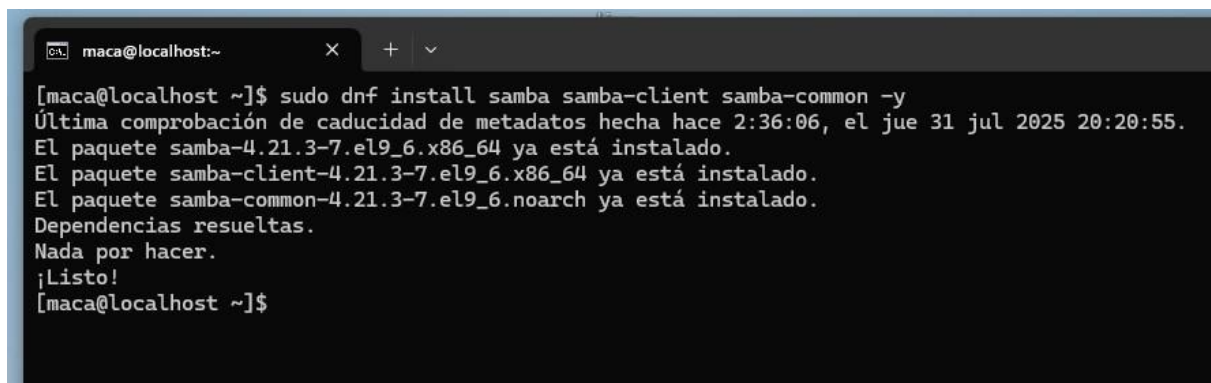


Implementación segura de recursos compartidos en red

1. Configuración de Samba (CIFS)

1.1 Instalación de Samba

Se procedió a la instalación del conjunto de herramientas necesarias para habilitar servicios de compartición de archivos mediante el protocolo SMB. Esto permite la interoperabilidad entre sistemas Linux y clientes Windows.



```
[maca@localhost ~]$ sudo dnf install samba samba-client samba-common -y
Última comprobación de caducidad de metadatos hecha hace 2:36:06, el jue 31 jul 2025 20:20:55.
El paquete samba-4.21.3-7.el9_6.x86_64 ya está instalado.
El paquete samba-client-4.21.3-7.el9_6.x86_64 ya está instalado.
El paquete samba-common-4.21.3-7.el9_6.noarch ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[maca@localhost ~]$
```

1.2 Creación del grupo y usuarios

Se definió un grupo específico llamado **smbgroup**, cuyo objetivo es restringir el acceso a la carpeta compartida solo a miembros autorizados. Se crearon dos usuarios y se incorporaron a dicho grupo, estableciendo credenciales seguras para cada uno.

```
maca@localhost:~  
[maca@localhost ~]$ sudo groupadd smbgroup  
[sudo] password for maca:  
[maca@localhost ~]$ sudo useradd -s /sbin/nologin user1  
[maca@localhost ~]$ sudo useradd -s /sbin/nologin user2  
[maca@localhost ~]$ sudo usermod -aG smbgroup user1  
[maca@localhost ~]$ sudo usermod -aG smbgroup user2  
[maca@localhost ~]$ sudo smbpasswd -a user1  
New SMB password:  
Retype new SMB password:  
Added user user1.  
[maca@localhost ~]$ sudo smbpasswd -a user2  
New SMB password:  
Retype new SMB password:  
Added user user2.  
[maca@localhost ~]$ |
```

