Server Exploits - File Shares

Module 2

Overview

File Sharing

File sharing in Active Directory is a great way for many users on the domain to access and store files remotely. Usually, an organization would have a dedicated file server that hosts many remote shares and folders for users to access. However, permissions regarding file are important. Users should not be able to access data they don't need to (Principle of Least Privilege). Sensitive information being out in the open on a network is a prime target for hackers to steal from an environment.

File Sharing - Permissions

A file or folder can have different permissions depending on how you set them. By default, a folder will inherit the permissions of the folder its in. So if you create a folder on a user's desktop, that folder will have the same permissions tied to it as the user's desktop. If you want to create custom permissions, you can disable inheritance for a folder.

There are several different permissions you can give to a folder. You can set each Active Directory group to have different permissions on a folder. Groups or users can have more than one of the following permissions to a file share.

File Sharing - Full Control

Allows the group or user to:

- **view file name and subfolders.**
- **navigate to subfolders.**
- **view data in the folder's files.**
- **add files and subfolders to the folder.**
- **change the folder's files.**
- **delete the folder and its files.**
- **change permissions.**
- **take ownership of the folder and its files.**

This is the highest level of privilege you can give, and in an ideal world should never be set for a file share given its high level of access.

File Sharing - Modify

Allows the group or user to:

- **view the file names and subfolders.**
- **navigate to subfolders.**
- **view data in the folder's files.**
- **add files and subfolders to the folder.**
- **change the folder's files.**
- **delete the folder and its files.**
- **open and change files.**

This is still very high access, giving the user or group permission to modify everything about the file share.

File Sharing - Read and Execute

Allows the group or user to:

- **view file names and subfolder names.**
- **navigate to subfolders.**
- **view data in the folder's files.**
- **run applications.**

There may be a reason to host applications on a remote file share. This lets users run remote applications without being able to modify the contents of the folder, which is usually supporting files for the application.

File Sharing - List Folder Contents

Allows the group or user to:

- **view the file names and subfolder names.**
- **navigate to subfolders.**
- **view folders.**
- **does not permit access to the folder's files.**

This is a pretty basic permission just allowing one to navigate through the folders in a file share without being able to actually open the files.

File Sharing - Read

Allows the group or user to:

- **view the file names and subfolder names.**
- **navigate to subfolders.**
- **open files.**
- **copy and view data in the folder's files.**

This just allows users and groups to read files on the share and not modify them or add new files.

File Sharing - Write

Allows the group or user to:

- **create folders.**
- **add new files.**
- **delete files.**

This just allows users and groups to add to the existing file share, but not actually read any of the files.

