Ransomware & Least Privilege

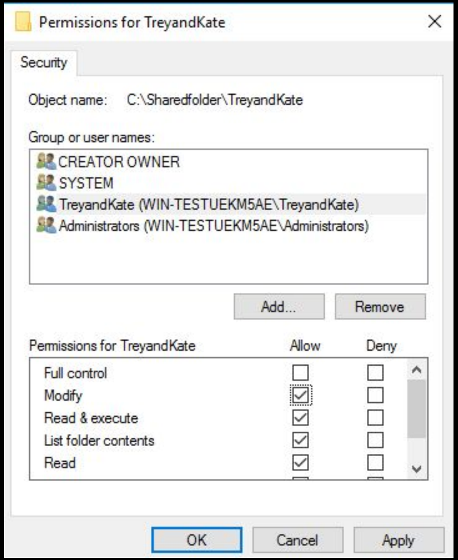
Being able to store files from a shared folder or drive from a file server is one of the most basic network functions, but it is also the most common way that a ransomware attack can **cripple** a company from the inside out.

We'll learn the simple but effective ways to enforce the principle of least privilege to limit the damage of a potential ransomware attack.

What is the principle of least privilege?

The idea of Least Privilege is to give users the lowest amount of permissions to get their job done. Not giving every user "full control" or the maximum amount of permissions one can have is something you want to avoid. Lower level employees don't need complete access to files like the system admin would need. By limiting users permissions to those only that they absolutely need it reduces the attack surface, making it harder for malware or in this case a ransomware attack to spread. People no matter who they are, are the weakest links when it comes to security, limiting users access to certain things is the best safeguard against malware or ransomware crippling the systems.

Why the PRINCIPLE of LEAST PRIVILEGE Matters
PoLP
SHRINK ATTACK SURFACE
IMPROVE operational PERFORMANCE
STOP MALWARE in its tracks
SOC2
Prepare for AUDITS
guard against HUMAN ERROR


Permissions for TreyandKate

Security

Object name: C:\Sharedfolder\TreyandKate

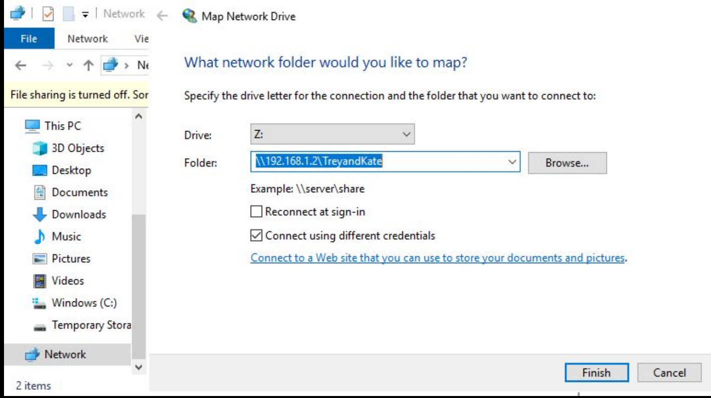
Group or user names:

- CREATOR OWNER
- SYSTEM
- TreyandKate (WIN-TESTUEKM5AE\TreyandKate)
- Administrators (WIN-TESTUEKM5AE\Administrators)

Permissions for TreyandKate	Allow	Deny
Full control	☐	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

How does file sharing work on a windows computer?

File sharing on a windows computer is a great tool to work collaboratively across a company, without having to be physically next to one another. File sharing works by creating a shared folder, that you give certain people or groups within a company access to. The shared folder is only accessible by computers that are on the same network, so people with the correct permissions can access the files as long as they are on the network. The folder will need user credentials to access, and each user will have their own permissions as what they can do within the folders. File sharing allows files to be shared in short, across a common network.