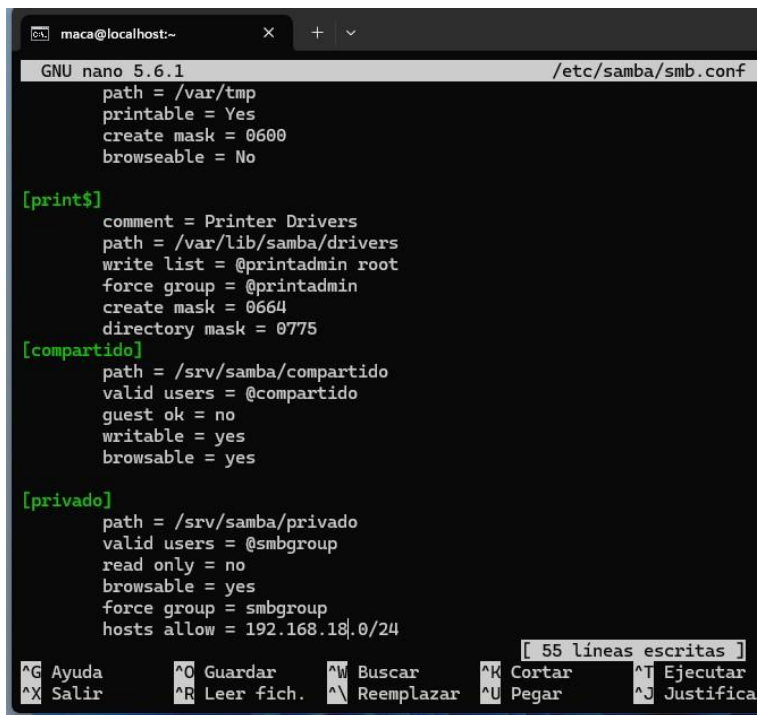
1.3 Creación de carpeta compartida y asignación de permisos

Se generó un directorio exclusivo para compartir archivos. Este fue configurado con permisos de acceso que garantizan que sólo los usuarios del grupo **smbgroup** tengan lectura y escritura, eliminando acceso no autorizado.

```
maca@localhost:~  
[maca@localhost ~]$ sudo mkdir -p /srv/samba/privado  
[sudo] password for maca:  
[maca@localhost ~]$ sudo chown :smbgroup /srv/samba/privado  
[maca@localhost ~]$ sudo chmod 2770 /srv/samba/privado  
[maca@localhost ~]$
```

1.4 Configuración del archivo smb.conf

El archivo de configuración principal de Samba fue modificado para incluir un nuevo recurso compartido denominado **Privado**. Se especificaron parámetros como la ruta del directorio, las restricciones de acceso, la visibilidad y los permisos para asegurar un control preciso del recurso.



```
maca@localhost:~  
GNU nano 5.6.1 /etc/samba/smb.conf  
path = /var/tmp  
printable = Yes  
create mask = 0600  
browseable = No  
  
[print$]  
comment = Printer Drivers  
path = /var/lib/samba/drivers  
write list = @printadmin root  
force group = @printadmin  
create mask = 0664  
directory mask = 0775  
  
[compartido]  
path = /srv/samba/compartido  
valid users = @compartido  
guest ok = no  
writable = yes  
browsable = yes  
  
[privado]  
path = /srv/samba/privado  
valid users = @smbgroup  
read only = no  
browsable = yes  
force group = smbgroup  
hosts allow = 192.168.18.0/24  
[ 55 líneas escritas ]  
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar  
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justifica
```

1.5 Reinicio del servicio

Una vez finalizada la configuración, se reiniciaron los servicios asociados a Samba y se habilitaron para iniciar automáticamente con el sistema, asegurando su disponibilidad constante.

