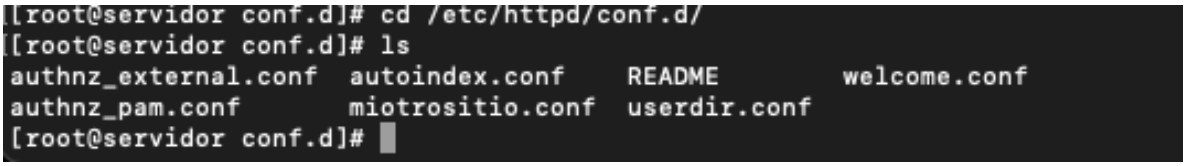
Ingresamos a conf.modules.d:
cd /etc/httpd/conf.modules.d/
ls



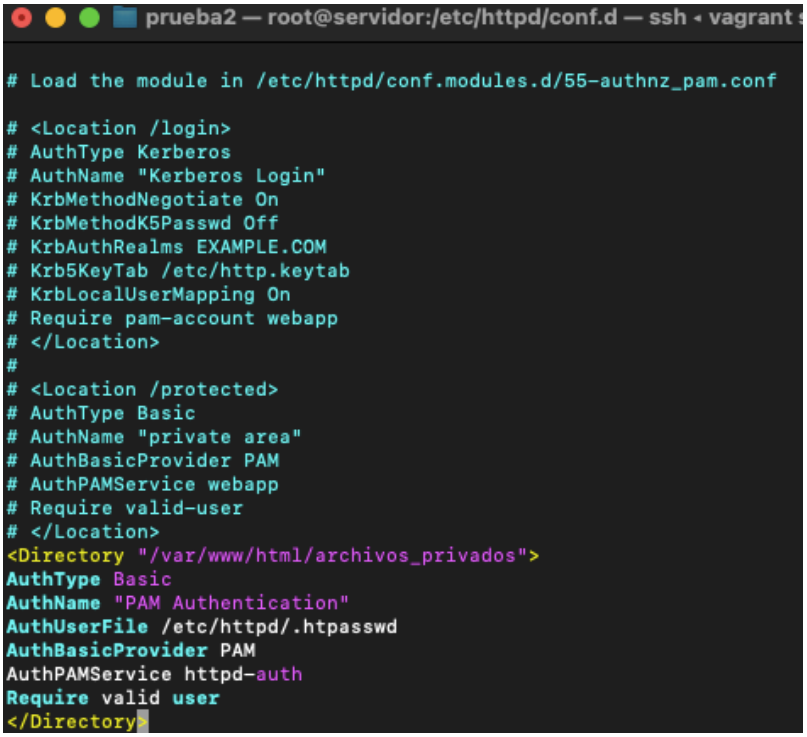
Editamos el archivo 55-authnz_pam.conf
sudo vim 55-authnz_pam.conf
Descomentamos borrando el # para así poder activar PAM



Ahora vamos a conf.d:
cd /etc/httpd/conf.d/
ls



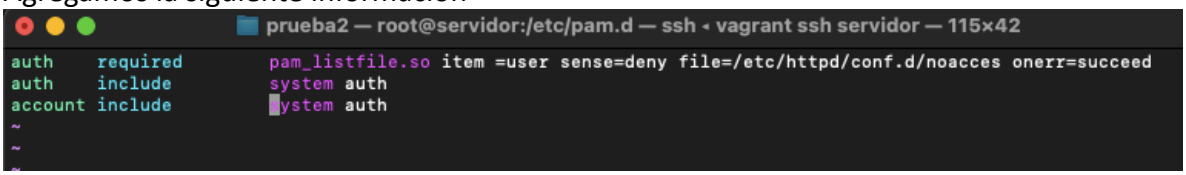
Editamos el archivo authnz_pam.conf el cual es el archivo de configuración PAM
sudo vim authnz_pam.conf



En la ruta cd /etc/pam.d/ creamos el archivo `vim httpd–authentication` y agregamos la configuración:

```
[[root@servidor ~]# cd /etc/pam.d/
[[root@servidor pam.d]# ls
 apache-auth        other           remote            su             vlock
[config-util        passwd          runuser           sudo           vsftpd
[crond              password-auth   runuser-l         sudo-i
 fingerprint-auth   polkit-1        smartcard-auth    su-l
 httpd-auth         postlogin       sshd              system-auth
 login              pwauth          sssd-shadowutils  systemd-user
```

