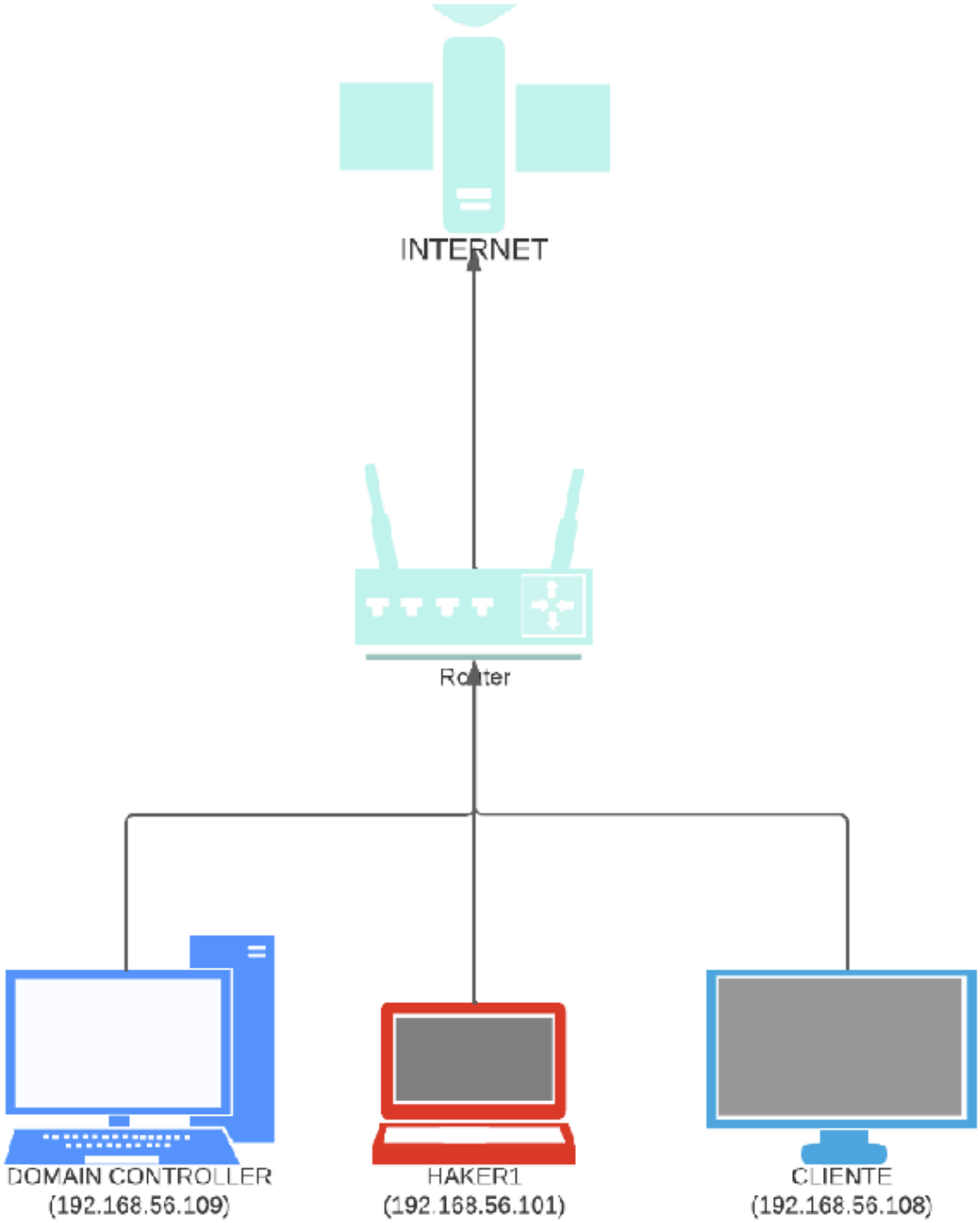
David Barros Caamaño

Bastianado de un AD

Índice

Entorno

El entorno de partido va a ser el siguiente:



En este entorno vemos que tenemos una máquina que va a funcionar como controlador de dominio o AD (192.168.56.109). Una máquina que va a funcionar como cliente de este controlador de dominio (192.168.56.108) y otra máquina que va a ser nuestro equipo atacante(192.168.56.101).

Partimos como base de una configuración por defecto de nuestro AD, es decir, tenemos instalado los requerimientos necesarios para tener un dominio en Windows, el equipo del AD está actualizado con las últimos parches y la máquina está añadida al dominio.

Vulnerabilidades

SMB RELAY

La primera vulnerabilidad de la que vamos a hablar se trata de SMB RELAY.