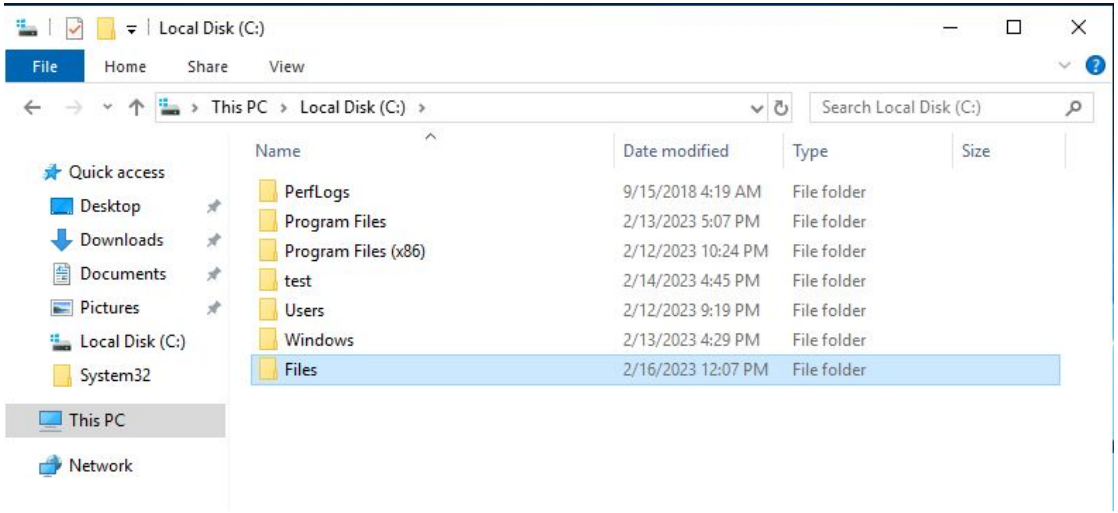
File Sharing - Permissions

When you give permissions to a member who is part of more than 1 group, they will get the most permissions they can from both their groups. For example, if User is part of Domain Users and Test_Group, and Domain Users has read access to a folder but Test_Group has read and write, User will get read and write permissions to that folder.

Creating a File Share

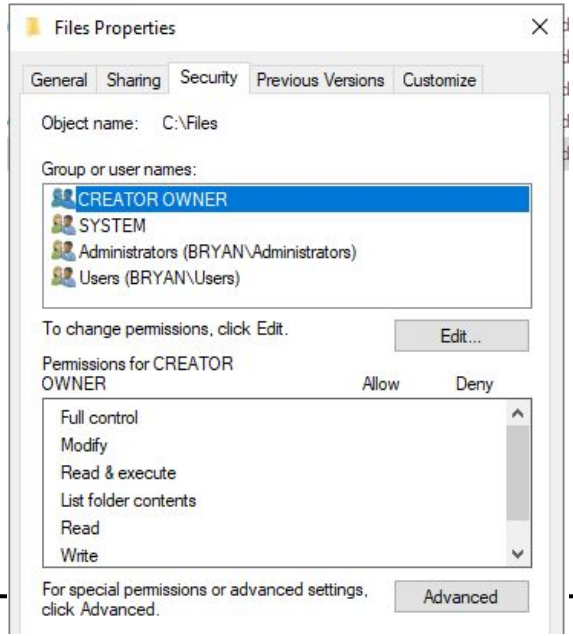
Creating a file share

The first thing we need to do is create a folder.I'm going to create on on my C drive on my DC by right-clicking and selecting new -> Folder. I call this folder Files.



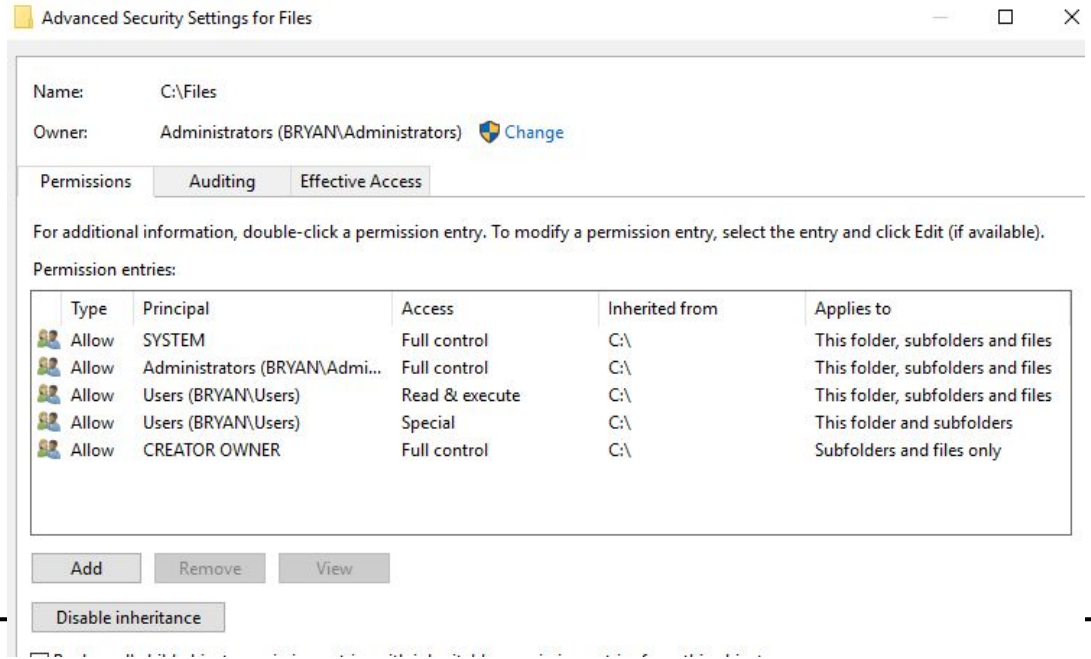
Creating a file share

I can right-click my folder and select Properties. Under the Security Tab, I can see all the permissions for all groups the folder has inherited by being on the C drive. Note that if a group isn't shown, then that group has on permissions on the folder.