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

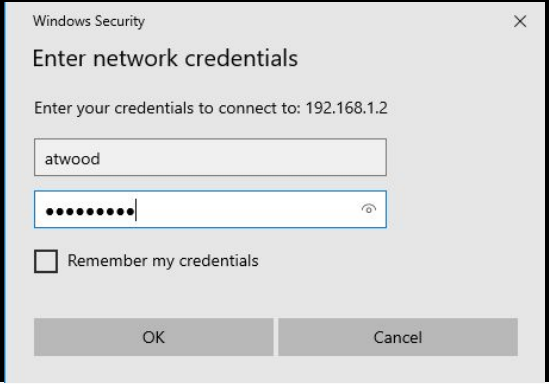
Folder: \\192.168.1.2\TreyandKate

Example: \\server\share

☐ Reconnect at sign-in

☑ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.1.2

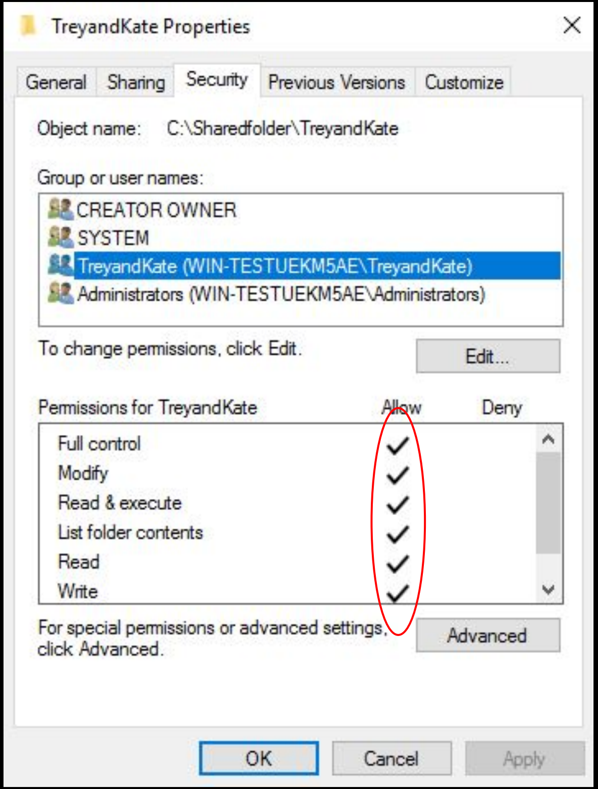
atwood

••••••••••

☐ Remember my credentials

How do the basic permissions on files and directories work?

Basic permissions on files work as follows; all users have permissions such as, read & write, edit, create, delete, or modify. These permissions work differently within a directory, for example if you're user account is only allowed to read, you can only access the files to view them and nothing else. Edit, create, and delete are simple as well, these permissions allow you to create, edit, or delete files within the directory. Giving users these permissions depending on their role within the company is vital, you can't give users too much access to things they don't need access to, it ties back with reducing the attack surface of a potential attack.



TreyandKate Properties

Object name: C:\Sharedfolder\TreyandKate

Group or user names:

- CREATOR OWNER
- SYSTEM
- TreyandKate (WIN-TESTUEKM5AE\TreyandKate)
- Administrators (WIN-TESTUEKM5AE\Administrators)

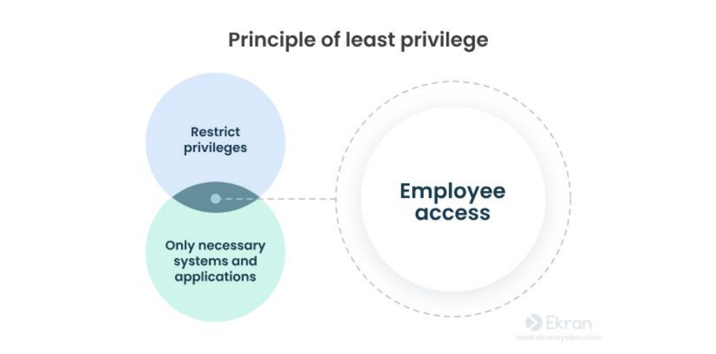
To change permissions, click Edit.