Agregamos la siguiente información



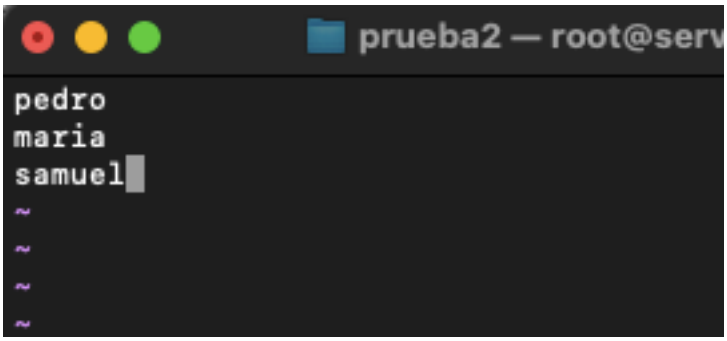
USUARIOS DENEGADOS

Vamos a la siguiente ruta:

cd /etc/httpd/conf.d/

Creamos el archivo para guardar los usuarios denegados

vim noacces



Damos permisos

chgrp apache /etc/httpd/conf.d/noacces
chmod 640 /etc/httpd/conf.d/noacces

Ahora cambiomos el permiso httpd para que puede leer

chgrp apache /etc/shadow
chmod 440 /etc/shadow

```
[[root@servidor conf.d]# chgrp apache /etc/httpd/conf.d/noacces
[[root@servidor conf.d]# chmod 640 /etc/httpd/conf.d/noacces
[[root@servidor conf.d]# chgrp apache /etc/shadow
[[root@servidor conf.d]# chmod 440 /etc/shadow
```

Reiniciamos el httpd:
systemctl restart httpd

Creamos el directorio de archivos_privados en la siguiente ruta:
cd /var/www/html/
mkdir archivos_privados

```
[[root@servidor conf.d]# systemctl restart httpd
[[root@servidor conf.d]# cd /var/www/html/
[[root@servidor html]# ls
directorio_prot  inventario  main.html
[[root@servidor html]# mkdir archivos_privados
[[root@servidor html]# ls
archivos_privados  directorio_prot  inventario  main.html
[root@servidor html]#
```

Entramos al archivos_privados
cd archivos_privados
`vim index.html`

prueba2 — root@servidor:/var/www/html/archivos_privados — ssh ◂ vagrant ssh se

```
<!DOCTYPE html>
<html>
<head>
    <title>Página de Acceso Privado</title>
</head>
<body>
    <h1>Hola, esta es la página de Acceso Privado</h1>
    <p>Bienvenido a mi página personal para la demostracion del parcial practivo</p>
</body>
</html>

~
~
~
```

Asignamos permisos al index.html
chmod 755 index.html

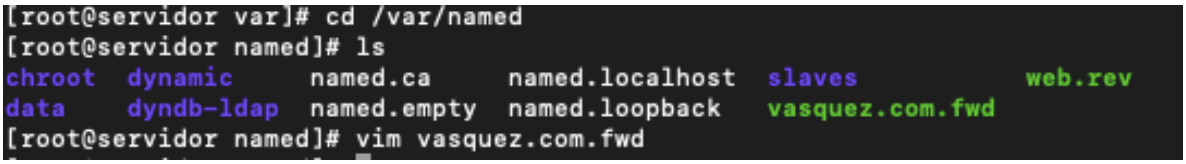
```
[[root@servidor archivos_privados]# chmod 755 index.html
[[root@servidor archivos_privados]# ls
 index.html
 [root@servidor archivos_privados]#
```