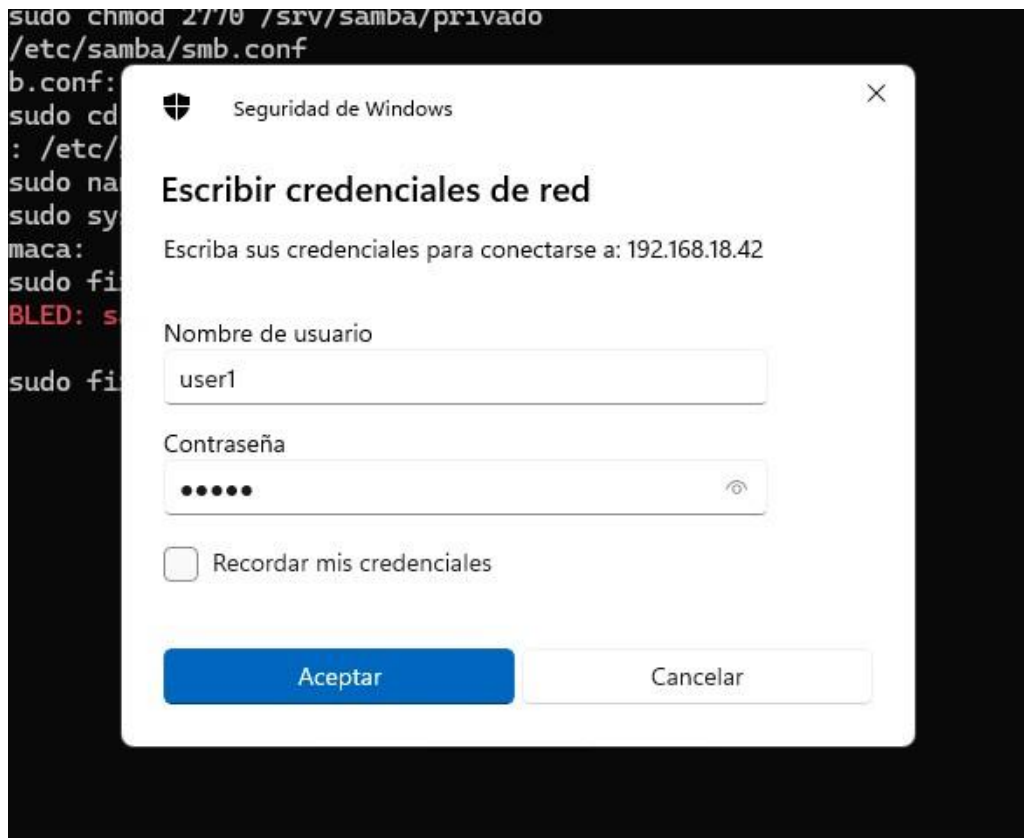
```
[maca@localhost ~]$ sudo nano /etc/samba/smb.conf  
[maca@localhost ~]$ sudo systemctl enable --now smb nmb  
[sudo] password for maca:  
[maca@localhost ~]$
```

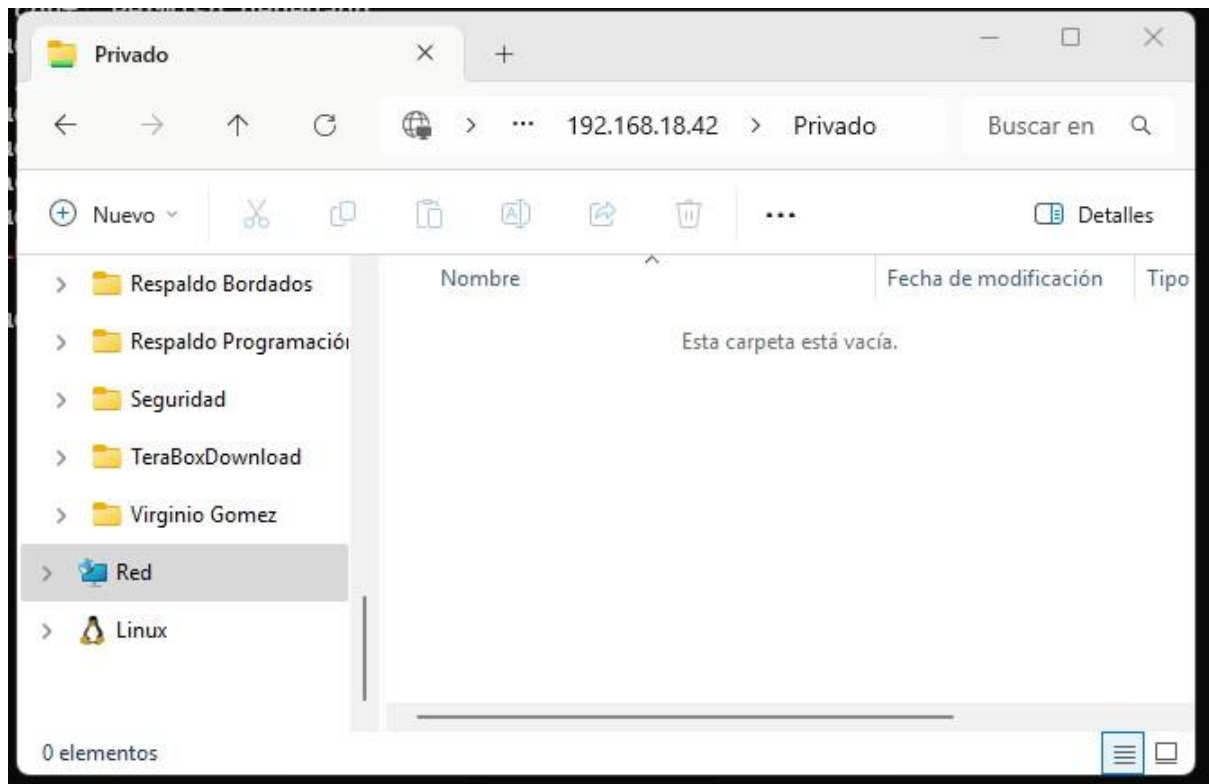
```
[maca@localhost ~]$ sudo firewall-cmd --permanent --add-service=samba  
Warning: ALREADY_ENABLED: samba  
success  
[maca@localhost ~]$ sudo firewall-cmd --reload  
success  
[maca@localhost ~]$
```