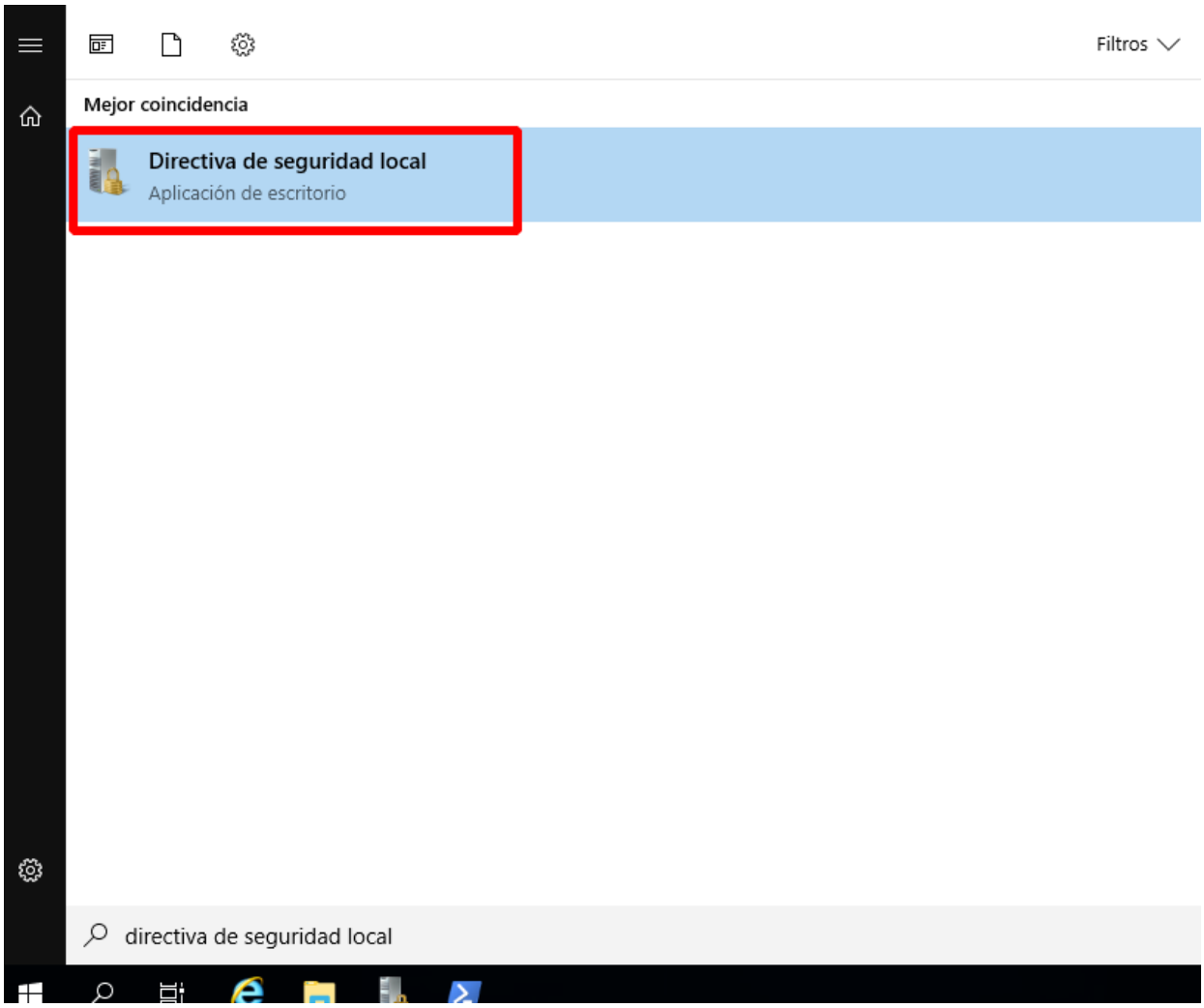
SMB RELAY no es más que una técnica ampliamente utilizada a la hora de hacer pentesting en entornos de directorio activo para tú como atacante ganar acceso a los equipos de una red. Lo que sucede es que en muchas redes empresariales existen sistemas automatizados que lo que hacen es, conectarse a otros equipos de la red para realizar tareas como por ejemplo:realizar un inventario del software instalado, actualizar antivirus, realizar backups y un largo etcétera.

Entones lo que harían los atacantes es, quedarse en escuchar a la espera de que alguno de estos sistemas automatizados se conecten con él. En el momento de que el equipo víctima se conecte con nosotros nos enviara su hash ntlmv2 para hacer la autenticación, este hash lo que podremos hacer con él es pasarlo por un programa de craqueo de hash offline como hashcat. Si el hash es lo suficientemente débil obtendremos las contraseñas de ese usuario. Con este tipo de técnica podemos obtener tanto un hash de un usuario admin como de un usuario sin privilegios.

