**Unidad Didáctica 6. Compartición de recursos en red mediante el protocolo CIFS/SAMBA**

**Ejercicio 1. Busca y amplía información relacionada con SMB/CIFS.**

**Protocolo SMB**

El protocolo SMB es uno de los más antiguos y con el paso del tiempo ha permitido el acceso a archivos y directorios, además de recursos de red. Se encarga de intercambiar información entre procesos de un sistema. Fue creado por IBM.

SMB son las siglas de Server Message Block. Este protocolo cliente-servidor se encarga de gestionar el acceso a esos archivos o directorios. Concretamente fue desarrollado en el año 1983. Ha estado presente en los diferentes sistemas operativos de Windows.

**Usos del SMB:**

* Intercomunicación entre servidores
* Gestión de cambios para directorios y registros
* Posibilidad de compartir carpetas, impresoras y demás archivos.
* Acceso de edición y navegación a través de una red
* Soporte de enlaces simbólicos
* Bloqueo oportunista
* Bloqueo de archivos
* Conmutación por error transparente, que facilita el mantenimiento del hardware y software
* Uso compartido de clústeres mediante SMB escalables



El protocolo SMB permite compartir archivos entre dispositivos y ha evolucionado desde SMB 1 hasta SMB 3.1.1, usado en Windows 10/11 y Server 2016. Cada versión mejoró en seguridad, velocidad y características. Es crucial mantener SMB actualizado para evitar vulnerabilidades, como el exploit Eternal Blue usado en el ataque de ransomware Wanna Cry.

**Protocolo CIFS**

CIFS es un protocolo que permite a los programas hacer peticiones de archivos y servicios en ordenadores remotos a través de Internet. Desarrollado por Microsoft, CIFS es una variación pública o abierta del anterior protocolo SMB. Utiliza el modelo de programación cliente/servidor.

Estos protocolos de intercambio de archivos se diseñaron originalmente para conexiones de red cableadas, por lo que requieren un gran número de transacciones de petición/respuesta y su rendimiento disminuye considerablemente en los enlaces WAN de alta latencia como Internet.



**Ejercicio 2. Investiga sobre las vulnerabilidades en SMBv1, SMBv2 y SMBv3.**

**Vulnerabilidad en SMBv1**

Las vulnerabilidades en SMBv1 son bien conocidas y representan un riesgo significativo para la seguridad en redes modernas. Este protocolo, introducido en 1983, no fue diseñado para los estándares de seguridad actuales y ha demostrado ser vulnerable a múltiples ataques. A continuación, se destacan los principales aspectos relacionados con sus vulnerabilidades:

Cuando SMBv1 fue desarrollado, las amenazas cibernéticas eran mucho menos complejas que las actuales. Esto se refleja en su diseño, que carece de medidas de seguridad esenciales como:

* Cifrado de datos: La información transmitida no está protegida, facilitando su interceptación.
* Autenticación robusta: Los sistemas que usan SMBv1 son vulnerables a ataques de fuerza bruta o suplantación de identidad

**Vulnerabilidad en SMBv2**

SMBv2 mejoró significativamente la seguridad frente a SMBv1, pero aún presenta vulnerabilidades que pueden comprometer sistemas mal configurados o desactualizados. Una de las más graves es EternalChampion (SMBGhost), que permite la ejecución remota de código. También es vulnerable a ataques de transmisión (SMB Relay), exposición de credenciales mediante capturas de hashes NTLM y ataques de denegación de servicio con paquetes mal formados.

Si bien SMBv2 es más seguro, su configuración incorrecta o falta de actualizaciones puede permitir explotación de permisos, ataques de fuerza bruta, y problemas en la validación de paquetes. Por ello, mantenerlo actualizado y configurado correctamente es esencial para minimizar riesgos.

**Vulnerabilidad en SMBv3**

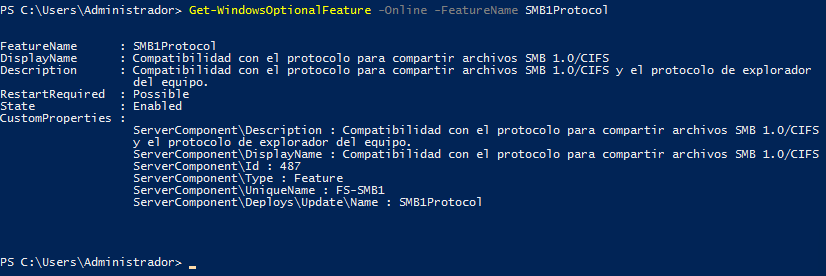
SMBv3 es la versión más avanzada del protocolo y presenta importantes mejoras en seguridad y rendimiento respecto a versiones anteriores, pero no es completamente inmune a vulnerabilidades. Entre los problemas más relevantes se encuentran fallos en configuraciones de SMB Multichannel y SMB Direct, que pueden ser explotados para interceptar o manipular datos si no se utiliza cifrado adecuado.