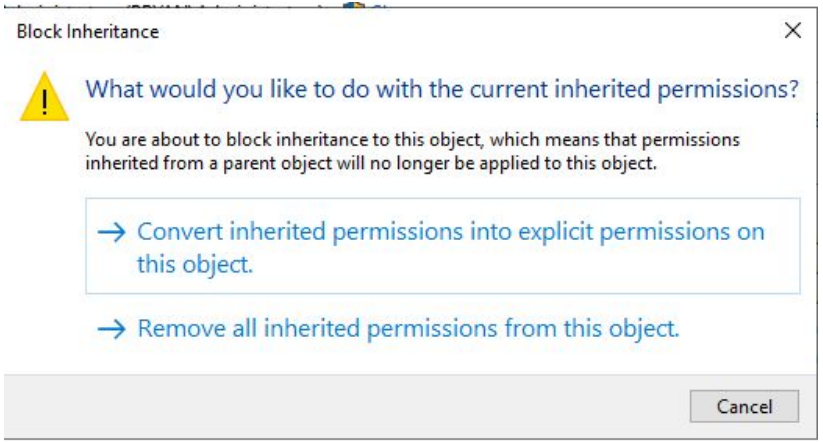
Creating a file share

Because I want to set up my own custom permissions, I want to disable inheritance. Click on the Advanced button in the Security Tab, then click Disable Inheritance.



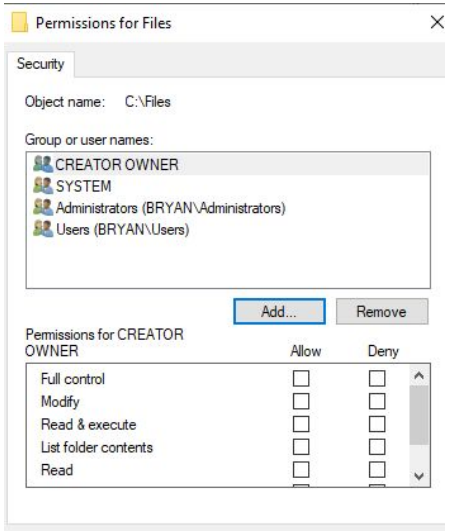
Creating a file share

You'll want to select "Convert inherited permissions into explicit permissions on this object". This will disable the folder's inheritance so that it will not inherit permissions from being on the C drive, but retain the permissions it had by default. We can then modify the permissions ourselves. If you click "remove all inherited permissions" then no one will have permissions on this folder, and no one will be able to modify anything about it including the permissions.