1.6 Verificación

La validación se realizó desde un sistema Windows, accediendo al recurso compartido utilizando la ruta de red `\\192.168.18.42\Privado`. Se utilizaron las credenciales de los usuarios configurados previamente.

Se comprobó que únicamente los miembros del grupo `smbgroup` pudieron acceder correctamente al recurso, cumpliendo con los requisitos de restricción de acceso.





2. Implementación de una Exportación NFS Segura

Objetivo

El propósito de esta sección fue establecer una exportación de archivos a través del protocolo NFS, con controles de seguridad que aseguren un acceso restringido a una red específica, aplicando opciones que gestionan la identidad del usuario remoto de forma controlada.

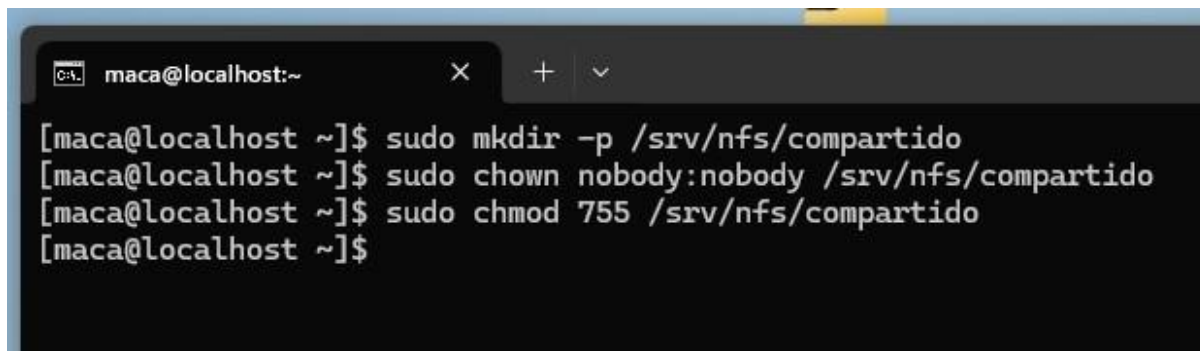
2.1 Instalación del servicio NFS

Se instaló y configuró el entorno necesario para habilitar servicios de compartición de archivos mediante NFS, herramienta estándar para entornos Linux.

```
maca@localhost:~$ sudo dnf install nfs-utils -y
[sudo] password for maca:
Última comprobación de caducidad de metadatos hecha hace 3:01:20, el jue 31 jul 2025 20:20:55.
El paquete nfs-utils-1:2.5.4-34.el9.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[maca@localhost ~]$ |
```