Además, en implementaciones sin cifrado SMB activado, los datos transmitidos pueden quedar expuestos a ataques de interceptación, comprometiendo la confidencialidad de la información. También existen riesgos de explotación en firmas SMB débiles o deshabilitadas, lo que abre la puerta a ataques de transmisión y manipulación de paquetes.

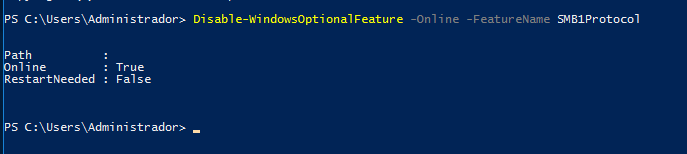
Aunque SMBv3 introduce herramientas como el cifrado extremo a extremo y mejoras en la autenticación, es crucial mantener las versiones actualizadas y usar configuraciones seguras para aprovechar al máximo su robustez y minimizar vulnerabilidades.

**Ejercicio 3. Muestra cómo deshabilitar la versión 1 de SMB.**

Para la detección de las versión 1 de SMB lanzaremos el siguiente comando en la terminal de PowerShell en Windows:



Y para deshabilitar la versión 1 lanzaremos el comando:



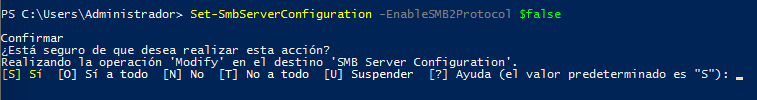
Como yo tenía deshabilitado ya el protocolo no me aparece la opción de elegir, pero si lo tuviésemos activos veremos la opción de poner Yes y se reiniciará el sistema.

**Ejercicio 4. Trabajando con el servidor de SMBv2, desactívalo y comprueba el resultado en el sistema. Finalizado lo anterior, realiza el mismo proceso para el cliente.**

Para desactivar SMBv2 en un sistema, primero debemos asegurarnos de tener acceso administrativo y realizar los cambios tanto en el servidor como en el cliente.

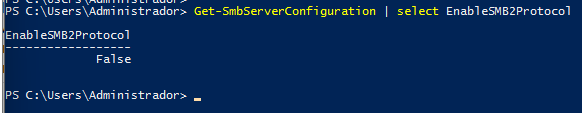
Para ello seguiremos los siguientes pasos en el servidor:

1. **Desactivar SMBv2:** Ejecuta el siguiente comando en PowerShell para desactivar SMBv2:



Este comando desactiva el protocolo SMBv2 en el servidor. Al ejecutarlo, el servidor ya no podrá usar SMBv2 para compartir archivos.

1. **Verificar que SMBv2 está desactivado**: Para comprobar que SMBv2 está desactivado, utiliza el siguiente comando:



El resultado debería indicar que el valor de EnableSMB2Protocol es False.

1. **Reiniciar el servidor**: Es recomendable reiniciar el servidor para asegurarse de que los cambios se apliquen correctamente

**Ejercicio 5. Busca información sobre los permisos NTFS. Aplica lo encontrado compartiendo carpetas con otros clientes Windows 10.**

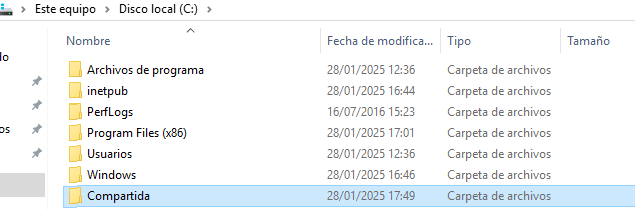
Los permisos NTFS son esenciales para controlar el acceso y las acciones que los usuarios pueden realizar en archivos y carpetas en discos formateados con el sistema de archivos NTFS en sistemas Windows. Los permisos NTFS permiten una gestión avanzada de la seguridad para proteger los datos frente a accesos no autorizados.