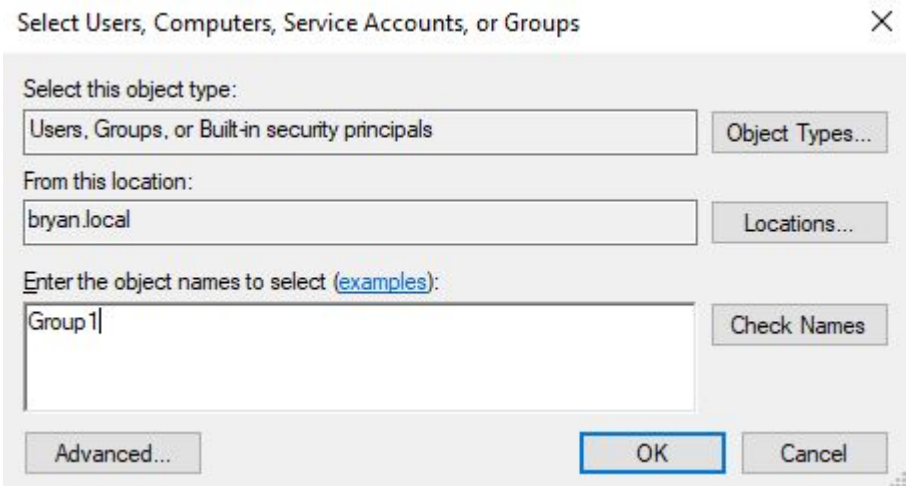
Creating a file share

We can now modify the permissions of the file. After you hit Apply for disabling the inheritance, you will be brought back to the Security Tab. I have already created a group of Users called Group1 I would like to give Read access to this folder. I click Edit in the Security Tab.



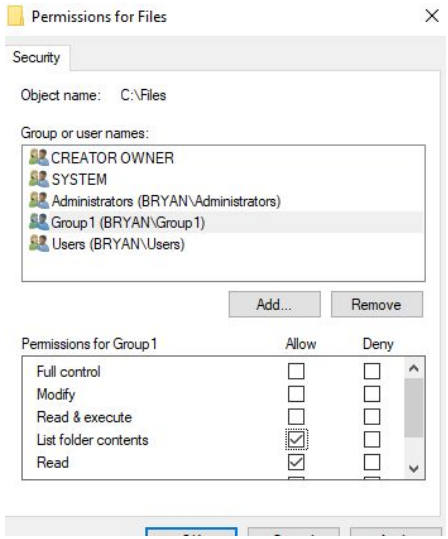
Creating a file share

Because Group1 is not listed under Groups or user names, I need to add Group1 to assign it permissions. I do that by clicking Add, then typing the name of my group, and hitting OK.



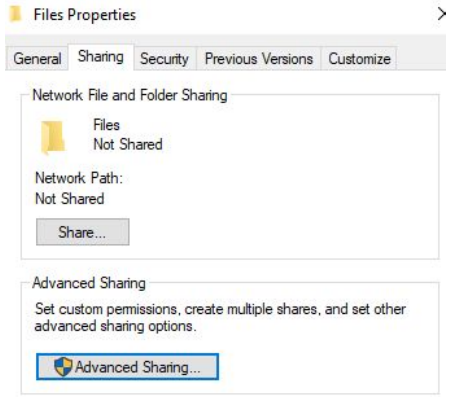
Creating a file share

I can now assign permissions to Group1 by checking the boxes under the Permissions for Group 1 box. Because I only want to give limited access to read files and navigate folders access, I only select the Read and List folder contents permissions, then hit Apply.



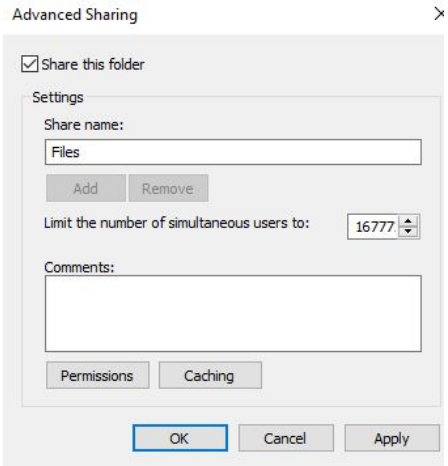
Creating a file share

With the permissions set up, I can go to the Sharing tab.



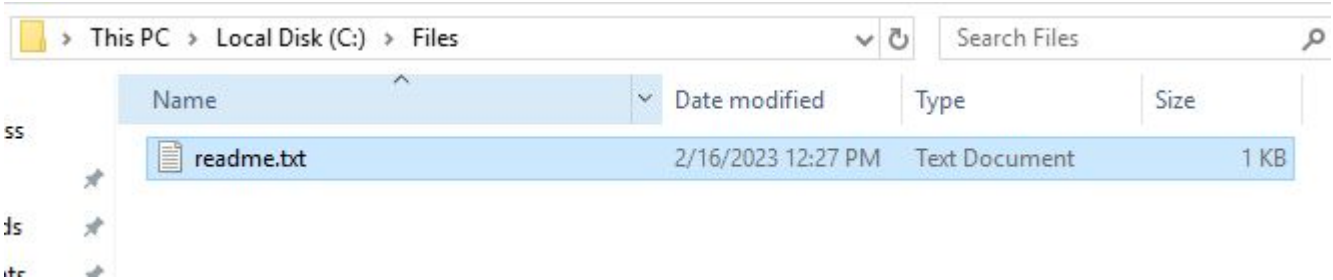
Creating a file share

I click on Advanced Sharing and click the Share this folder box. Here you can create your share name, which by default is the name of the folder. You can also limit the number of users that can access the file share at a time. This setting can be left default.