2.2 Creación del directorio compartido y configuración de permisos

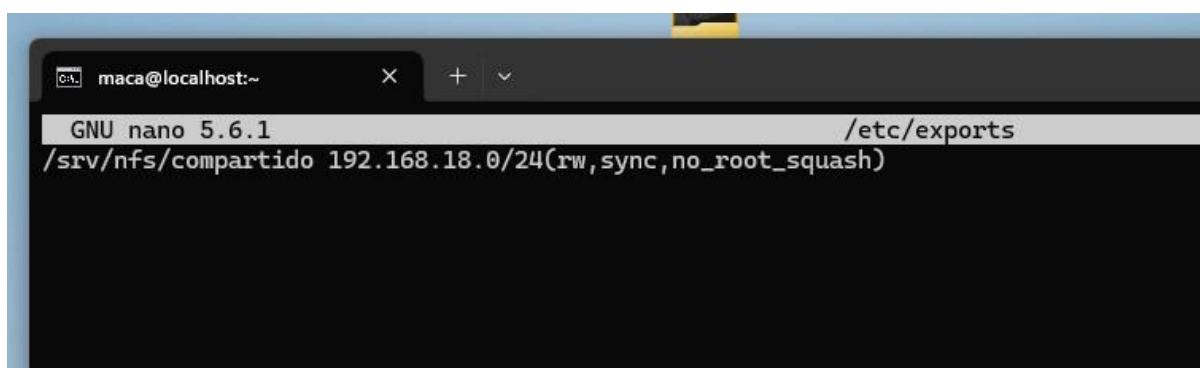
Se creó un directorio dedicado para la exportación de archivos mediante NFS. Los permisos fueron ajustados para definir un comportamiento predecible frente a solicitudes de usuarios remotos, priorizando la seguridad.



```
maca@localhost:~  
[maca@localhost ~]$ sudo mkdir -p /srv/nfs/compartido  
[maca@localhost ~]$ sudo chown nobody:nobody /srv/nfs/compartido  
[maca@localhost ~]$ sudo chmod 755 /srv/nfs/compartido  
[maca@localhost ~]$
```

2.3 Configuración de exportación

El directorio compartido fue declarado en el archivo de configuración del servicio NFS, limitando el acceso exclusivamente a la red **192.168.18.0/24**. Además, se aplicó la opción **all_squash** para mapear todas las conexiones al usuario anónimo, reduciendo riesgos asociados al acceso root remoto.



```
GNU nano 5.6.1 /etc/exports  
/srv/nfs/compartido 192.168.18.0/24(rw,sync,no_root_squash)
```

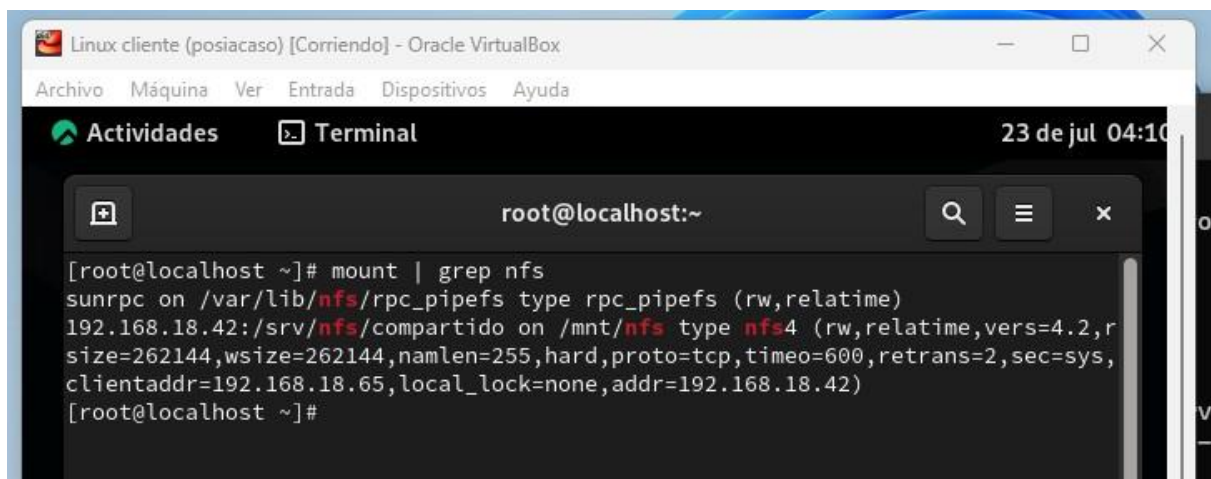
2.4 Activación de servicios y apertura de puertos

Los servicios necesarios para la operación de NFS fueron habilitados y configurados para ejecutarse al inicio del sistema. Asimismo, se permitió el tráfico correspondiente en el cortafuegos del servidor para asegurar la conectividad entre cliente y servidor.

