

Ingresamos a nuestra máquina virtual servidor

Instalamos PAM:

dnf -y install mod_authnz_pam

```
prueba2 — root@servidor:~ — ssh - vagrant ssh servidor — 80x24

=====
Install 1 Package

Total download size: 21 k
Installed size: 31 k
Downloading Packages:
mod_authnz_pam-1.2.2-3.el9.x86_64.rpm                29 kB/s | 21 kB    00:00
-----
Total                                              14 kB/s | 21 kB    00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : mod_authnz_pam-1.2.2-3.el9.x86_64 1/1
  Running scriptlet: mod_authnz_pam-1.2.2-3.el9.x86_64 1/1
  Verifying      : mod_authnz_pam-1.2.2-3.el9.x86_64 1/1

Installed:
  mod_authnz_pam-1.2.2-3.el9.x86_64

Complete!
```

Ingresamos a conf.modules.d:

cd /etc/httpd/conf.modules.d/

ls

```
[root@servidor ~]# cd /etc/httpd/conf.modules.d/
[root@servidor conf.modules.d]# ls
00-base.conf      00-mpm.conf      01-cgi.conf      55-authnz_pam.conf
00-brotli.conf    00-optional.conf 10-authnz_external.conf README
00-dav.conf       00-proxy.conf    10-h2.conf
00-lua.conf       00-systemd.conf  10-proxy_h2.conf
[root@servidor conf.modules.d]#
```

Editamos el archivo 55-authnz_pam.conf

sudo vim 55-authnz_pam.conf

Descomentamos borrando el # para así poder activar PAM

```
prueba2 — root@servidor:/etc/httpd/conf.modules.d — ssh ◀ vagrant ssh...
# LoadModule authnz_pam_module modules/mod_authnz_pam.so
```

Ahora vamos a conf.d:

cd /etc/httpd/conf.d/

ls

```
[root@servidor conf.d]# cd /etc/httpd/conf.d/
[root@servidor conf.d]# ls
authnz_external.conf  autoindex.conf  README  welcome.conf
authnz_pam.conf       miositio.conf   userdir.conf
[root@servidor conf.d]#
```

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

sudo vim authnz_pam.conf

```
prueba2 — root@servidor:/etc/httpd/conf.d — ssh ◀ vagrant t
# Load the module in /etc/httpd/conf.modules.d/55-authnz_pam.conf

# <Location /login>
# AuthType Kerberos
# AuthName "Kerberos Login"
# KrbMethodNegotiate On
# KrbMethodK5Passwd Off
# KrbAuthRealms EXAMPLE.COM
# Krb5KeyTab /etc/httpd.keytab
# KrbLocalUserMapping On
# Require pam-account webapp
# </Location>
#
# <Location /protected>
# AuthType Basic
# AuthName "private area"
# AuthBasicProvider PAM
# AuthPAMService webapp
# Require valid-user
# </Location>
<Directory "/var/www/html/archivos_privados">
AuthType Basic
AuthName "PAM Authentication"
AuthUserFile /etc/httpd/.htpasswd
AuthBasicProvider PAM
AuthPAMService httpd-auth
Require valid user
</Directory>
```

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-1       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

```
auth    required    pam_listfile.so item=user sense=deny file=/etc/httpd/conf.d/noaccess onerr=succeed
auth    include     system auth
account include     system auth
~
~
~
```

USUARIOS DENEGADOS

Vamos a la siguiente ruta:

`cd /etc/httpd/conf.d/`

Creamos el archivo para guardar los usuarios denegados

`vim noaccess`

```
pedro
maria
samuel
~
~
~
~
```

Damos permisos

```
chgrp apache /etc/httpd/conf.d/noaccess  
chmod 640 /etc/httpd/conf.d/noaccess
```

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

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

```
# Change this to listen on a specific IP address, but note that if
# 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 the
# directives contained in it are actually available _before_ they are
# statically compiled modules (those listed by 'httpd -l') do not need
```

CREACION DE LOS DNS

cd /etc/

sudo vim named.conf

```
prueba2 — root@servidor:/etc — ssh — va
};
include "/etc/crypto-policies/back-ends/bind.config";
};
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};
zone "." IN {
    type hint;
    file "named.ca";
};
/* Zona hacia adelante*/
zone "vasquez.com" IN {
    type master;
    file "vasquez.com.fwd";
};
/* Zona reversa*/
zone "web" IN {
    type master;
    file "web.rev";
};
/* Zona hacia adelante*/
zone "parcialpractico.com" IN {
    type master;
    file "parcialpractico.com.fwd";
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
-- INSERT --
```

```
[root@servidor var]# cd /var/named
[root@servidor named]# ls
chroot  dynamic  named.ca    named.localhost  slaves  web.rev
data    dyndb-ldap  named.empty  named.loopback   vasquez.com.fwd
[root@servidor named]# vim vasquez.com.fwd
```

```

prueba2 — root@servidor:/var/named — ssh ◀ vagrant
$ORIGIN parcialprcatico.com.
$TTL 3H
@      IN SOA  server.parcialpractico.com. root@parcialpractico.com. (
                                0      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
@      IN     NS   server.parcialpractico.com.
server IN     A    192.168.50.3
cliente IN    A    192.168.50.2
www      IN    CNAME server
www2     IN    CNAME cliente
~
~
~