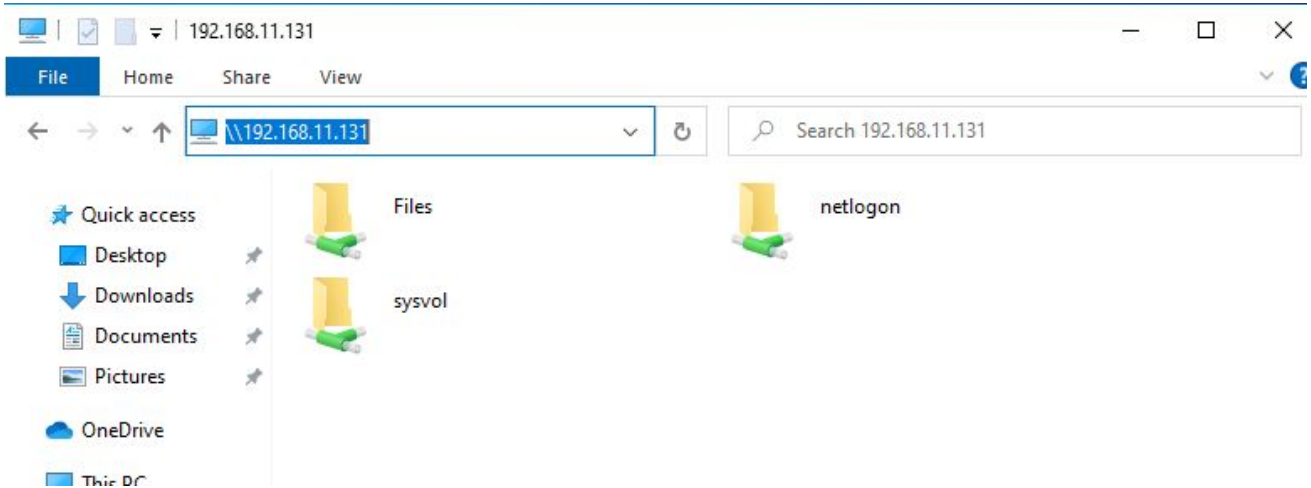
Creating a file share

After you hit OK, you are now ready to view the folder from your workstation. Before I log into my workstation as a user that's a member of Group1, I create a text file for that user to read. The user should be able to read the text document, but not be allowed to modify it or add more documents.



