Actividad Calificable 3.1
Bastionado de identidad y gestión de credenciales Kerberos

Volodimir Yarmash Yarmash

Contexto

Trabajáis como Administradores de Sistemas en una empresa de ciberseguridad. Se os ha asignado la tarea de implementar un sistema de autenticación centralizado y seguro en un entorno híbrido (Windows/Linux). Se aplicarán técnicas de bastionado para asegurar que las credenciales no viajen en texto claro y que el sistema sea resistente a ataques de suplantación.

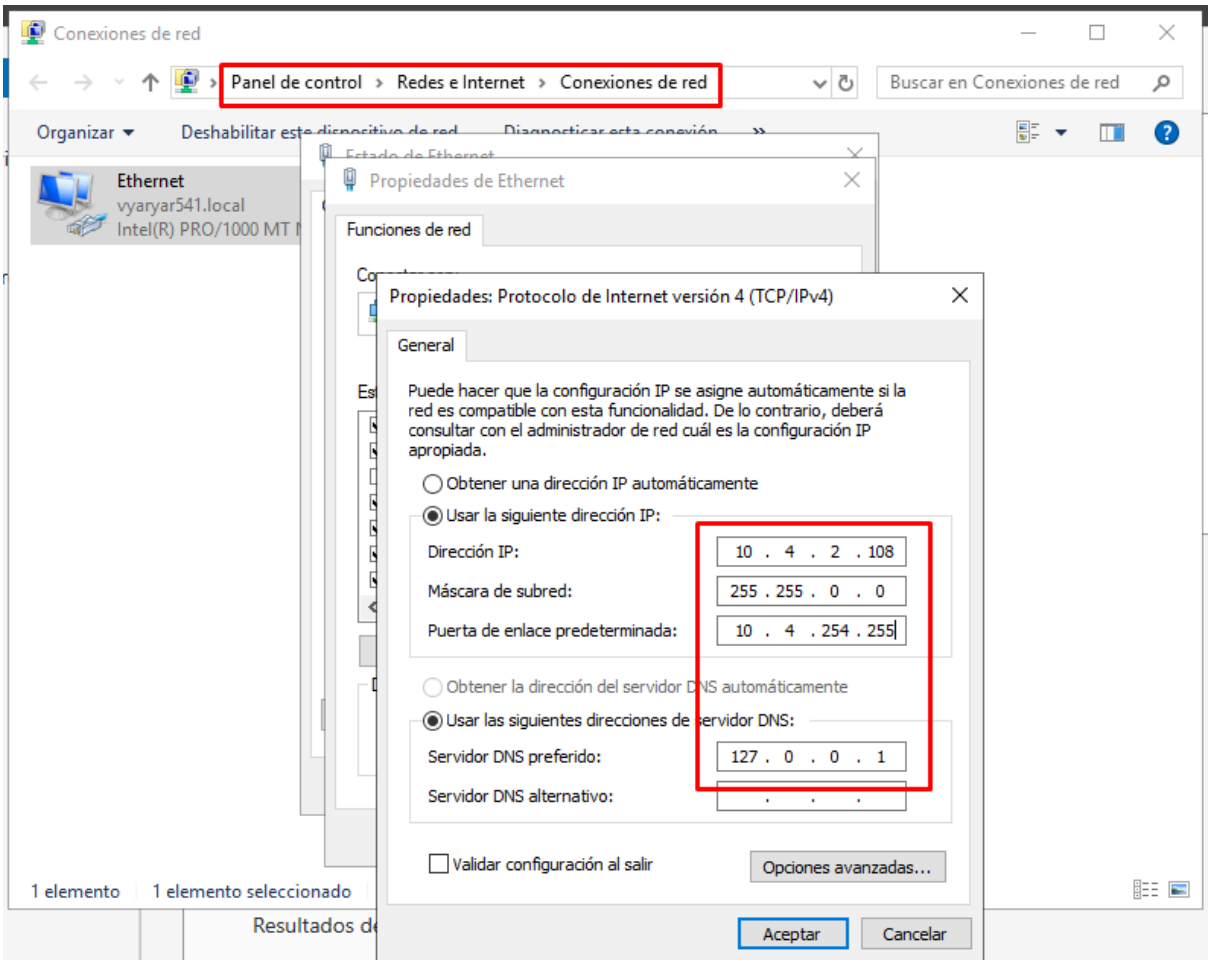
Personalización

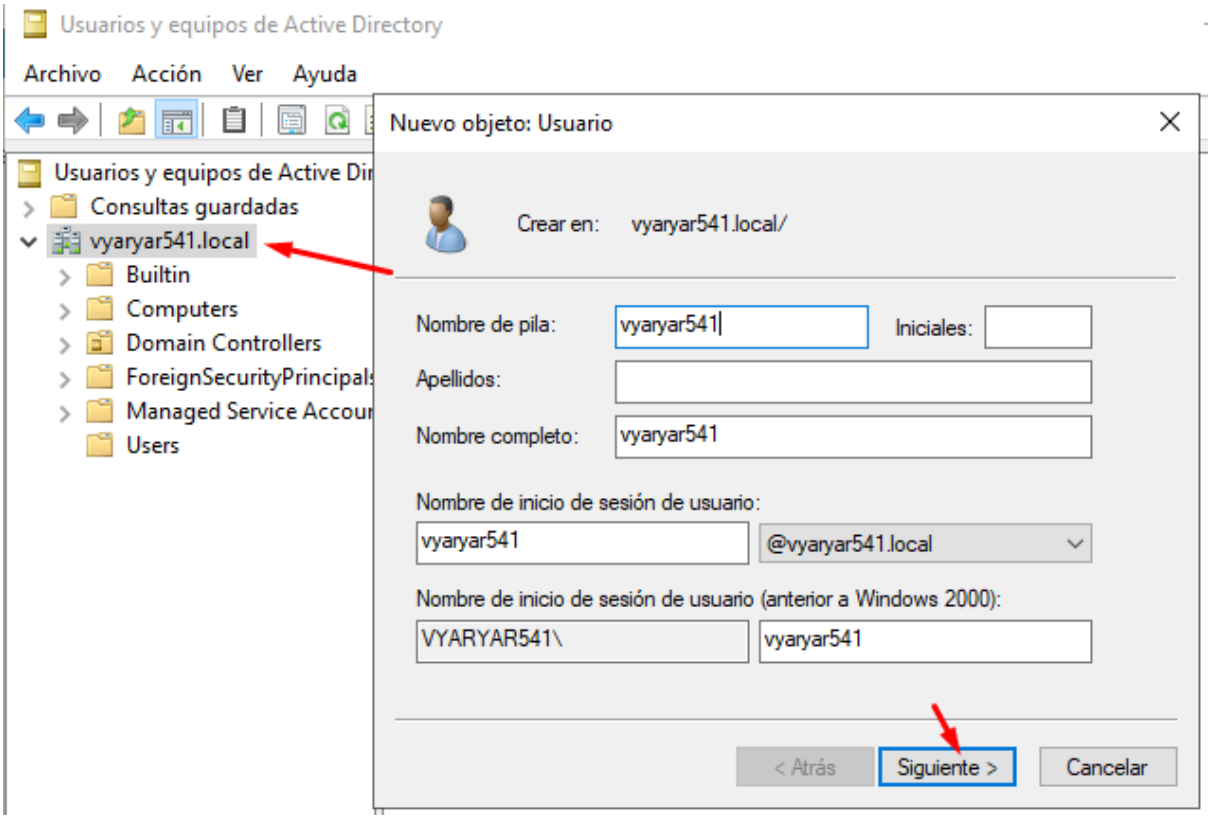
Para que el ejercicio sea válido, deberás sustituir los siguientes valores en toda la configuración:

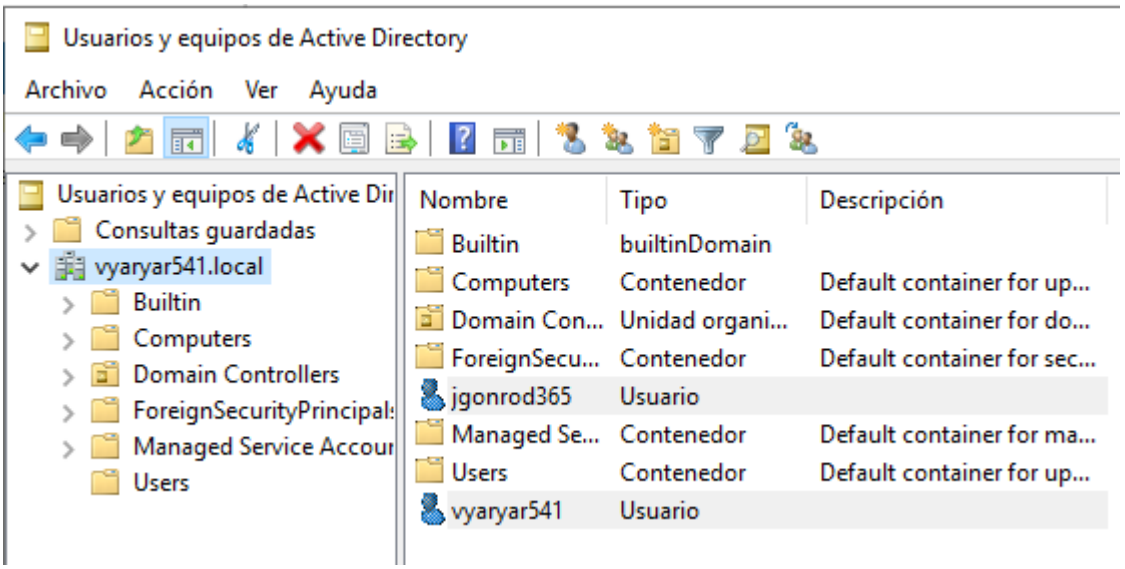
• [DNI3]: Las últimas 3 cifras de tu DNI (ej: si es 12345678, usarás 678).
• [DNI1]: La última cifra de tu DNI (ej: si es 12345678, usarás 8).
• [USER]: Tu nombre de usuario en Pasen (ej: jgonrod365).
• [PC]: Tu número de PC en clase con dos dígitos.
• [PROFE]: jgonrod365
• [TU_IP]: La dirección IP que te corresponda.

Escenario técnico

• Una máquina virtual servidor llamada Kerberos-Server-[USER]
o Windows Server 2019 con Active Directory (dominio: [USER].local)
o IP estática: 10.4.2.1[PC]
o Máscara: 255.255.0.0
o Gateway: 10.4.254.255
o Debes crear dos usuarios: [USER] y [PROFE]
• Una máquina virtual cliente llamada Kerberos-Client-[USER]
o Debian 13 con interfaz gráfica.
o IP estática: 10.4.2.2[PC]
o Máscara y gateway iguales que el servidor.
o DNS: apuntando a la IP del servidor y a otro de Google/Cloudflare.







1. Preparación y bastionado del cliente

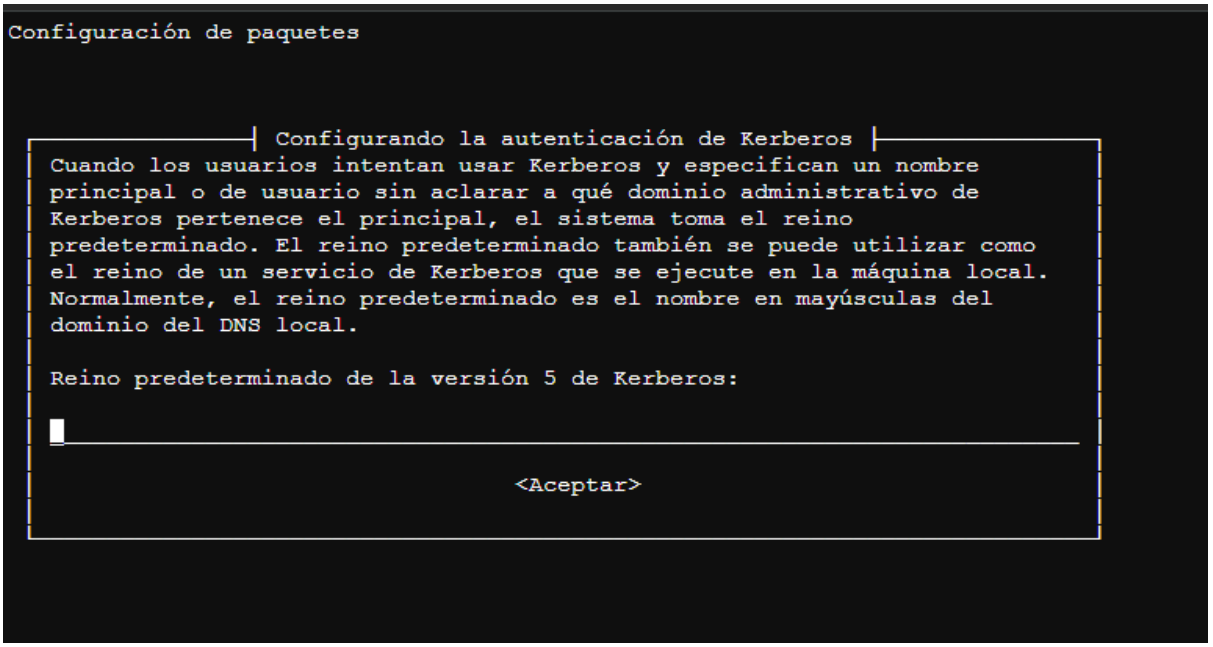
Instalar los paquetes necesarios (sssd sssd-ad sssd-tools realmd adcli krb5-user samba-common-bin) y asegurar el sistema de archivos.

