SMB Server

Click to add subtitle

Basic

What is it?

- One of the simpleset protocols out there
- Allows for a computer to share its files with others
  - That is why a file server realizes SMB roles

Trivia: linux's version is called samba

Vulnerability History

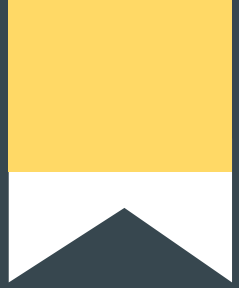
Old SMB

- Very vulnerable
- Bad stuff centered around it:
  - EternalBlue
  - Ransomware WannaCry

SMB / CIFS / SMB1

- If SMB1 is on... turn it OFF
  - Is old and vulnerable to bad stuff mentioned previously-> allows for possible remote code execution (RCE)
  - Only reason it exists: backwards compatibility with useless computers
- Use SMB2 or SMB3 (are more secure)
- IF SMB1 is necessary get the patch (MS17-010)

Setup



What can an SMB server be?

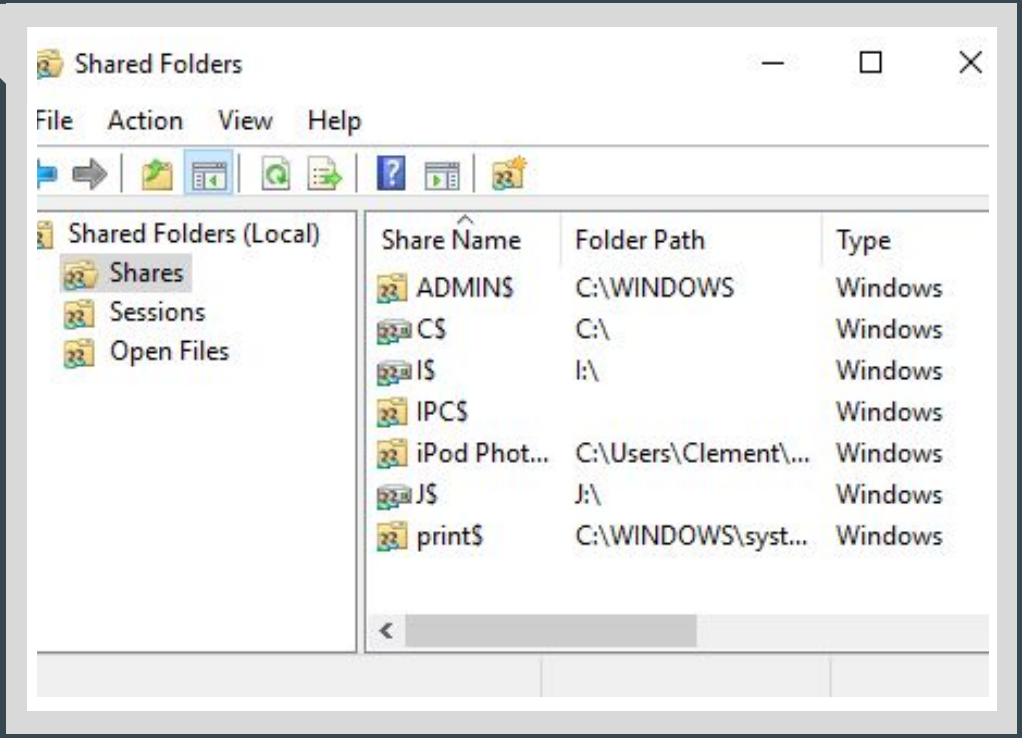
Workstations

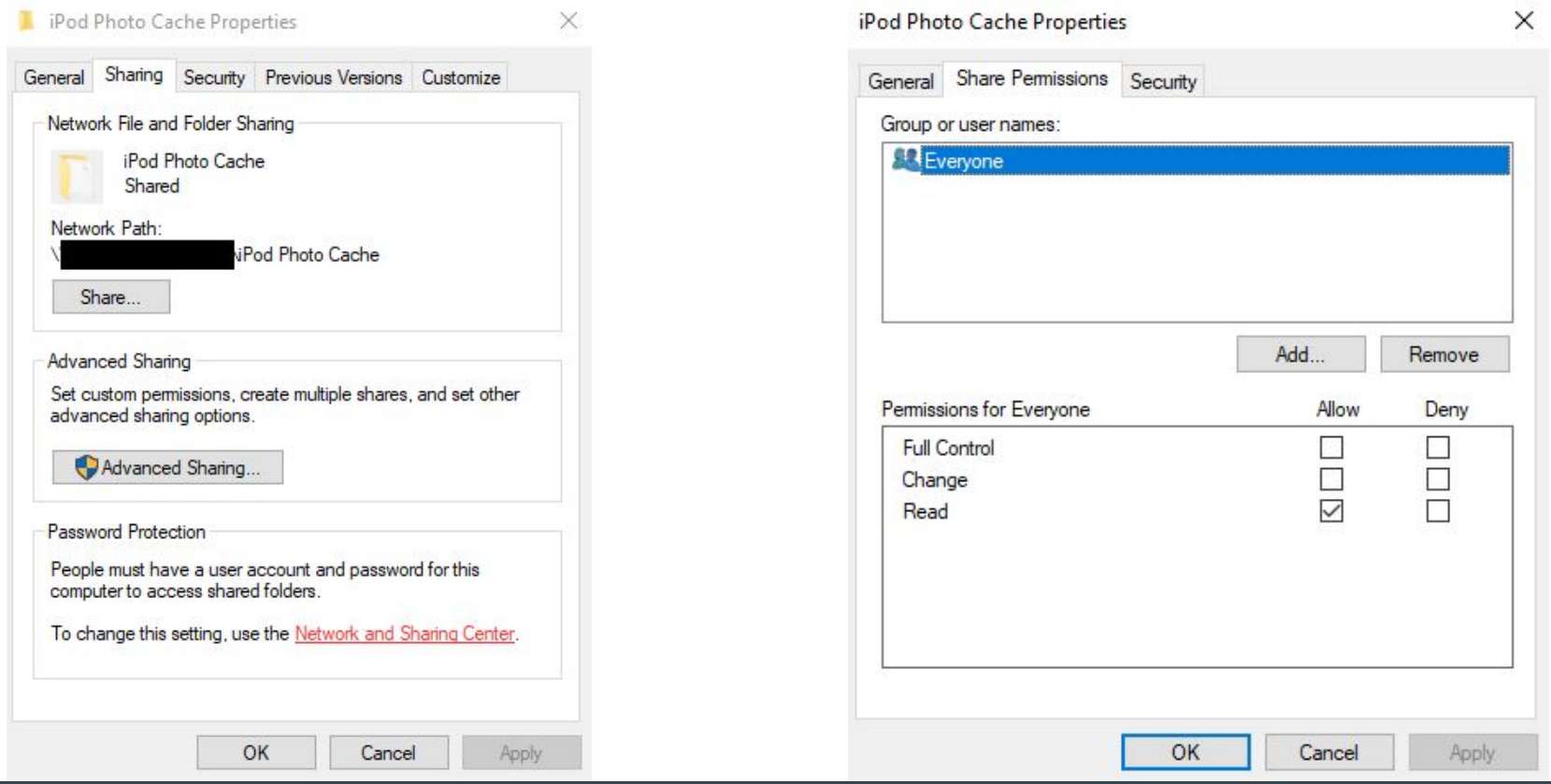
Servers

What to do?

- Share a folder
  - fsmgmt.msc
  - Or just go to the folder's properties and share it under the Share tab.

fsmgmt.msc


Shared Folders