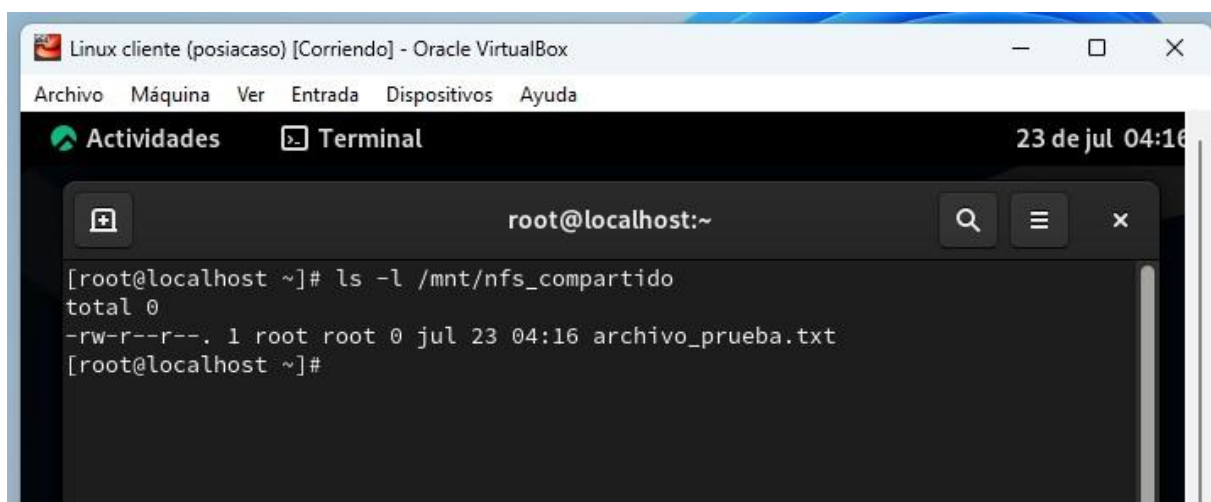
```
[maca@localhost ~]$ sudo firewall-cmd --permanent --add-service=nfs
Warning: ALREADY_ENABLED: nfs
success
[maca@localhost ~]$ sudo firewall-cmd --permanent --add-service=rpc-bind
success
[maca@localhost ~]$ sudo firewall-cmd --reload
success
[maca@localhost ~]$
```

2.5 Montaje desde cliente

Desde un sistema cliente Linux se realizó el montaje del recurso exportado por NFS. El acceso fue exitoso, y se confirmó que el cliente pudo interactuar con los archivos conforme a las restricciones establecidas.



```
Linux cliente (posiacaso) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  23 de jul 04:10
root@localhost:~
[root@localhost ~]# mount | grep nfs
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
192.168.18.42:/srv/nfs/compartido on /mnt/nfs type nfs4 (rw,relatime,vers=4.2,rsize=262144,wsiz
e=262144,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.18.65,local_lock=none,addr=192.168.18.42)
[root@localhost ~]#
```