• sssd y realmd: Permiten que Debian entienda la estructura de usuarios del Active Directory.

• krb5-user: Proporciona las herramientas necesarias para gestionar los tickets de seguridad.

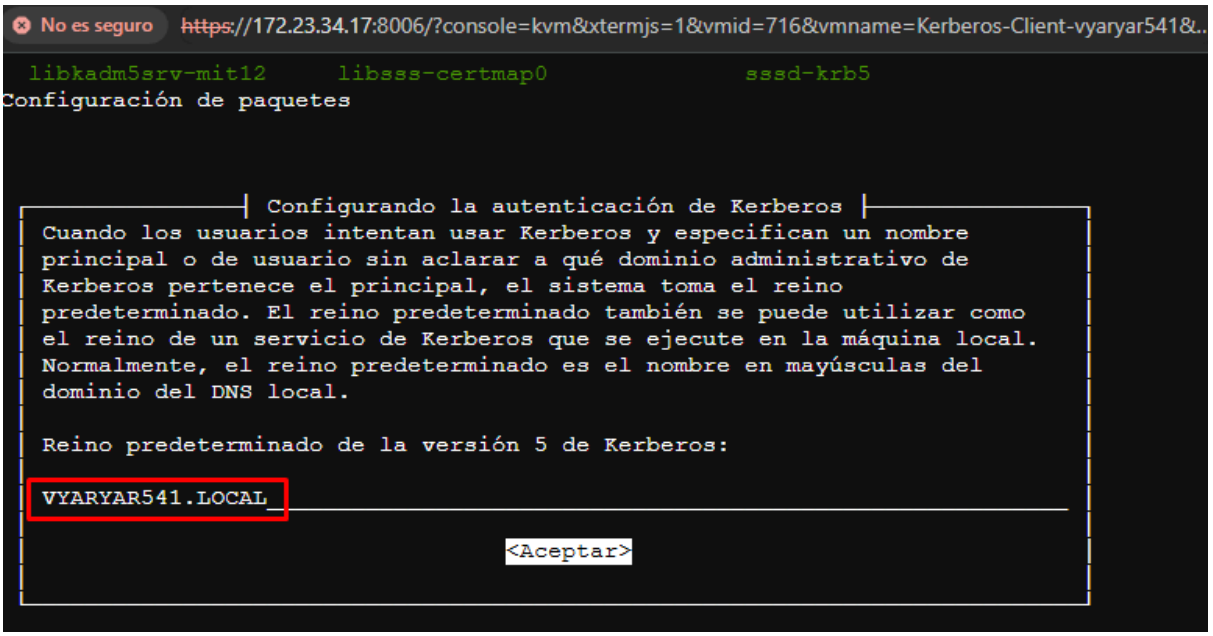
• Sincronización horaria: Es obligatorio que la hora de Debian y el Server

coincidan (máximo 5 min de desfase) porque Kerberos usa marcas de tiempo para evitar ataques de denegación (replay attacks).