Permissions for TreyandKate	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

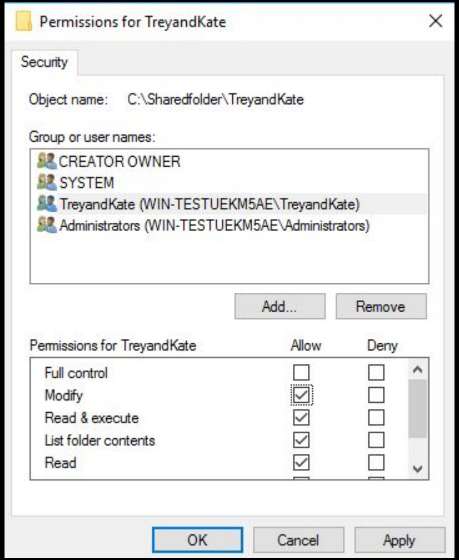
For special permissions or advanced settings, click Advanced.

How to enforce least privilege so ransomware attacks have the least impact

The enforcement of least privilege is vital. Ransomware attacks are one of the most crippling malware attacks a company can face. Limiting user permissions to important company files is vital to lower the attack surface of a ransomware attack. Limiting user permissions to those only necessary to do their job, isn't going to resolve the problem from a ransomware attack but it'll greatly reduce the impact of it. The most efficient way to enforce least privilege, is to only assign users permissions that they need to just do their job, nothing more nothing less. Users are the weakest part of a system, restricting access to important information is the best failsafe you can do to limit the impact.



Principle of least privilege



Permissions for TreyandKate

Security

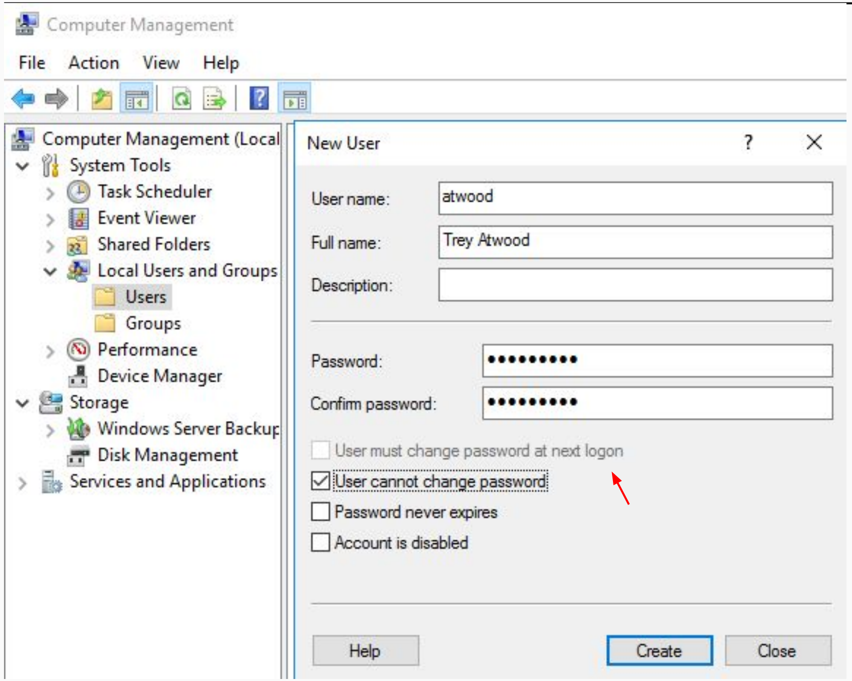
Object name: C:\Sharedfolder\TreyandKate

Group or user names:

- CREATOR OWNER
- SYSTEM
- TreyandKate (WIN-TESTUEKM5AE\TreyandKate)
- Administrators (WIN-TESTUEKM5AE\Administrators)

Permissions for TreyandKate	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

We start this exercise by creating two new users in our Windows Server, for this I used mine and my sisters names, Trey and Kate Atwood. We'll configure their privileges later, so for now their accounts are fine as is.