File Action View Help
Shared Folders (Local)
Shares
Sessions
Open Files
Share Name
Folder Path
Type
ADMIN$ C:\WINDOWS Windows
C$ C:\ Windows
I$ I:\ Windows
IPC$ Windows
iPod Phot... C:\Users\Clement\... Windows
J$ J:\ Windows
print$ C:\WINDOWS\syst... Windows



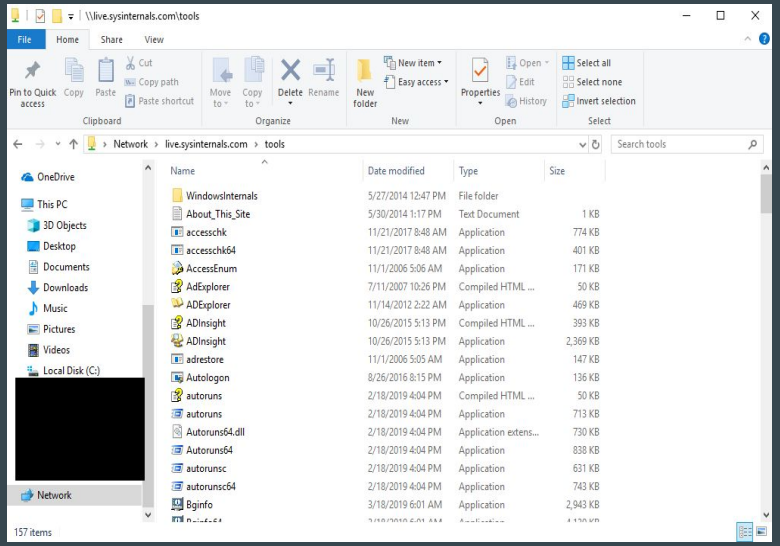
Folder's Properties

What does everyone mean?

- Permission- pertains to anyone who can get by your computer's firewall for a file share
  - If firewall is up to its max, someone from Russia cannot access your share
- Usually means users within your private network

Accessing the Share

How to access the share?



\\live.sysinternals.com\tools

1. Go to file explorer
2. Enter the UNC (Universal Naming Convention) path
   a. EX: \\CLEM-COMPUTER\iPod Photo Cache
   b. \\live.sysinternals.com\tools
      i. try this at home!
      ii. Access from Windows Explorer

Security

What should be Secured?

- Use common sense
  - 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

END

By a Troy kid

AKA Asapre