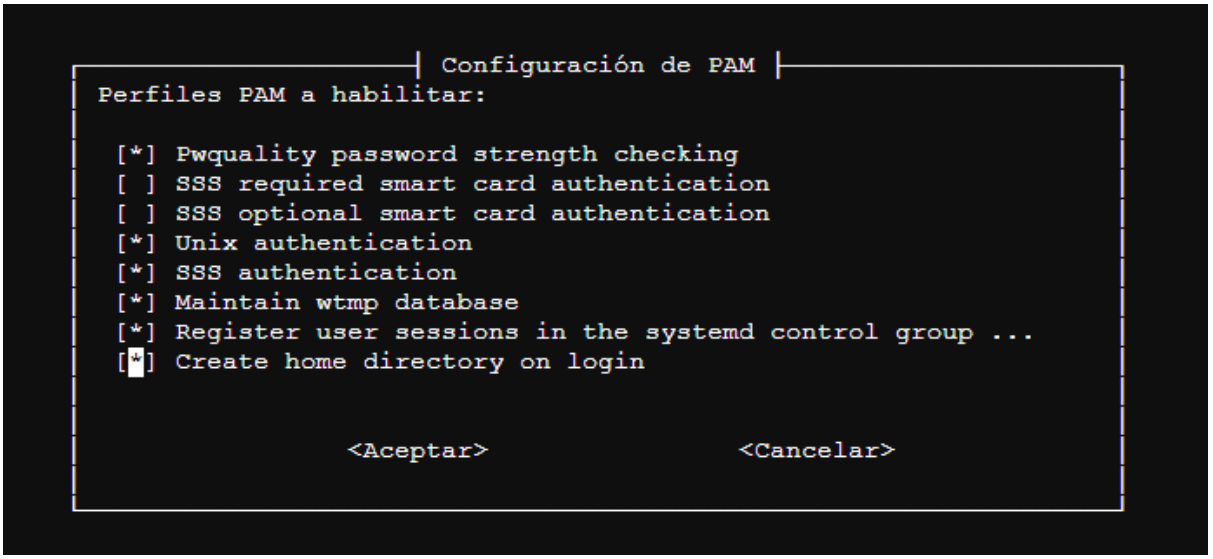


2. Unión al dominio e identidad

Unir la máquina al dominio y configurar SSSD.
1. Une la máquina al dominio haciendo uso del usuario Administrador.
2. Edita el fichero de configuración de SSSD (sssd.conf) y establece permisos restrictivos de lectura y escritura solamente al usuario propietario (root).
• Unión al dominio: Para que el servidor confíe en el cliente Debian como un dispositivo legítimo de la red.
• Permisos: Es una medida de bastionado crítico; el fichero contiene información sensible de la estructura del dominio y solo root debe acceder a él.



Nos unimos al Realm
realm join --user=Administrador VYARYAR541.LOCAL -v
Asignamos al propietario root y grupo root
chown root:root /etc/sssd/sssd.conf
Y aplica permisos de lectura y escritura al root
chmod 600 /etc/sssd/sssd.conf
Con el comando pam-auth-update vamos a cambiar nuestra configuración marcando la casilla de crear directorio ar hacer login



3. Ciclo de vida de las credenciales

Utilizar los comandos de Kerberos para gestionar el acceso.
1. kinit para solicitar el ticket inicial (TGT) para [USER]
2. klist para visualizar los tickets activos y su fecha de expiración.
3. kdestroy para eliminar las credenciales de la caché.
• kinit: Para demostrar que el sistema de autenticación funciona sin enviar la contraseña a cada servicio.
• klist: Para auditar la validez y autenticidad de los tickets.
• kdestroy: Para aplicar el principio de privilegio mínimo y seguridad del puesto; al terminar, no deben quedar credenciales utilizables en la memoria.

Solicitamos con kinit vyaryar541@VYARYAR541.LOCAL

```
root@debian:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: vyaryar541@VYARYAR541.LOCAL

Valid starting     Expires            Service principal
29/01/26 19:55:44  30/01/26 05:55:44  krbtgt/VYARYAR541.LOCAL@VYARYAR541.LOCAL
        renew until 30/01/26 19:55:40
root@debian:~#
```

Destruimos el tiquet con kdesytroy

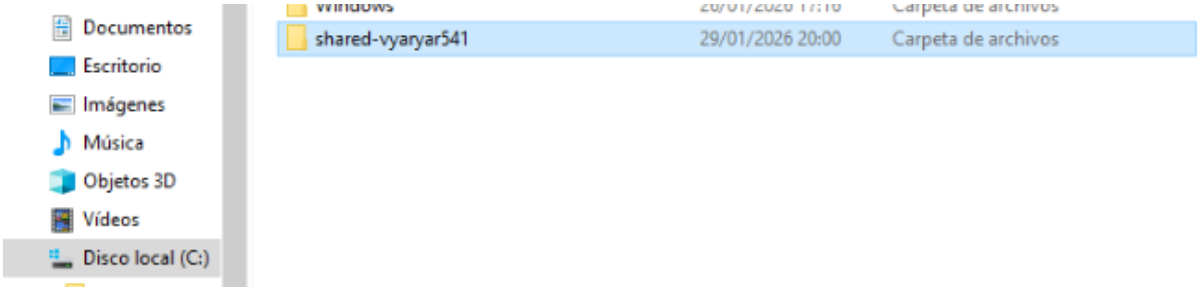
```
root@debian:~# kdestroy
root@debian:~# klist
klist: No credentials cache found (filename: /tmp/krb5cc_0)
root@debian:~#
```