```

Almacenamos usuarios y contraseñas

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

Tntmasc4

```
cat /etc/httpd/.htpasswd
```

```

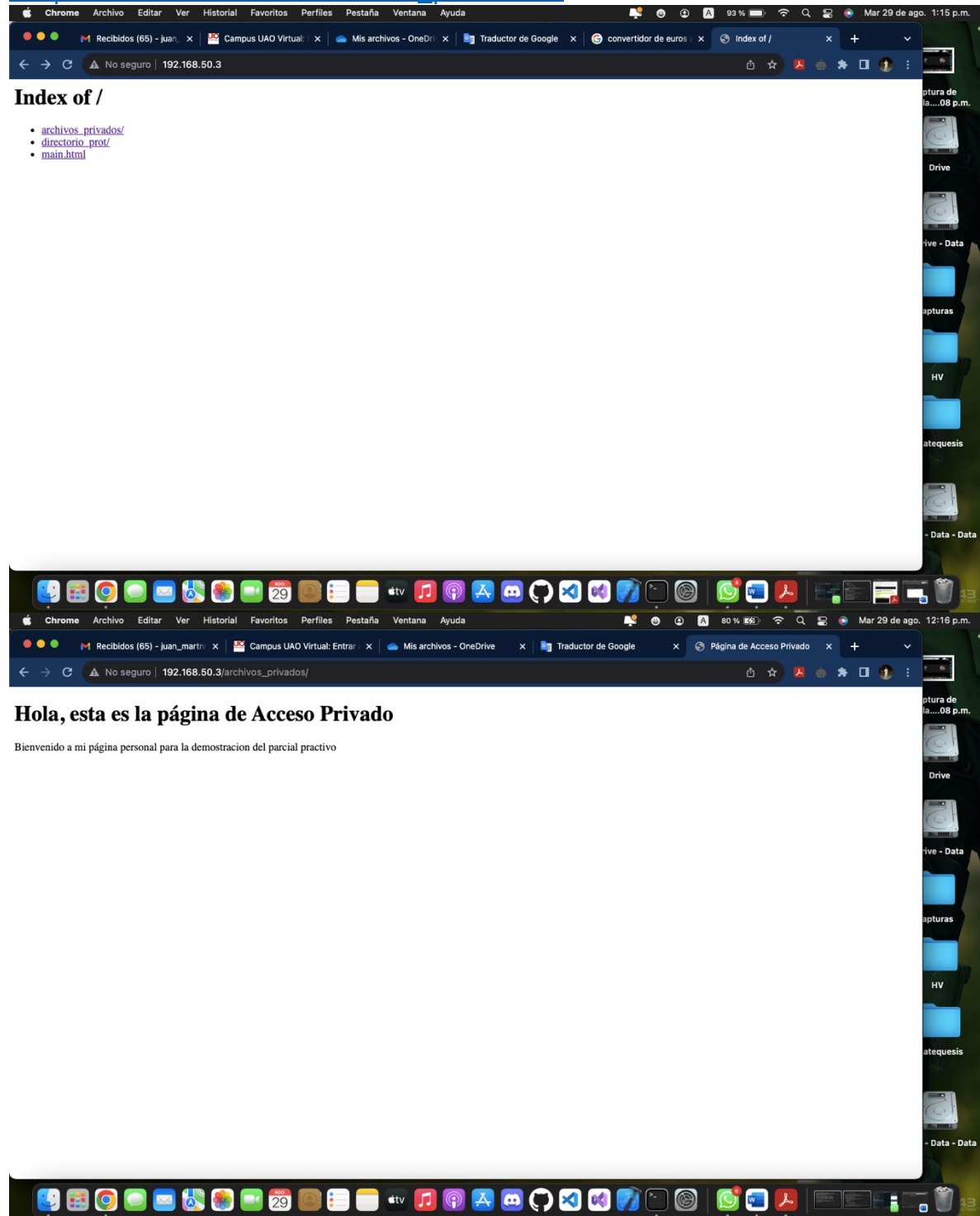
[root@servidor named]# htpasswd -c /etc/httpd/.htpasswd martin
New password:
Re-type new password:
Adding password for user martin
[root@servidor named]# cat /etc/httpd/.htpasswd
martin:$apr1$HmDAVbhF$2JkGshVtoytEqK02aQscY0
[root@servidor named]#

```

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 (Pluggable 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

```
ngrok — -zsh — 91x24
Last login: Thu Aug 24 11:27:24 on ttys000
juanmartinvasquezcaicedo@JUANS-MacBook-Air-5 ~ % cd desktop/ngrok
juanmartinvasquezcaicedo@JUANS-MacBook-Air-5 ngrok % ./ngrok config add-authtoken 2URBSERRx]
SP3slnUJ08QipDANKE_2GsTKWu9ugp3xqMz1koUp
Auth token saved to configuration file: /Users/juanmartinvasquezcaicedo/jjjjjjjjjjjjjjjjjjjjj
juanmartinvasquezcaicedo@JUANS-MacBook-Air-5 ngrok % ./ngrok http 80
```

```
ngrok — ngrok http 80 — 125x23
ngrok (Ctrl+C to quit)
Take our ngrok in production survey! https://forms.gle/aXiBFwzEA36DudFn6

Session Status      online
Account             JMartin27 (Plan: Free)
Version             3.3.4
Region              United States (us)
Latency             107ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://a227-2800-484-af8d-7600-d6c-913c-d80d-cc1d.ngrok-free.app -> http://localhost:80

Connections      ttl    opn    rt1    rt5    p50    p90
                  0      0      0.00  0.00  0.00  0.00
```