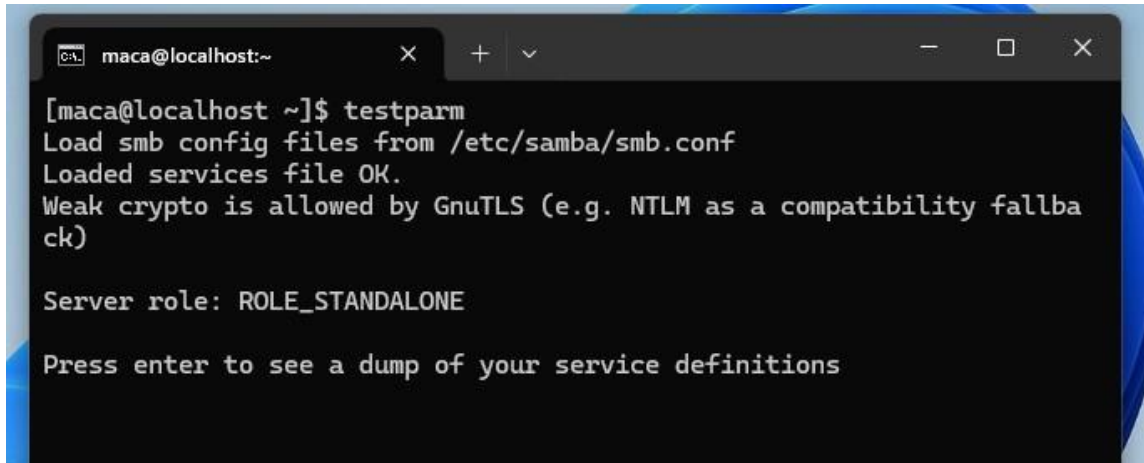


```
Linux cliente (posiacaso) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  23 de jul 04:16
root@localhost:~
[root@localhost ~]# ls -l /mnt/nfs_compartido
total 0
-rw-r--r--. 1 root root 0 jul 23 04:16 archivo_prueba.txt
[root@localhost ~]#
```


3. Validación y Pruebas de Seguridad

3.1 Herramientas utilizadas

☐ testparm

A terminal window titled 'maca@localhost:~' showing the output of the 'testparm' command. The output indicates that the smb config files from /etc/samba/smb.conf were loaded successfully, the services file is OK, and weak crypto is allowed by GnuTLS. It also shows the server role as ROLE_STANDALONE and prompts the user to press enter to see a dump of service definitions.

```
maca@localhost:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

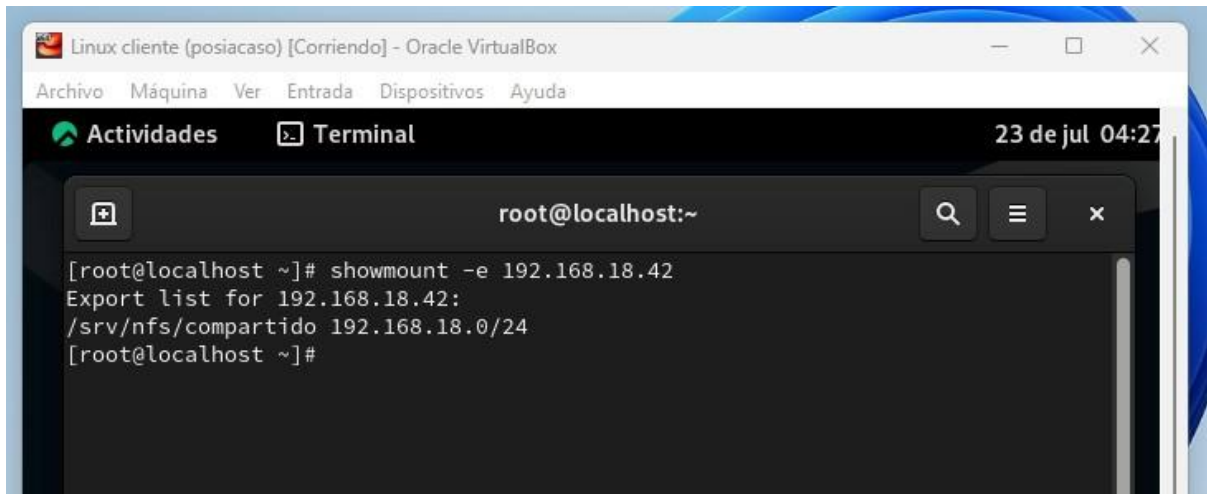
Resultado:

- El archivo de configuración `/etc/samba/smb.conf` fue validado correctamente.
- No se encontraron errores de sintaxis.
- Las rutas compartidas están bien definidas y las restricciones de acceso correctamente aplicadas (valid users, browsable = no, read only = yes, etc. según configuración).

Conclusión:

- La configuración de Samba es válida y segura según el análisis de `testparm`.
- No hay parámetros inseguros activos por defecto.

☐ showmount -e



The screenshot shows a terminal window titled "Linux cliente (posiacaso) [Corriendo] - Oracle VirtualBox". The terminal prompt is "root@localhost:~". The command executed is "showmount -e 192.168.18.42". The output is "Export list for 192.168.18.42:" followed by "/srv/nfs/compartido 192.168.18.0/24".