4. Acceso a recursos y Single Sign-On

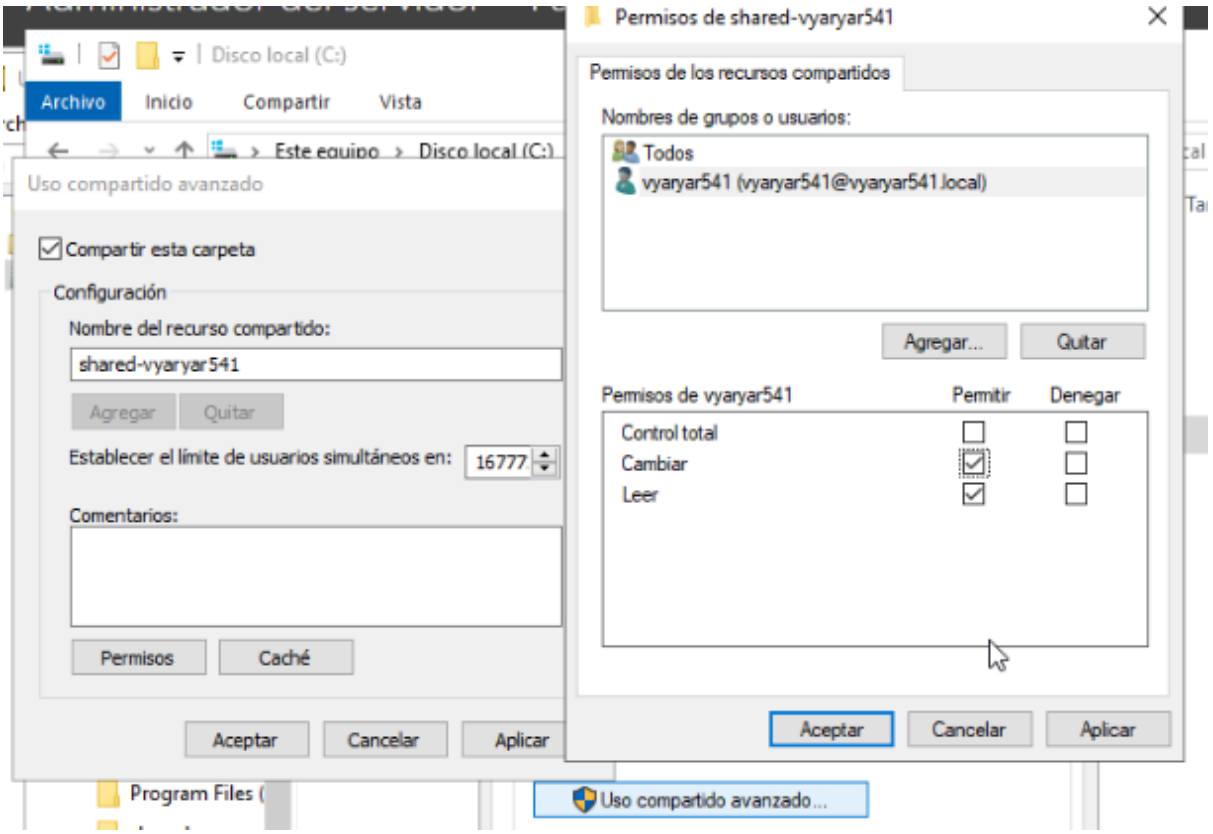
Crear una carpeta compartida en Windows Server (\shared-[USER]) y acceder desde Debian sin introducir contraseña usando smbclient -k

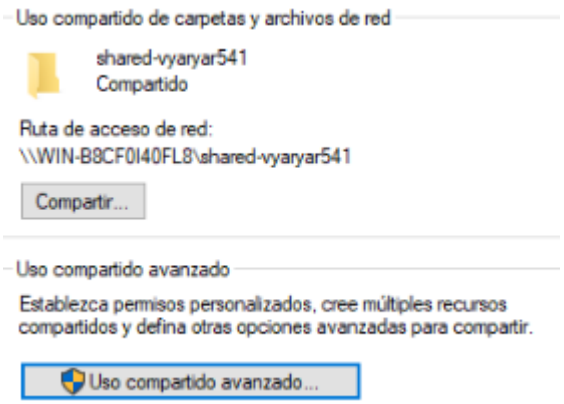
• Para verificar el Single Sign-On (SSO). Al usar la opción -k (Kerberos), el sistema usa el ticket que ya tienes. Esto preserva la privacidad de los datos al no solicitar la clave constantemente.