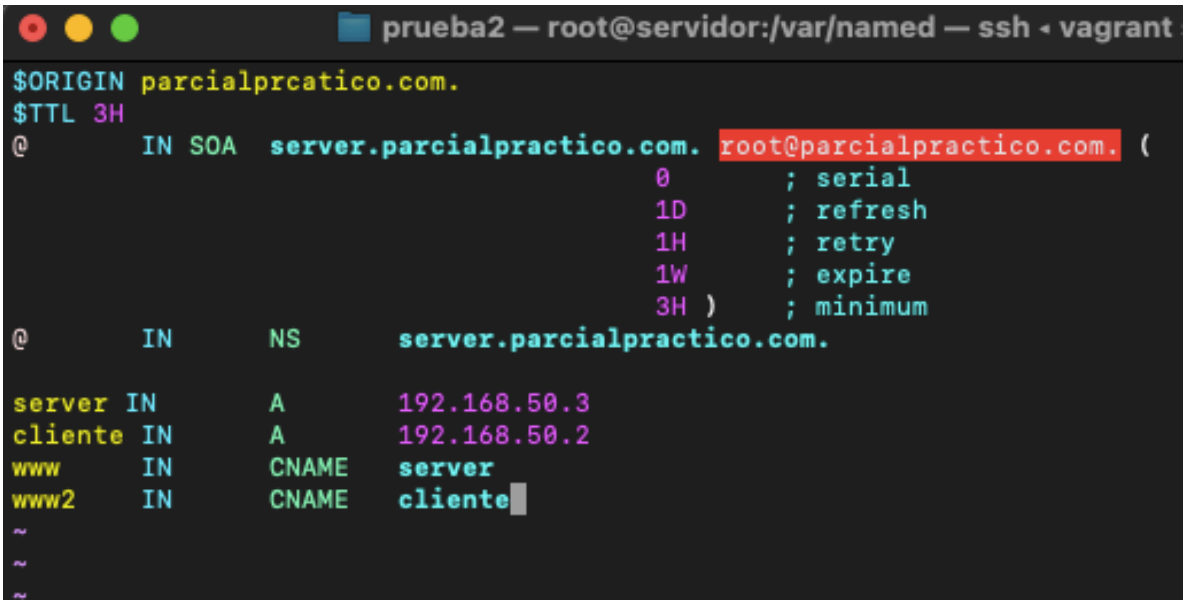
CREACION DEL VirtualHost para poder acceder desde nuestro navegador
cd /etc/httpd/conf
ls
Editamos el `httpd.conf`
`Vim httpd.conf`

```
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts.  See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
<VirtualHost *:80>
    ServerName www.parcialpractico.com
    DocumentRoot /var/www/html/
</VirtualHost>

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a
# have to place corresponding `LoadModule' lines at this location so t
# directives contained in it are actually available _before_ they are
```