User name: atwood

Full name: Trey Atwood

Description:

Password: ••••••••••

Confirm password: ••••••••••

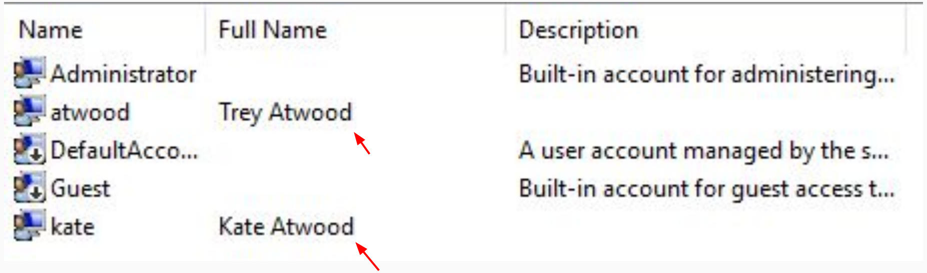
□ User must change password at next logon

☑ User cannot change password

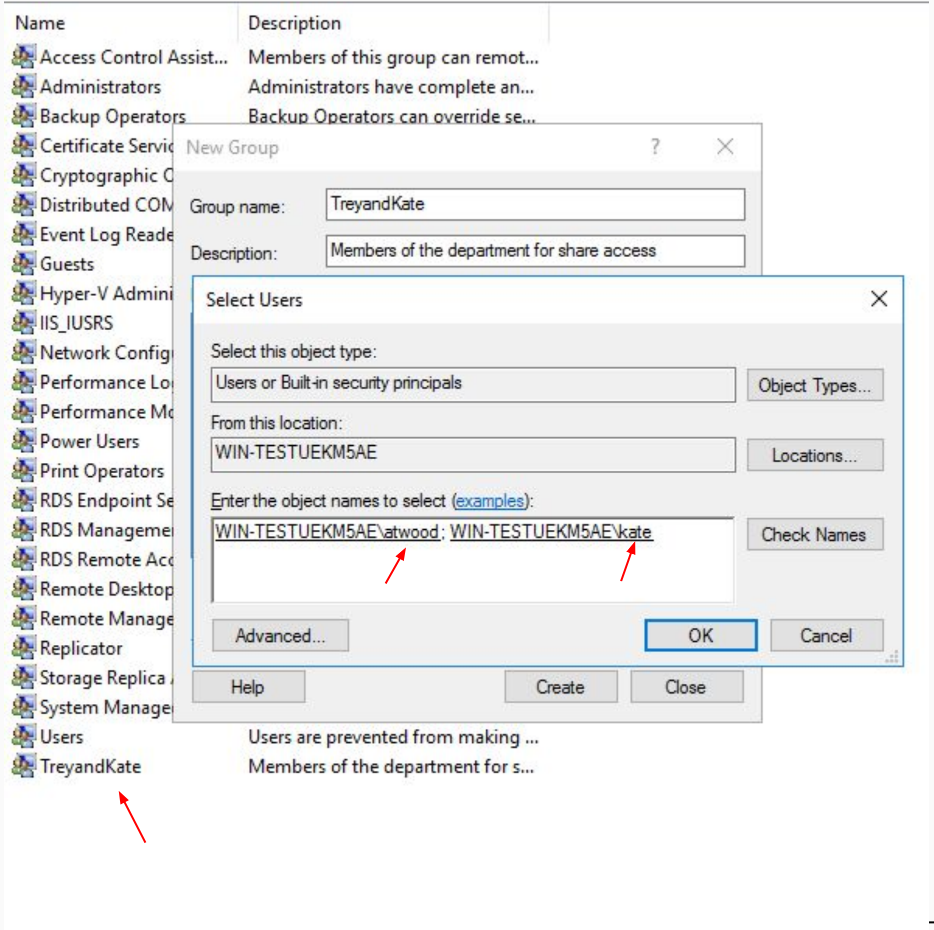
□ Password never expires

□ Account is disabled

When creating these new accounts, make sure to uncheck the box for the user to change their password for their next login.



Name	Full Name	Description
Administrator		Built-in account for administering...
atwood	Trey Atwood	
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
kate	Kate Atwood	



Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Servic	
Cryptographic C	
Distributed COM	
Event Log Reade	
Guests	
Hyper-V Admini	
IIS_IUSRS	
Network Config	
Performance Lo	
Performance Mo	
Power Users	
Print Operators	
RDS Endpoint Se	
RDS Manageme	
RDS Remote Acc	
Remote Desktop	
Remote Manage	
Replicator	
Storage Replica	
System Manage	
Users	Users are prevented from making ...
TreyandKate	Members of the department for s...