Creamos la carpeta



Con click derecho le damos a compartir:





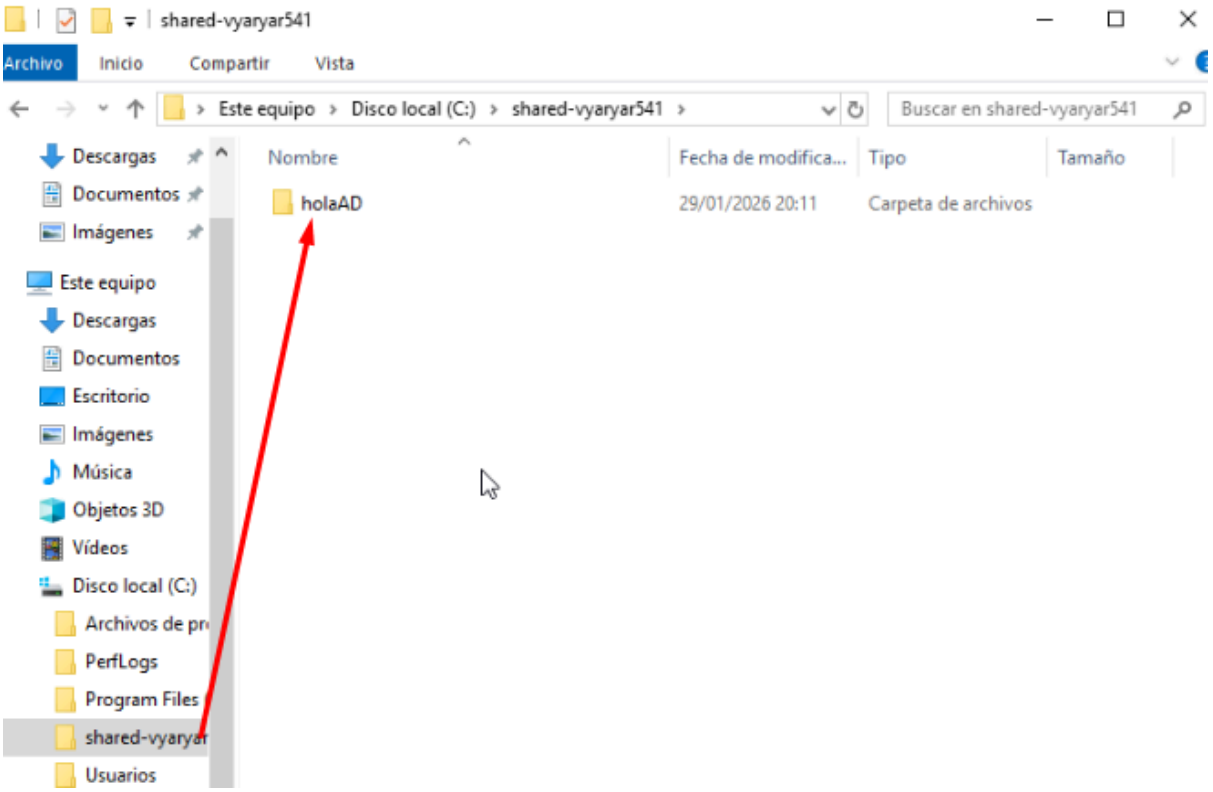
Ahora en debian iniciamos de nuevo con kinit vyaryar541@VYARYAR541.LOCAL y combrobamos con klist
entramos dentro con en comando smbclient -k

```
root@debian:~# smbclient -k //WIN-B8CF0I40FL8/shared-vyaryar541
WARNING: The option -k|--kerberos is deprecated!
Try "help" to get a list of possible commands.
smb: \> la
la: command not found
smb: \> ls
  .                                   D        0  Thu Jan 29 20:00:33 2026
  ..                                  D        0  Thu Jan 29 20:00:33 2026

                8247551 blocks of size 4096. 5258206 blocks available
smb: \> mkdir holaAD
smb: \> ls
  .                                   D        0  Thu Jan 29 20:11:12 2026
  ..                                  D        0  Thu Jan 29 20:11:12 2026
  holaAD                              D        0  Thu Jan 29 20:11:12 2026

                8247551 blocks of size 4096. 5258206 blocks available
smb: \>
```