CREACION DE LOS DNS
cd /etc/
sudo vim named.conf





Almacenamos usuarios y contraseñas

`htpasswd –c /etc/httpd/.htpasswd martin`

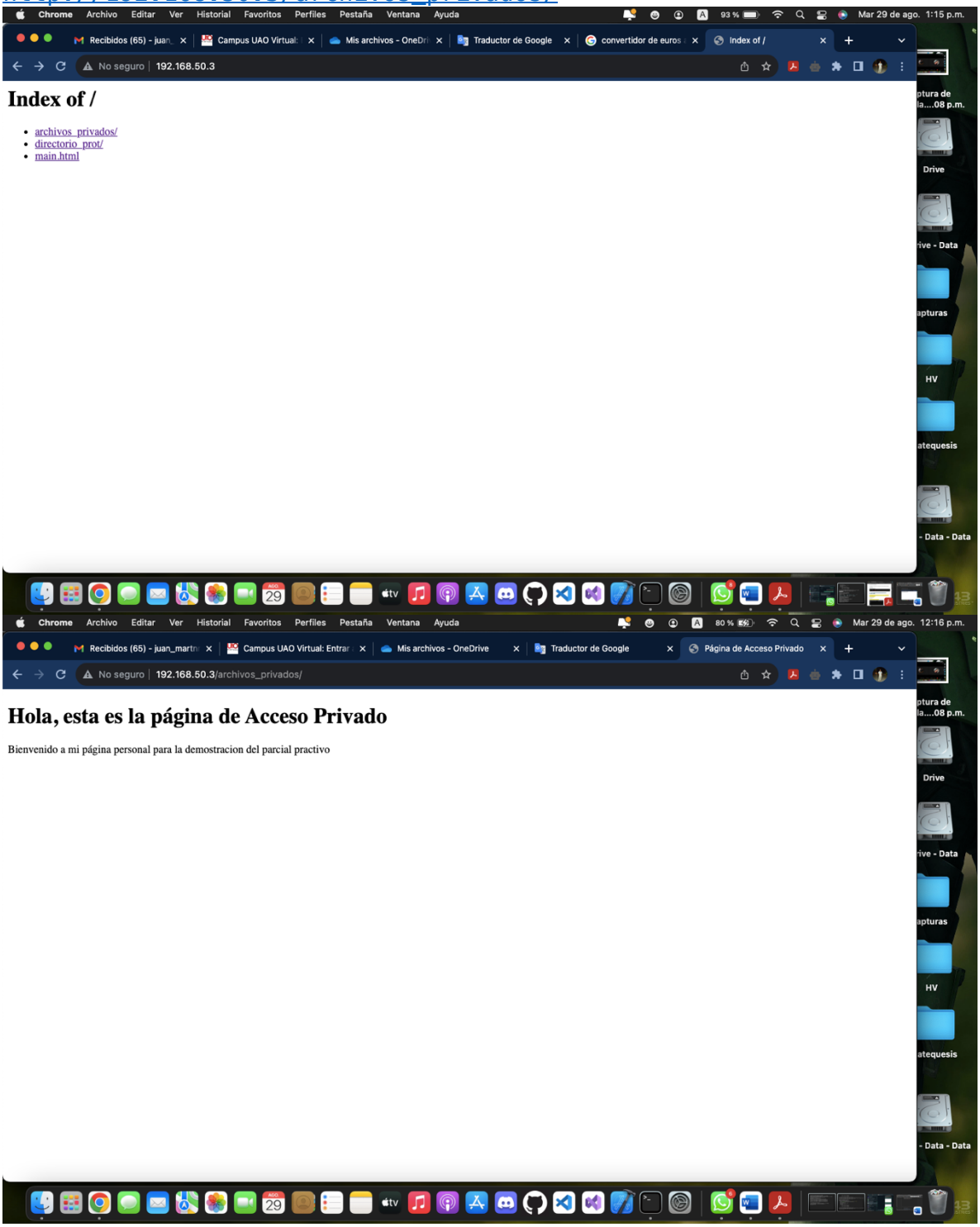
Tntmasc4

`cat /etc/httpd/.htpasswd`

Para adicionar un archico de contraseñas usamos:

sudo htpasswd /etc/httpd/claves <nombre_usuario>

http://192.168.50.3/archivos_privados/



Cómo se garantiza que la autenticación se realice mediante PAM y cómo se aplica la denegación de acceso a la lista de usuarios?

Autenticación mediante PAM:

PAM (Plugable Authentication Module) es un marco de autenticación que permite a los sistemas Unix-like (como Linux) controlar cómo se autentican los usuarios. En tu configuración de Apache, has utilizado PAM para gestionar la autenticación de los usuarios que intentan acceder a un recurso protegido.

En la configuración de Apache, has definido la autenticación básica (AuthType Basic) en el directorio /archivos_privados. Esto significa que cuando un usuario intenta acceder a ese directorio, Apache requerirá un nombre de usuario y contraseña válidos.

La línea AuthUserFile "/ruta/a/tu/archivo/.htpasswd" especifica la ubicación del archivo .htpasswd, que almacena los nombres de usuario y las contraseñas. Esto garantiza que solo los usuarios con credenciales válidas puedan autenticarse.

Denegación de acceso a usuarios:

Has creado un archivo llamado usuarios_denegados.txt que contiene los nombres de usuario que deben ser denegados el acceso al directorio /archivos_privados. Luego, has configurado la directiva Deny from file en el VirtualHost para restringir el acceso a estos usuarios.

Cuando un usuario intenta acceder al directorio protegido, Apache verifica si su nombre de usuario se encuentra en el archivo usuarios_denegados.txt. Si se encuentra en la lista, Apache niega el acceso y muestra un error 403.

En resumen, garantizas que la autenticación se realice mediante PAM configurando AuthType Basic y AuthUserFile, y aplicas la denegación de acceso a usuarios específicos al configurar la directiva Deny from file.

Tercera Parte