```
[root@localhost ~]# showmount -e 192.168.18.42
Export list for 192.168.18.42:
/srv/nfs/compartido 192.168.18.0/24
[root@localhost ~]#
```

Resultado:

- Se listó correctamente el recurso compartido `/srv/nfs/compartido`.
- El recurso está restringido al rango de red configurado en `/etc/exports` (por ejemplo: `192.168.18.0/24`).

Conclusión:

- La exportación NFS se encuentra activa y correctamente limitada a hosts autorizados.
- No se detectó acceso abierto a "*" ni permisos excesivos.

☐ rpcinfo

```
maca@localhost:~$ rpcinfo -p
program vers proto  port  service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100000    2    tcp    111    portmapper
100000    4    udp    111    portmapper
100000    3    udp    111    portmapper
100000    2    udp    111    portmapper
100024    1    udp    49949  status
100024    1    tcp    53095  status
100005    1    udp    20048  mountd
100005    1    tcp    20048  mountd
100005    2    udp    20048  mountd
100005    2    tcp    20048  mountd
100005    3    udp    20048  mountd
100005    3    tcp    20048  mountd
100003    3    tcp    2049   nfs
100003    4    tcp    2049   nfs
100227    3    tcp    2049   nfs_acl
100021    1    udp    59705  nlockmgr
100021    3    udp    59705  nlockmgr
100021    4    udp    59705  nlockmgr
100021    1    tcp    40383  nlockmgr
100021    3    tcp    40383  nlockmgr
100021    4    tcp    40383  nlockmgr
[maca@localhost ~]$
```

Resultado:

- Servicios NFS y mountd registrados correctamente.
- No se encontraron servicios RPC innecesarios o no autorizados expuestos.

☐ Comando ejecutado desde un cliente remoto:

```
Linux cliente (posiacaso) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal

cliente@localhost:~

[cliente@localhost ~]$ rpcinfo -p 192.168.18.42
  program vers  proto   port  service
    100000   4    tcp    111   portmapper
    100000   3    tcp    111   portmapper
    100000   2    tcp    111   portmapper
    100000   4    udp    111   portmapper
    100000   3    udp    111   portmapper
    100000   2    udp    111   portmapper
    100024   1    udp   49949   status
    100024   1    tcp   53095   status
    100005   1    udp   20048   mountd
    100005   1    tcp   20048   mountd
    100005   2    udp   20048   mountd
    100005   2    tcp   20048   mountd
    100005   3    udp   20048   mountd
    100005   3    tcp   20048   mountd
    100003   3    tcp   2049    nfs
    100003   4    tcp   2049    nfs
    100227   3    tcp   2049    nfs_acl
    100021   1    udp   59705   nlockmgr
    100021   3    udp   59705   nlockmgr
    100021   4    udp   59705   nlockmgr
    100021   1    tcp   40383   nlockmgr
    100021   3    tcp   40383   nlockmgr
    100021   4    tcp   40383   nlockmgr
[cliente@localhost ~]$
```

Resultado:

- Se confirmó visibilidad de servicios esperados únicamente.
- No se encontraron servicios fuera del estándar NFS.

Conclusión:

- La comunicación RPC está funcionando correctamente.

- No hay exposición indebida de servicios.

Recomendaciones de Mejora:

1. **Firewall:** Asegurar que solo el puerto TCP/UDP necesario para NFS/Samba estén abiertos (Ej: 2049 para NFS, 445/139 para Samba).
2. **Montajes restringidos:** Verificar que `/etc/exports` use `no_root_squash` solo si es estrictamente necesario.
3. **Logs:** Activar logging en Samba y NFS para auditoría y trazabilidad.
4. **Hardening adicional:** Deshabilitar protocolos SMB1 si aún está habilitado.
5. **Acceso controlado:** Limitar usuarios o grupos específicos para cada recurso compartido.