### 4.3 SMB Server

One of the simplest protocols out there, the Server Message Block protocol allows for a computer to share its files with others. A server that realizes the SMB role, therefore, is a file server.

# Vuln History

Now you may be thinking, why do I need to know about the old SMB? Trust me, it’s important, because the old one is vulnerable. Ever heard of EternalBlue? Maybe you’ve heard of the ransomware WannaCry? They are both centered around SMB’s old versions.

## SMB / CIFS / SMB1

If you have SMB1 turned on, TURN IT OFF. This protocol is very old and is vulnerable to EternalBlue and WannaCry, allowing for possible remote code execution (RCE). The only reason why it still exists as a possible feature in the newer Windows systems is for backwards compatibility with computers you will probably never use.

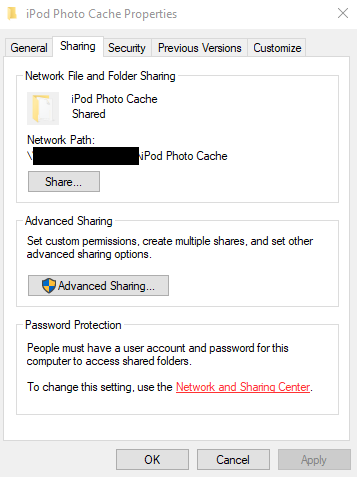
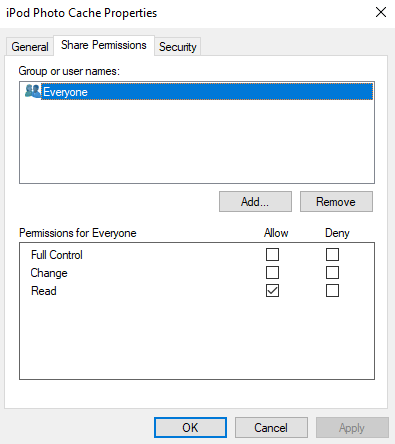
Please, please, please use SMB 2 or SMB 3 instead, they are way more secure.

If you absolutely need to use SMB1, make sure to install the SMB1 patch (see MS17-010)

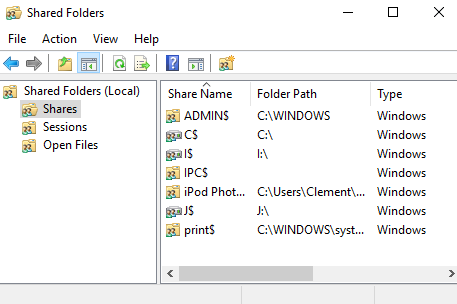
# Setup

To set up an SMB server, you will need to share a folder. You can use fsmgmt.msc or just go to the folder’s properties and share it under the Share tab. That’s it.

If you haven’t realized from the above instructions yet, both workstations and servers can be SMB servers. Very cool! not really but yay i guess

Note: the Everyone permission pertains to anyone who can get by your computer’s firewall for a file share. This means that if your firewall is up to its max, someone from Russia cannot access your share.

Usually, “Everyone” will mean users within your private network.

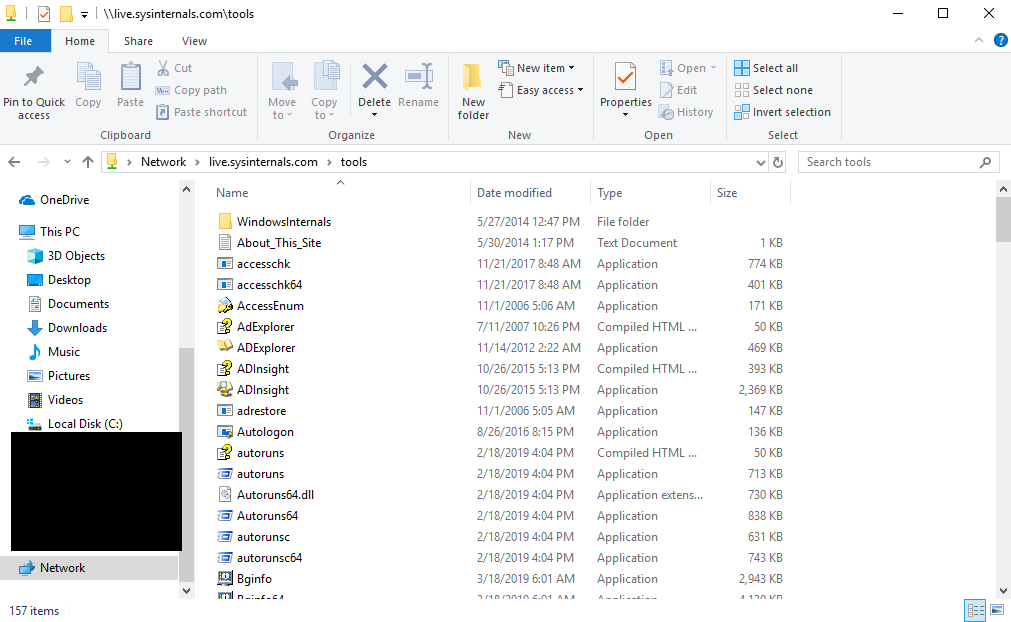


# Accessing the Share

To access the share, go to file explorer. Then, enter the UNC (Universal Naming Convention) path. For example:

\\CLEM-COMPUTER\iPod Photo Cache

\\live.sysinternals.com\tools ← you should try this at home! if your computer or network do not block SMB, you can access sysinternals tools straight from Windows Explorer!



# Security

When file sharing comes to mind, what should be secured?

USE COMMON SENSE! :D

* Make sure the files in the share are what you want to share
* Set the correct permissions
* Ensure that the FREAKING PROTOCOL IS SECURE WHY WINDOWS WHY ARE YOU LIKE THIS ahem yeah just disable SMB1 and update