New Group

Group name: TreyandKate

Description: Members of the department for share access

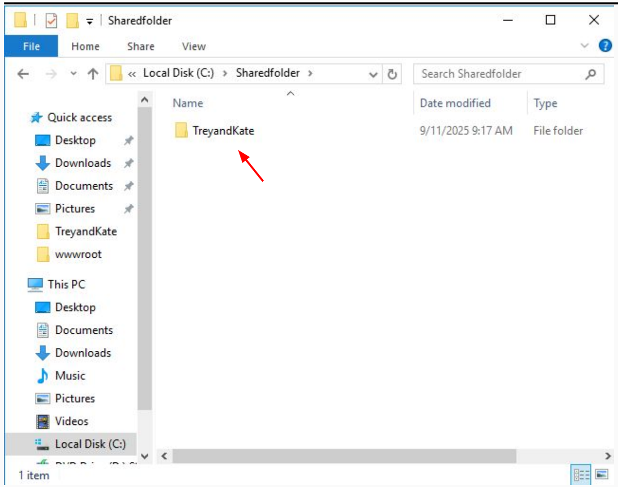
Select Users

Select this object type: Users or Built-in security principals

From this location: WIN-TESTUEKM5AE

Enter the object names to select (examples): WIN-TESTUEKM5AE\atwood; WIN-TESTUEKM5AE\kate

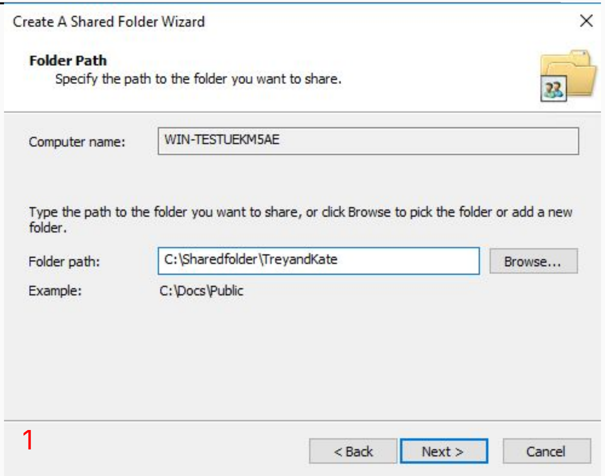
Staying in the Computer Management tool on the windows machine we now want to create a new group for our two new users we just created. To do that we right click in the blank space in the groups tab and create a new group, for this I named our group TreyandKate, added a short description and finally added the two accounts to the group.



Name	Date modified	Type
TreyandKate	9/11/2025 9:17 AM	File folder

For the next step we need to create a shared folder, so our windows machine can have files shared to and from it from our azure machine.

To do this we create a new folder on our windows machine, I keep the name the same; TreyandKate


Create A Shared Folder Wizard

Folder Path

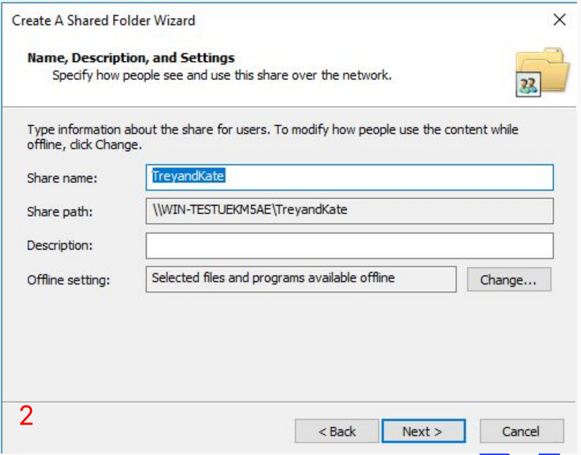
Specify the path to the folder you want to share.

Computer name: WIN-TESTUEKM5AE

Type the path to the folder you want to share, or click Browse to pick the folder or add a new folder.

Folder path: C:\Sharedfolder\TreyandKate

Example: C:\Docs\Public


Create A Shared Folder Wizard

Name, Description, and Settings

Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use the content while offline, click Change.