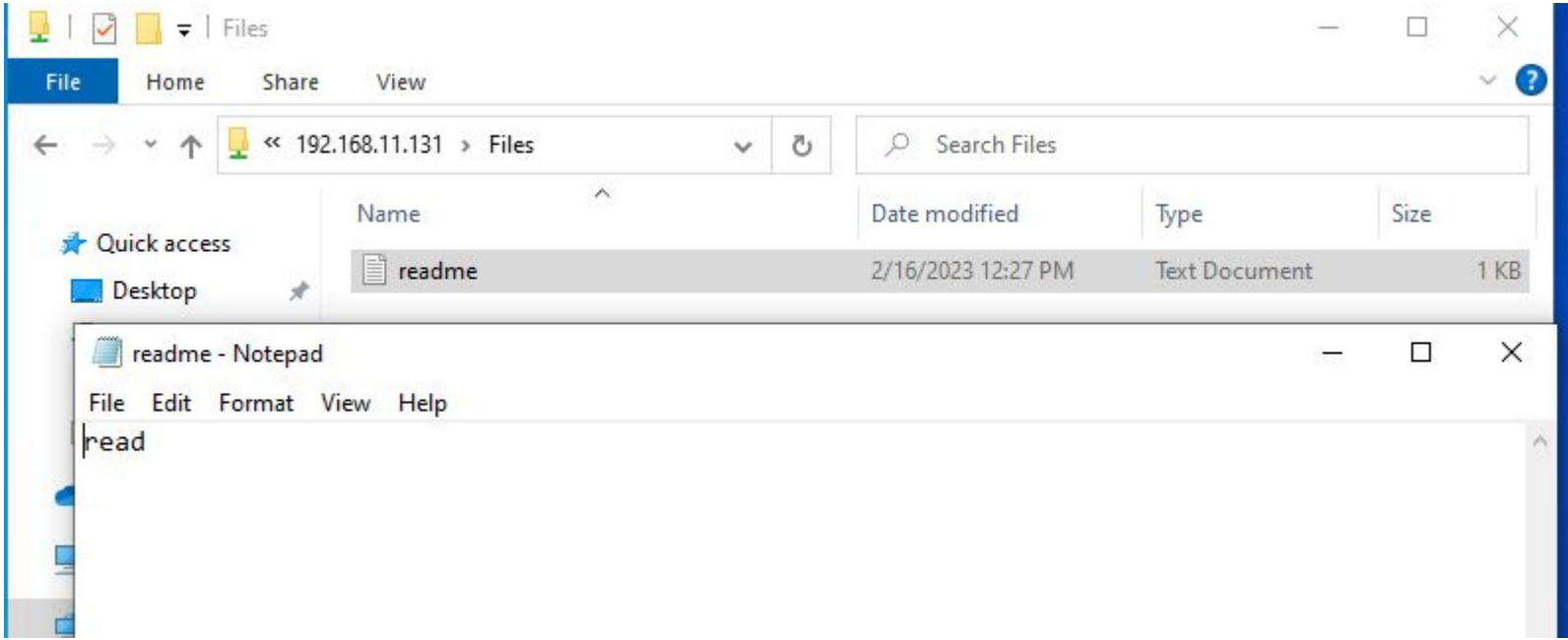
Creating a file share

After logging into my workstation as my Group1 member, I can open up my file explorer and navigate to my file share by typing \\<dc_ip>. My DC's IP address is 192.168.11.131. We can see the Files share, so lets click on that.



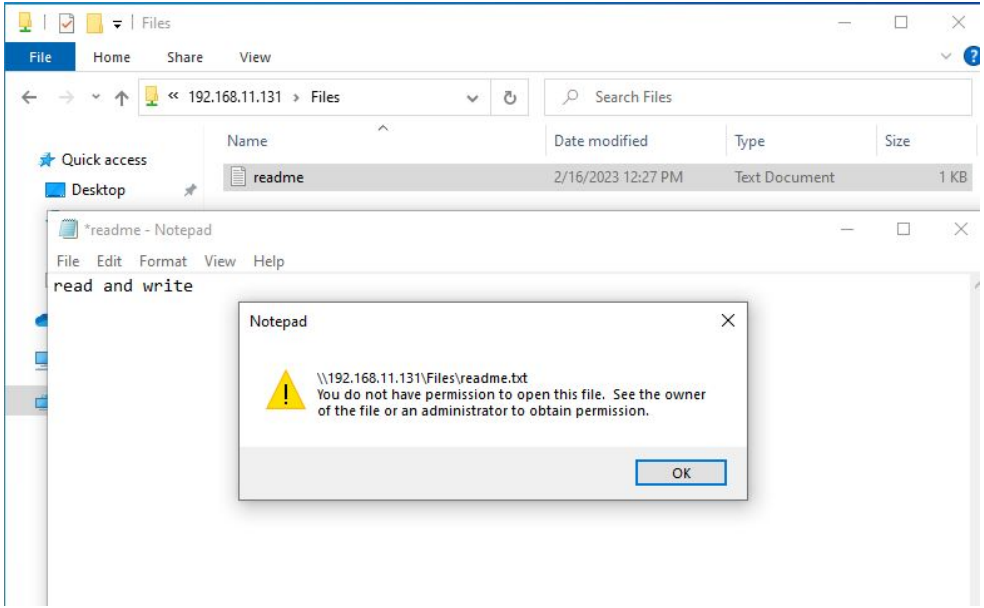
Creating a file share

Here I can see my readme text file, and I can open and read it.