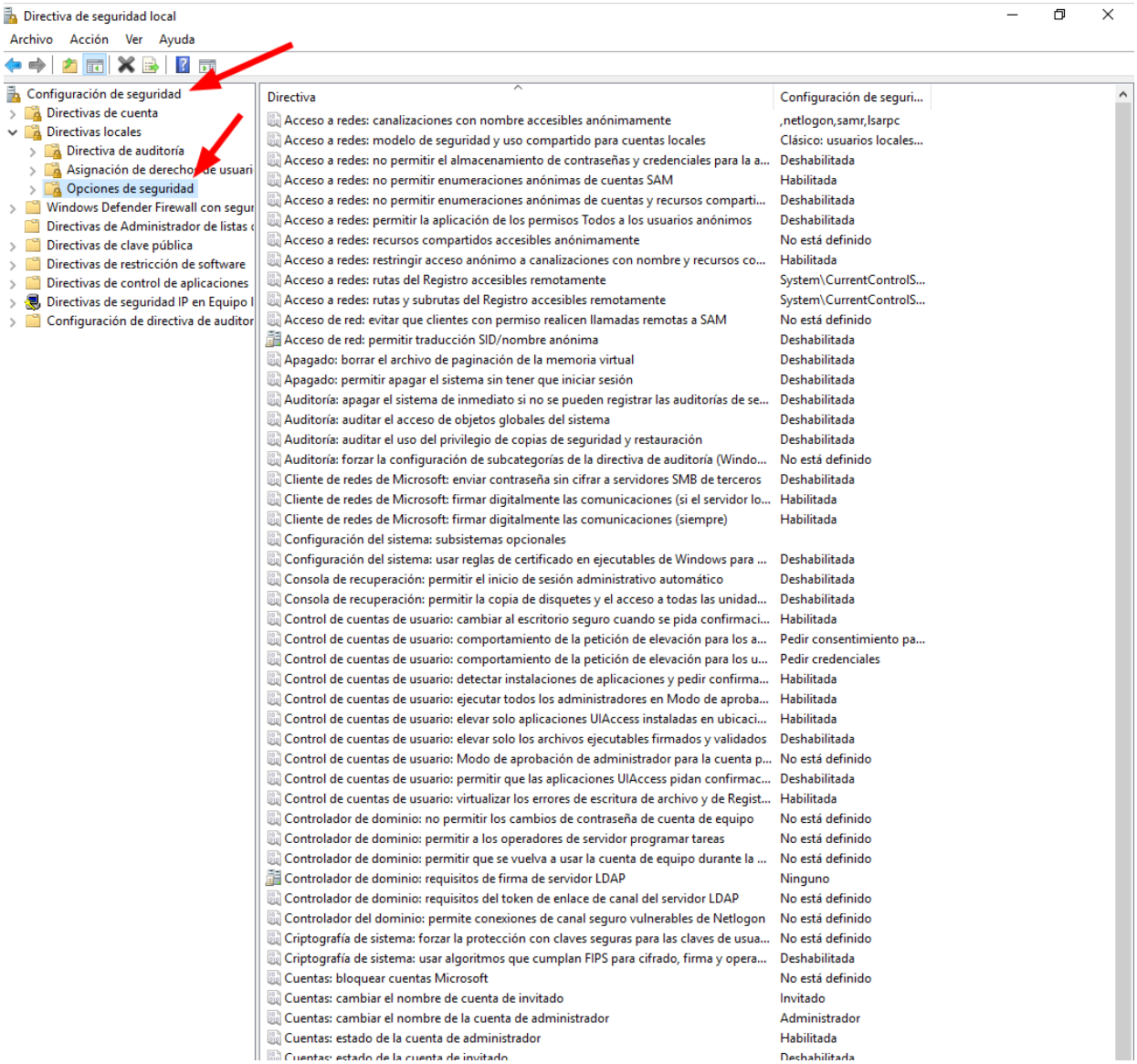
Todo esto es debido a que por defecto en los equipos Windows (tanto servidor como cliente) no se firman los paquetes del protocolo smb, por lo tanto, no se puede comprobar la autenticidad de estos mismos.

Para subsanar este tipo de ataque lo que debemos hacer es lo siguiente:

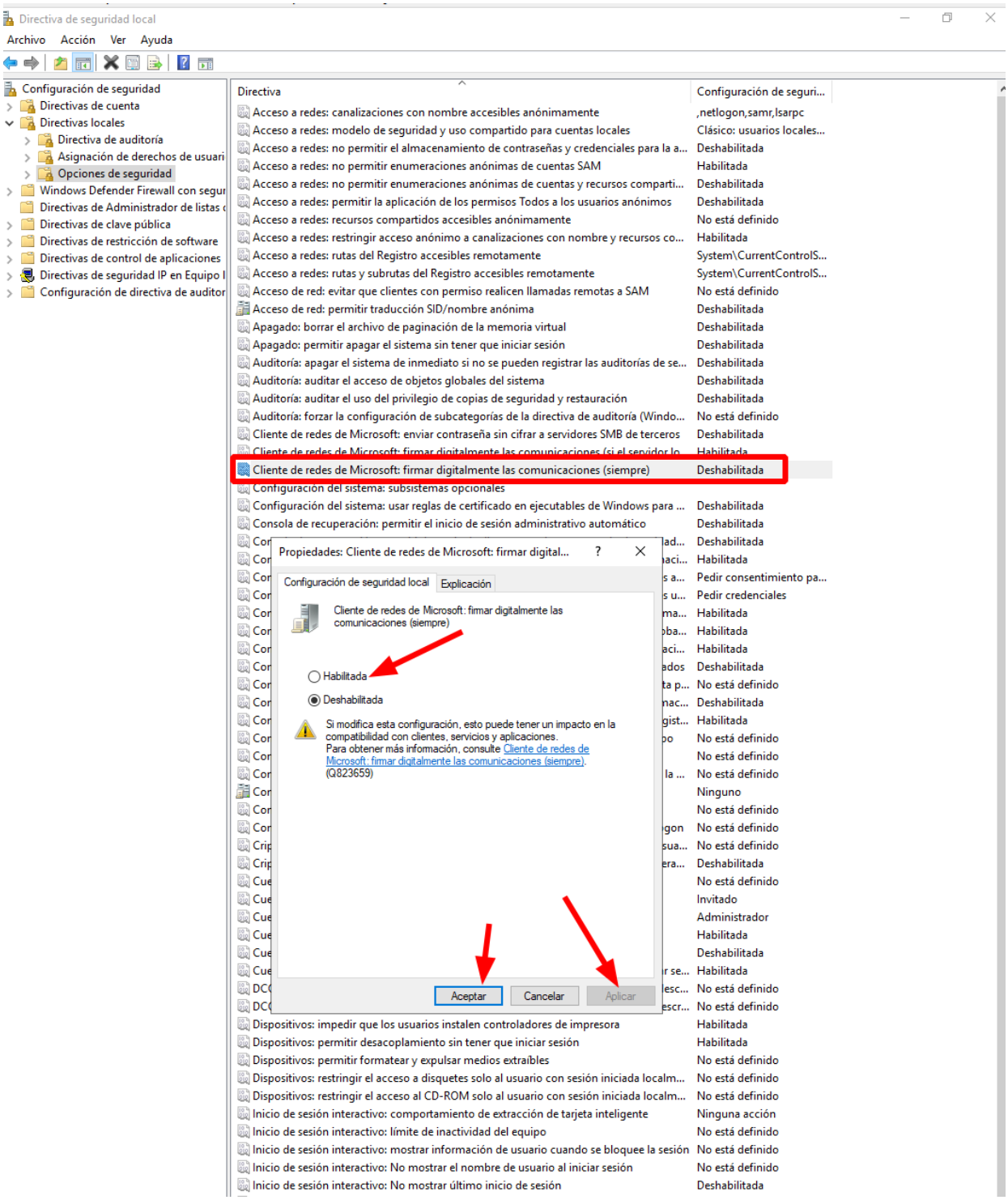
Lo primero será acceder al panel de Directiva de seguridad Local de nuestro servidor:



En este panel podremos ver varias directivas, pero la que nos interesa es la directiva de **"Opciones de seguridad"**, seleccionamos esta opción y nos aparecerán todas las directivas que se aplican al equipo.



Dentro de estas, la opción que nos interesa será **Clientes de redes de Microsoft: firmar digitalmente todas las comunicaciones(siempre)**. Esta opción aparece **deshabilitada** por defecto, tendremos que habilitarla como se refleja en la siguiente figura:



Luego de hacer esto reiniciaremos nuestra máquina, con esto las comunicaciones por SMB estarán firmadas.

Conexión por WinRM

WinRM es un protocolo estándar basado en protocolo simple de acceso a objetos (SOAP), que permite la interoperación entre hardware y sistemas operativos de diferentes proveedores. Esto quiere decir que es un protocolo utilizado por los servicios de Microsoft para la administración remota de equipos para aplicar configuraciones, realizar gestiones, etc.

El problema que presenta este protocolo es que una vez un usuario conozca nuestro usuario y contraseña podrá autenticarse en nuestra máquina sin ningún tipo de restricciones de forma remota.

Existen numerosas herramientas que automatizan este proceso para los atacantes, como por ejemplo evil-winrm. Este programa está basado principalmente en la librería WinRM Ruby la cual cambió su forma de trabajar desde su versión 2.0. Ahora, en lugar de usar el protocolo WinRM, está usando PSRP (Protocolo de comunicación remota de Powershell) para inicializar grupos de espacios de ejecución, así como para crear y procesar canalizaciones.

El protocolo de WinRM se aloja principalmente en el puerto 5985. Por lo que los atacantes lo podrán detectar fácilmente con programas de enumeración de puertos como nmap.

Para deshabilitar este servicio deberemos de ejecutar una powershell con privilegios de administrador y ejecutar:

```
Disable-PSRemoting -Force
```