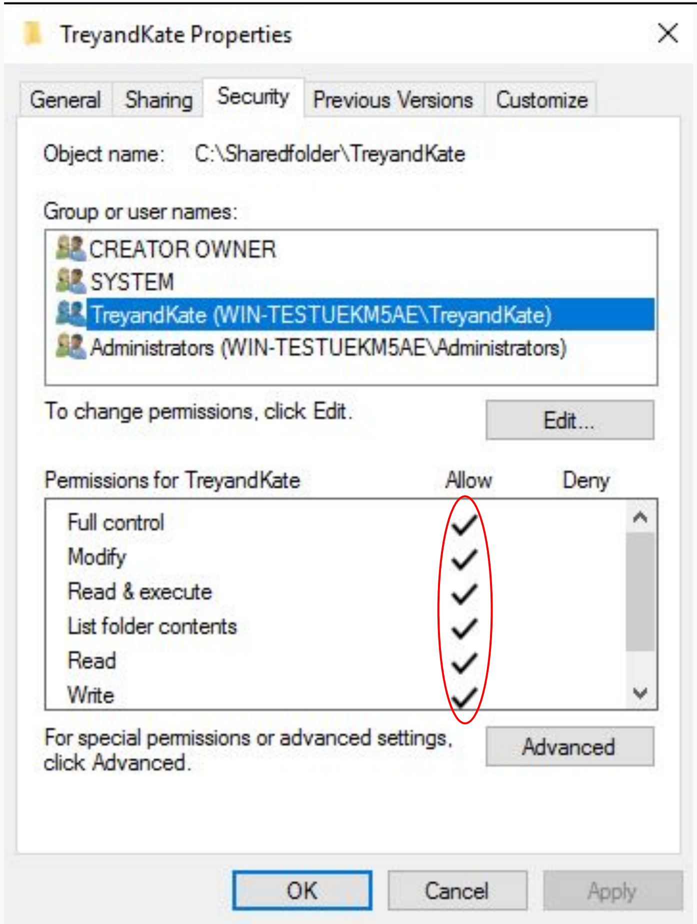
Share name: TreyandKate

Share path: \\WIN-TESTUEKM5AE\TreyandKate

Description:

Offline setting: Selected files and programs available offline

After creating our new folder in the file explorer of our windows machine, we need to go back to the Computer Management, and navigate to the Shared Folders tab, and follow the instructions on the wizard to the right (1 and 2) to create a new shared folder.



TreyandKate Properties

Object name: C:\Sharedfolder\TreyandKate

Group or user names:

- CREATOR OWNER
- SYSTEM
- TreyandKate (WIN-TESTUEKM5AE\TreyandKate)
- Administrators (WIN-TESTUEKM5AE\Administrators)

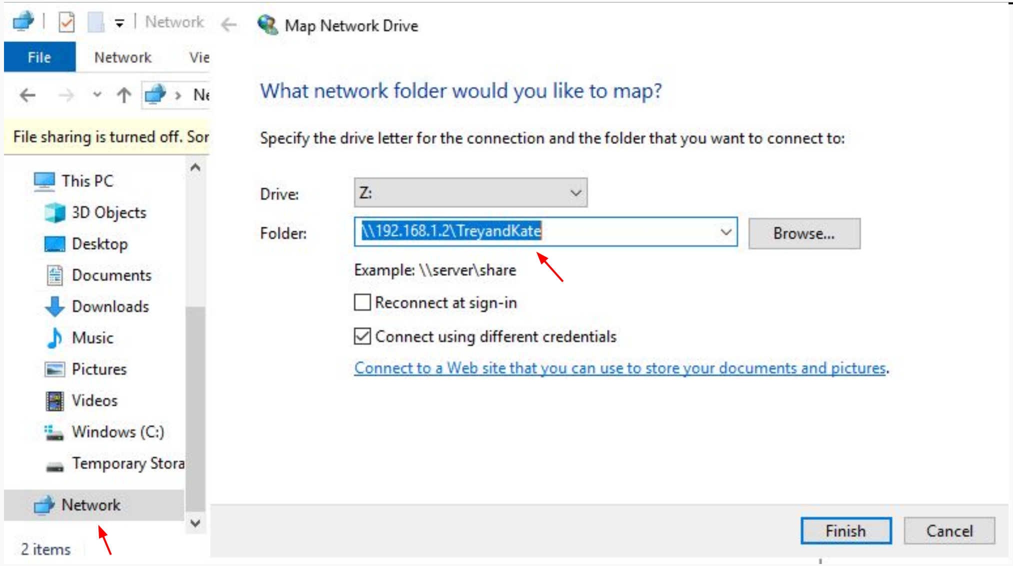
To change permissions, click Edit.