* **Permisos Básicos:**
  + Lectura: Permite al usuario ver el contenido del archivo o carpeta.
  + Escritura: Permite modificar archivos o agregar nuevos datos.
  + Modificar: Permite leer, escribir y borrar archivos o carpetas.
  + Control total: Permite cualquier acción, incluidos cambios de permisos
* **Permisos Avanzados:** Incluyen opciones como tomar posesión del archivo o cambiar atributos específicos.

Estos permisos son configurados directamente en las propiedades de archivos o carpetas bajo la pestaña Seguridad, y funcionan junto con las opciones de compartir en red para gestionar el acceso remoto.

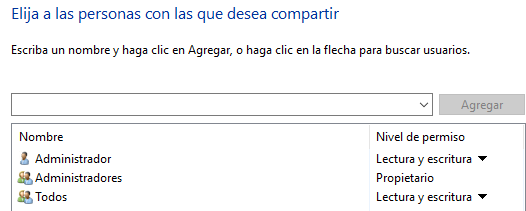
1. **Crear la carpeta:**

Crea una nueva carpeta en C:\ llamada “Compartida”

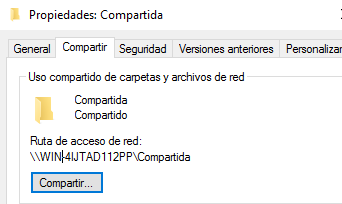


1. **Habilitar el uso compartido:**

Sigue los siguientes pasos: Propiedades → Compartir → Compartir… → elige Todos

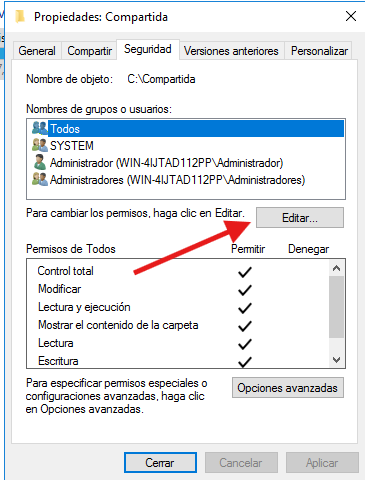


1. **Comprobar la ruta de acceso de red**



1. **Acceder a los permisos NTFS**

Sigue los siguientes pasos: Propiedades → Seguridad → Haz clic en Editar para modificar los permisos de los usuarios o grupos.

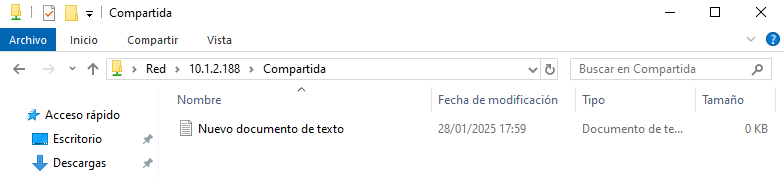


1. **Asignar permisos específicos**

Aquí podremos aplicar los permisos distinguidos por diferentes usuarios. Por ejemplo podemos asignar permisos de lectura y escritura a un usuario específico y a otro solo modificar esta carpeta

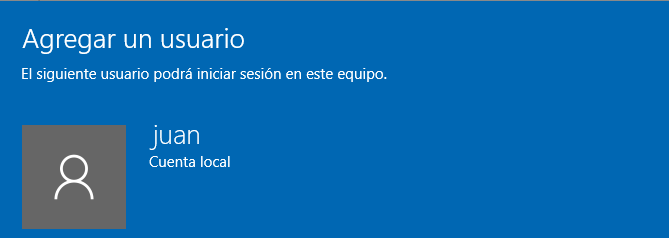
1. **Accede a la Carpeta desde otro equipo**

En un equipo Windows 10, abre el Explorador de Archivos y escribe la ruta de red en la barra de direcciones. Si tenemos los permisos necesarios podremos crear, modificar y eliminar documentos, en este caso podemos ver cómo hemos creado un documento

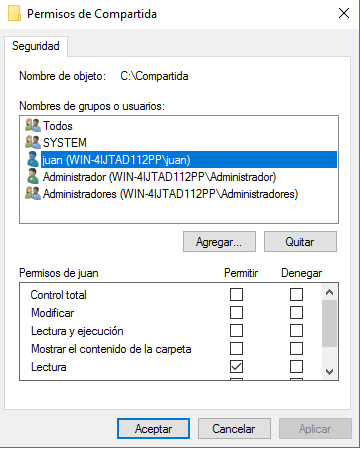


En caso de un usuario nuevo:

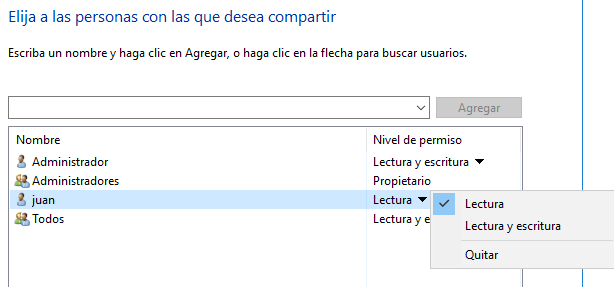
1. Comenzaremos creando el usuario juan



1. Aplicaremos este usuario a la carpeta compartida solo con el permiso de Lectura



1. Añadiremos el usuario Juan a los permisos de seguridad compartida de la carpeta con el permiso único de Lectura.

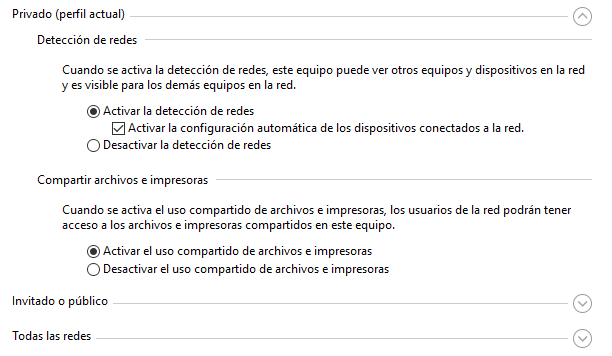


1. Guardamos la configuración y comprobamos desde la cuenta de juan los permisos actuales

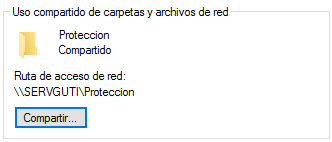
**Ejercicio 6. Configura el sistema para poder compartir archivos y carpetas con protección por contraseña y sin ella.**

**Compartir archivos con protección:**

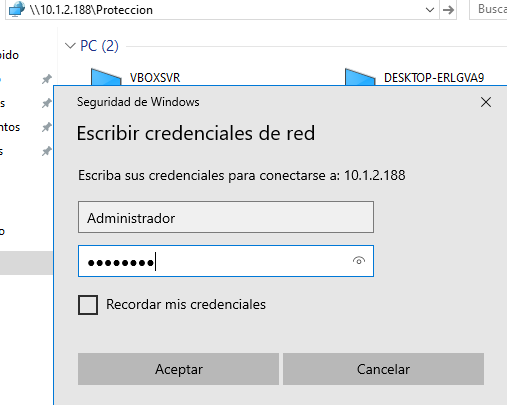
Para ello seguiremos los siguientes pasos: Centro de redes y recursos compartidos → Cambiar configuración de uso compartido avanzado → Cambiar configuración de uso compartido avanzado, además selecciona Habilitar el uso compartido con protección por contraseña.



Crea una nueva carpeta y compartirla en red

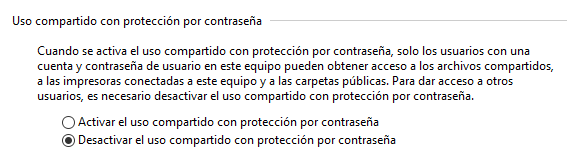


Buscar la carpeta compartida en un equipo cliente de Windows, si todo ha funcionado correctamente el servidor nos pedirá las credenciales correspondientes para el uso de la carpeta compartida. En ella podremos ver los archivos del interior y crear nuevos



**Compartir archivos sin protección:**

Para compartir los recursos compartidos sin credenciales, únicamente deberemos desactivar el uso compartido con protección por contraseña.



Una vez guardados los cambios, desde otro equipo de la red, buscaremos la ruta de la carpeta compartida y comprobaremos que no necesitamos credenciales

[Ver video de comprobación](https://drive.google.com/file/d/1Yo7AbAHcJ7CZ284qPwZ8scOglA5x_p84/view?usp=drive_link)