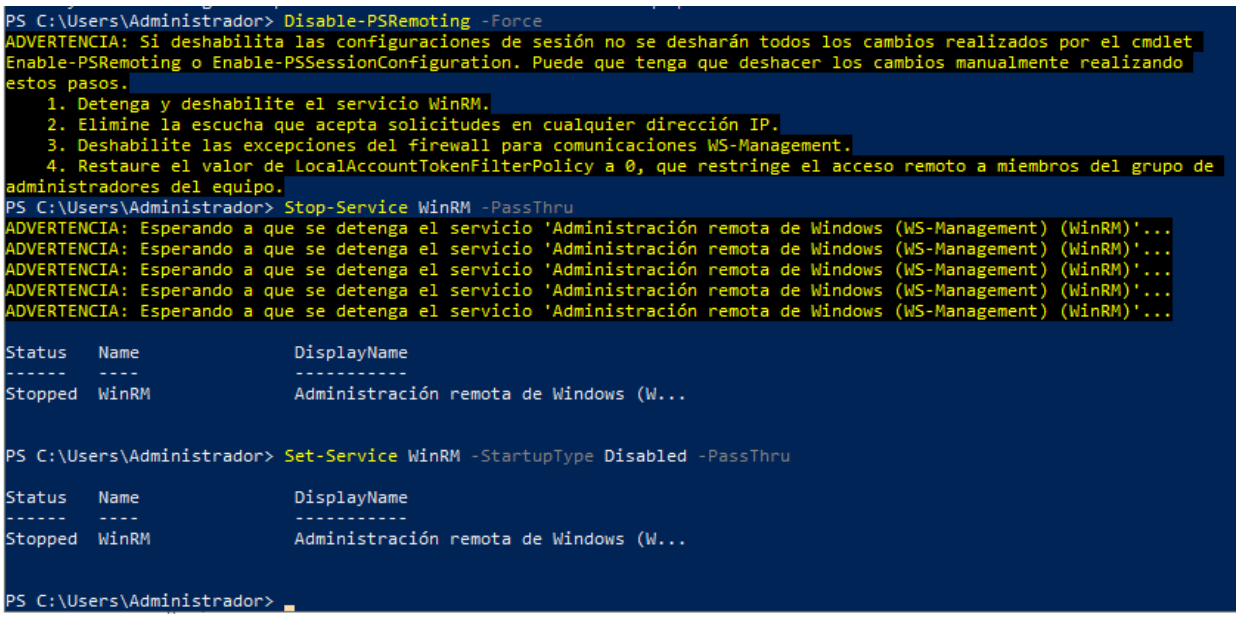
```
Stop-Service WinRM -PassThru
```

```
Set-Service WinRM -StartupType Disabled -PassThru
```

Estos comandos deshabilitarán los servicios de WinRM en nuestra máquina para así evitar conexiones inseguras.

El primer comando lo que hará es deshabilitar la ejecución de comandos remotos, sin embargo, para detener el servicio por completo deberemos ejecutar el segundo. Y el tercero sirve para establecer el servicio como detenido al inicio.

En la siguiente figura podemos ver la ejecución de los comandos:



Permisos en carpetas compartidas de red

Los permisos de carpetas compartidas en red son otro importante vector de ataque de red, puesto que muchas personas dan permisos innecesarios a los usuarios.

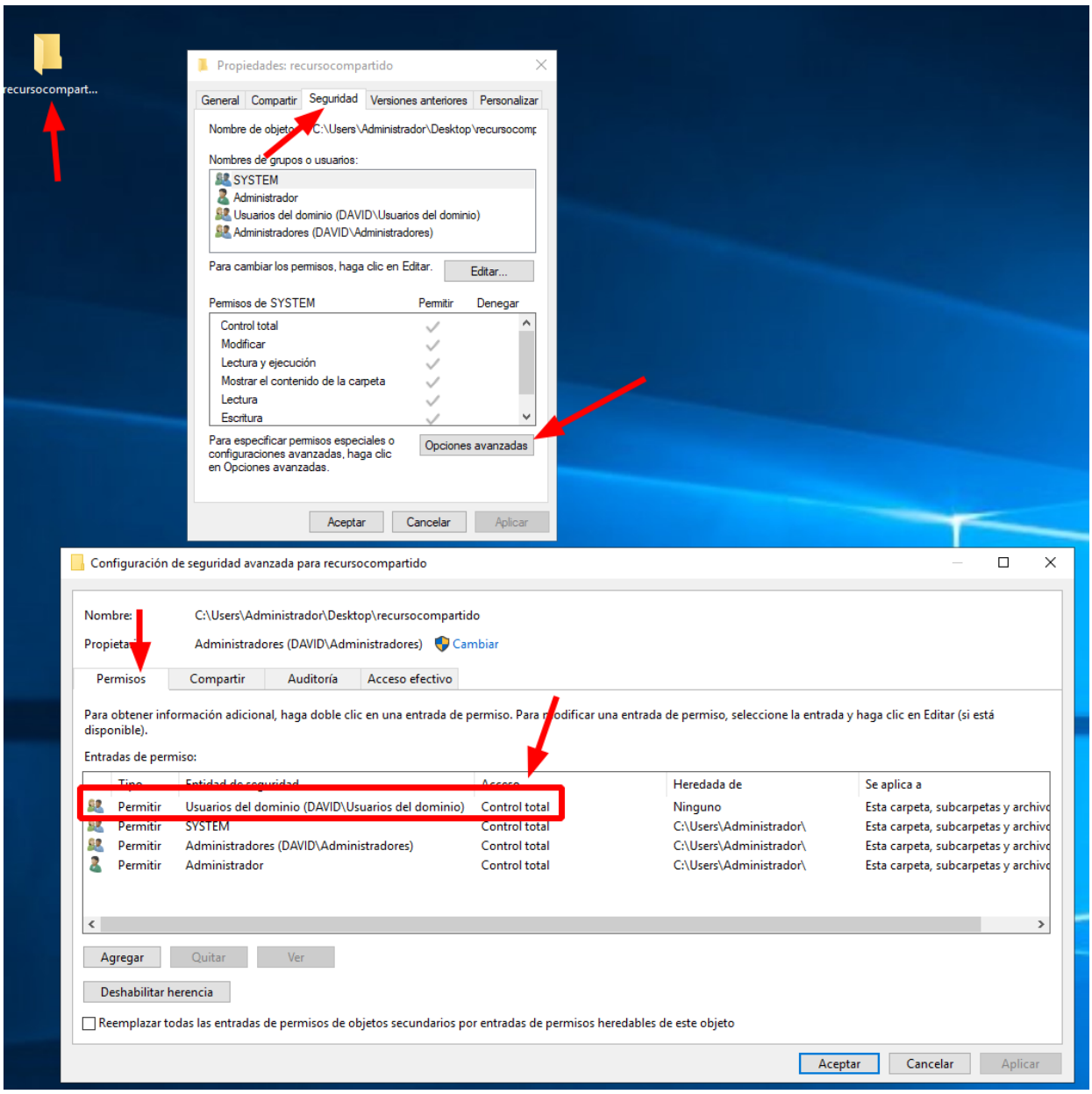
Si tenemos en cuenta que ya hemos obtenido las credenciales de un usuario del dominio a través de la técnica de SMB Relay podemos enumerar las carpetas compartidas que hay en el dominio y los permisos que este posee sobre estas.