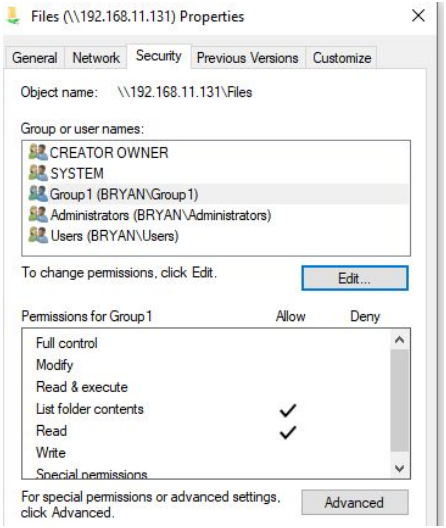
Creating a file share

When I try to modify the file and save it, I am presented with this error because I do not have write permissions for this folder. I am also unable to add any documents to the folder.



Creating a file share

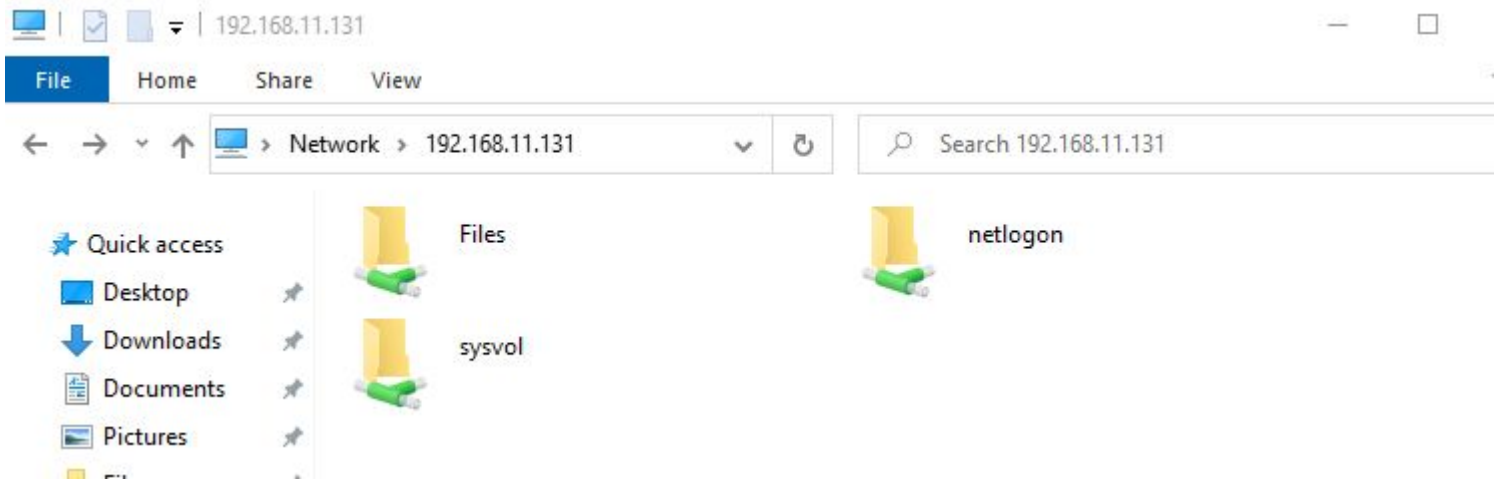
Because I have read access, I can read the folder's permissions but I can't edit them.



Extras

Sysvol and Netlogon

You have have noticed that on your DC there are 2 other shares, netlogon and sysvol. By default only local administrators can access these, and they are typical on DCs.



Sysvol and Netlogon

Sysvol is used to house GPOs and distribute them to objects on the domain. When you run gpupdate, your workstation gets its policies from here.

The netlogon share houses logon scripts. When a user logs into a machine, it executes the logon script on this share if there is one. This script can adjust things about the operating system, mnap network drives, or display welcome messages. By default, the netlogon share should be empty if you've not created logon scripts.