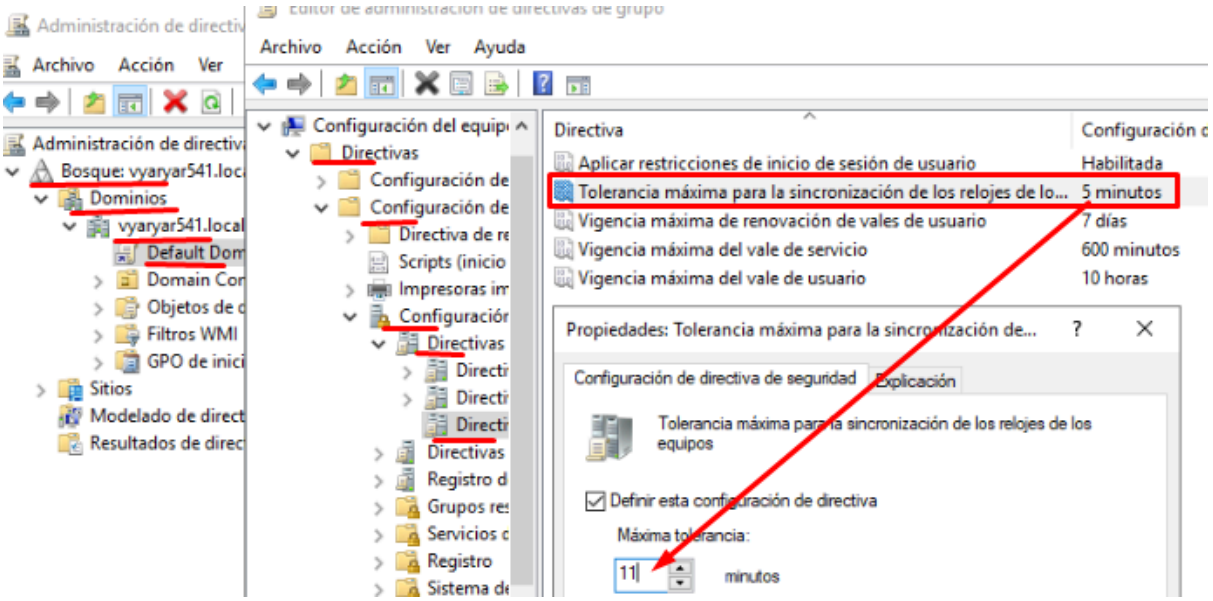
Comprobación:



5. Bastionado mediante GPO de Kerberos

Para realizar un análisis de riesgo práctico. Al reducir el margen de tiempo, endureces (bastionas) el sistema contra atacantes que intenten capturar y reutilizar tickets antiguos.
1. En Windows Server, edita la GPO de dominio: Directiva de Kerberos → Desfase máximo en el reloj = 1[DNI1] minutos.
2. En Debian, cambia la hora manualmente (deshabilitando previamente el servicio de sincronización automática) para que difiera en un número de minutos superior al establecido en el apartado previo.
3. Intenta hacer un kinit, mostrando y explicando el resultado.

Entramos a administración de directivas de grupo y llegamos al apartado de Directivas Kerberos.
Cambiamos el número de minutos por los que nos piden (1[DNI1])



Para comprobarlo debemos parar los servicios de sincronización del tiempo
systemctl stop systemd-timesyncd
systemctl stop qemu-guest-agent
Forzamos el desfase con date -s "xx:xx:xx"
Limpio el rastro anterior por si acaso kdestroy
e iniciamos con kinit vyaryar541@VYARYAR541.LOCAL
Probamos forzar la actualización de las directivas y reiniciar WindowsServer
Probamos, pero en mi caso sigue dando acceso, tras una larga investigacion y pruebas diferentes es posible que la respuesta esté en que Proxmox utiliza un reloj de hardware virtual (KVM-clock), kernel puede estar usando el reloj de alta precisión del procesador.

```
kinit vyaryar541@VYARYAR541.LOCAL
mié 29 ene 2025 20:00:00 CET
mié 29 ene 2025 20:00:00 CET
kdestroy: No credentials cache found while destroying cache
Password for vyaryar541@VYARYAR541.LOCAL:
root@debian:~# kdestroy
root@debian:~# kinit vyaryar541@VYARYAR541.LOCAL
Password for vyaryar541@VYARYAR541.LOCAL:
root@debian:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: vyaryar541@VYARYAR541.LOCAL

Valid starting     Expires            Service principal
29/01/26 20:45:30  30/01/26 06:45:30  krbtgt/VYARYAR541.LOCAL@VYARYAR541.LOCAL
        renew until 30/01/26 20:45:28
root@debian:~#
```

Final del ejercicio

Una vez hayas completado el ejercicio, apaga las máquinas virtuales y realízales una instantánea.
Las modificaciones posteriores a esta instantánea se perderán, ya que el profesor la restaurará antes de comenzar la corrección.
Entrega
Realiza un documento en formato PDF con todos los cambios efectuados y súbelo a

Moodle.