Para ello nos ayudaremos de herramientas como smbmap la cual no dirá que carpetas puede ver nuestro usuario del dominio y en cuáles de ellas puede escribir.

Una vez sepamos este tipo de permisos podremos subir un fichero malicioso a nuestra carpeta compartida, de tal forma que cuando un usuario administrador del dominio abra esta carpeta se nos mostrará su hash ntlmv2.

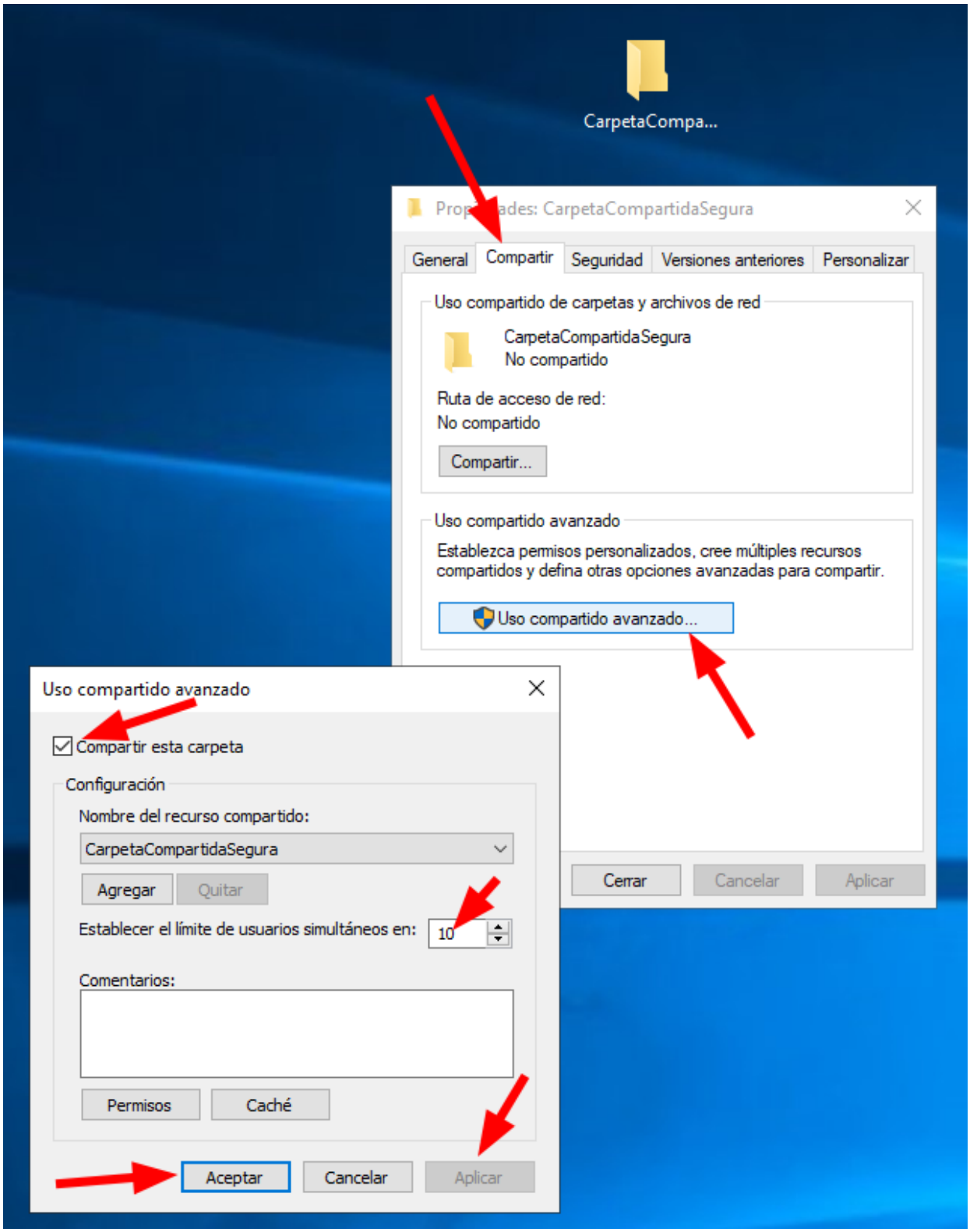
Para protegernos de este tipo de ataques, lo que deberemos hacer es administrar nuestras carpetas de tal forma que solo los usuarios que necesiten escribir en estas carpetas tengan dichos permisos y no todos los usuarios del dominio.

A continuación vemos un ejemplo de una carpeta compartida en al que cualquier usuario del dominio tiene privilegios para escribir en ella:

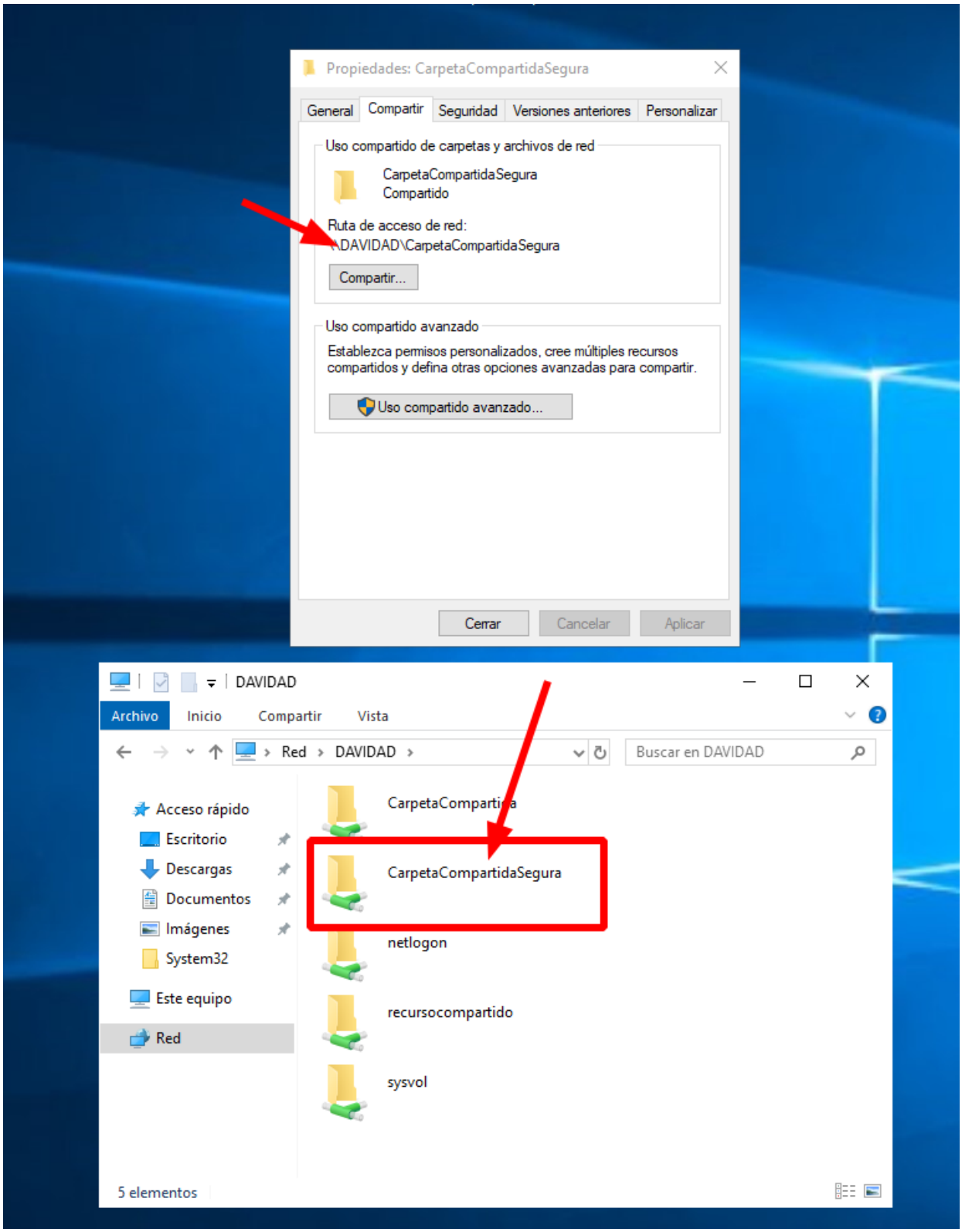


Para crear una carpeta con los privilegios justos para cada usuario, lo recomendable es:

Creamos una carpeta y en propiedades nos vamos a compartir, una vez aquí seleccionamos **Uso compartido avanzado** y limitamos el número de usuarios simultáneos a un número que nos sea adecuado, en este caso 10:



Una vez hecho esto tendremos nuestro recurso compartido creado, esto lo podemos ver si accedemos a la ruta que se nos indica en el apartado **Ruta de acceso de red**:

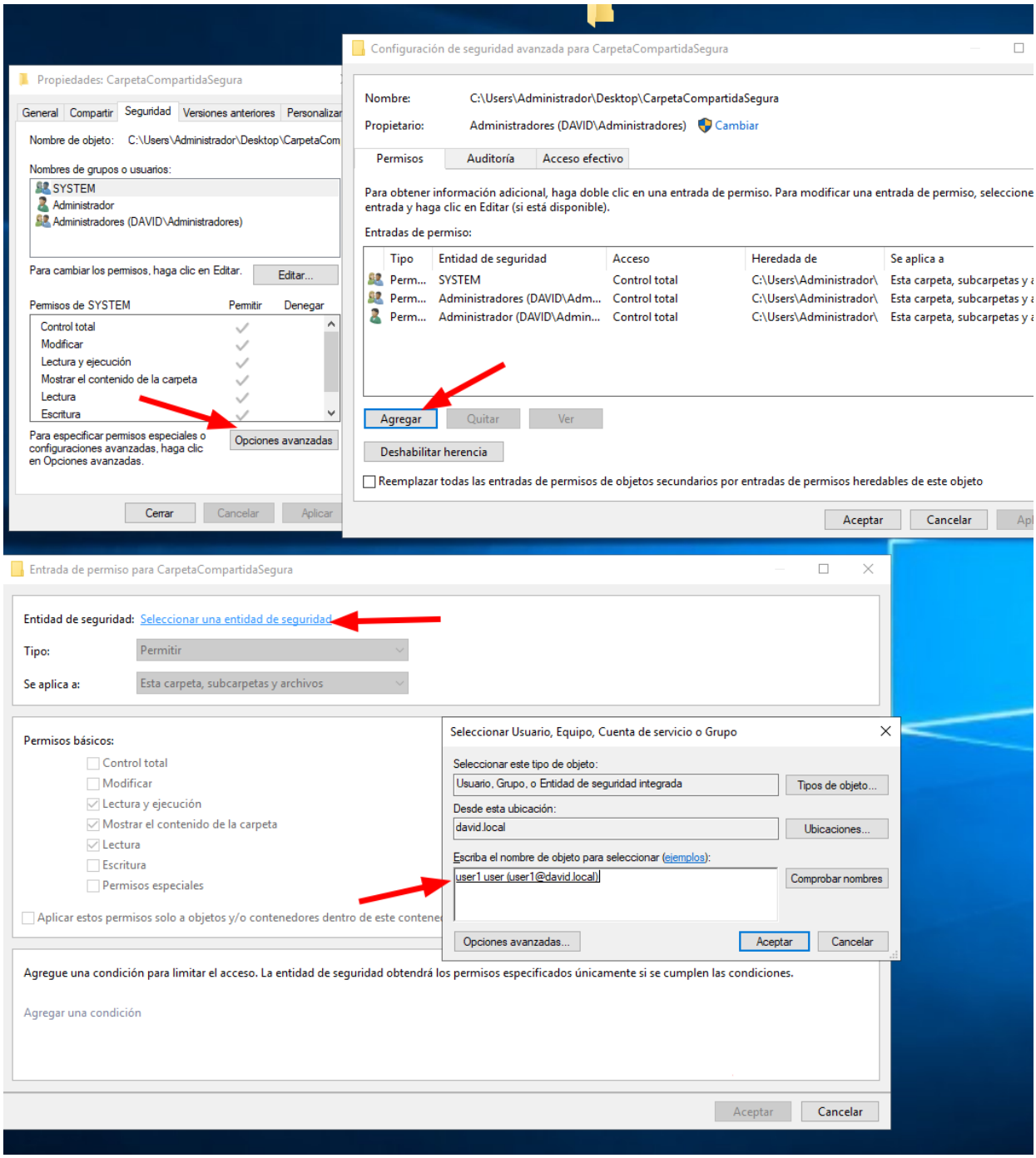


Pero esta carpeta solo tendrá permisos para que puedan acceder a ella los usuarios administradores del dominio.

A continuación deberemos acceder al apartado **Seguridad** y seleccionar **Opciones Avanzadas**.

Esto nos abrirá un panel en donde si seleccionamos **Agregar** nos mostrará otro panel en el que debemos seleccionar **Seleccionar una entidad de seguridad**. Una vez aquí deberemos escribir el nombre del grupo o en su defecto el usuario que queramos añadir. Lo más recomendable es crear previamente un grupo de usuarios que tendrán permisos para esa carpeta.

Una vez lo tengamos seleccionado haremos clic en comprobar nombres y se añadirá el usuario/grupo haciendo clic en aceptar:



Bibliografía

https://www.youtube.com/watch?v=-bNb4hwgkCo

https://www.youtube.com/watch?v=Ekw4X_QrHJ0

https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102

https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/overview-server-message-block-signing

https://learn.microsoft.com/es-es/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

https://learn.microsoft.com/en-us/answers/questions/1183850/how-can-i-do-to-enable-and-disable-winrm-(window-r

https://learn.microsoft.com/es-es/windows/win32/winrm/portal

https://infinitelogins.com/2020/06/17/enumerating-smb-for-pentesting/

https://10degres.net/smb-null-session/

https://github.com/Hackplayers/evil-winrm

https://github.com/ShawnDEvans/smbmap