Permissions for TreyandKate	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

In the properties for the shared folder “TreyandKate”, I have allowed users in the group “TreyandKate” to have full control over the folder, allowing them to create new files, edit and delete anything within this folder.

Giving users the ability to fully control a file is the highest level of permissions the users can receive. You’re able to pick and choose what to give users within a group, for example instead of giving my user Kate full access to the folder I could just give her “read” permissions, which will allow her to access the folder, but only let her view the files that are in it already. Limiting her from creating / deleting or editing files that are already in the folder



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.2\TreyandKate

Browse...

Example: \\server\share

□ Reconnect at sign-in

☑ Connect using different credentials

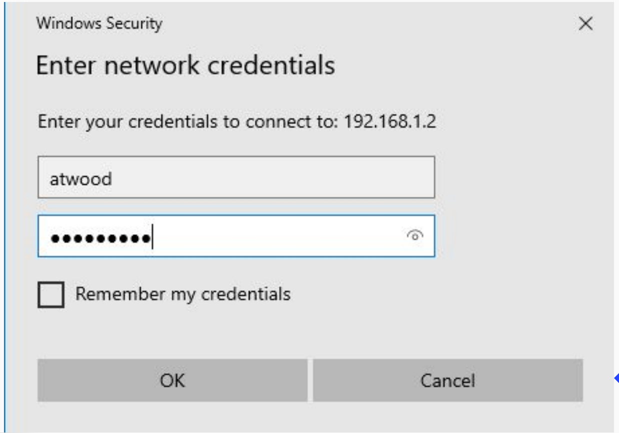
Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

We now want to check to make sure that the shared file we just created is accessible with both accounts.

In order to do this we want to go to our Azure Machine, and go to file explorer, right click on the network tab in the bottom left and enter: \\192.168.1.2\TreyandKate.

Once we enter that this window will popup asking for a username to access the folder, I'll login first with my Trey account, then with Kate's account next.



Windows Security

Enter network credentials

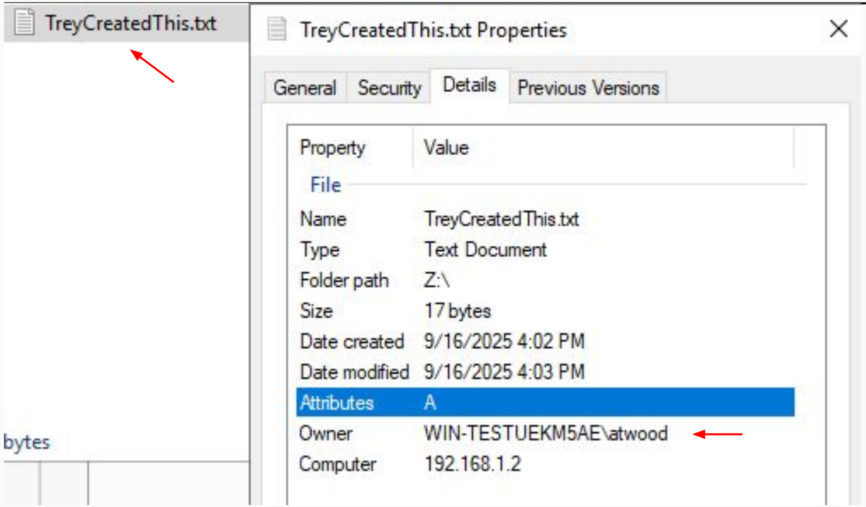
Enter your credentials to connect to: 192.168.1.2

atwood

●●●●●●●●●

□ Remember my credentials

OK Cancel



TreyCreatedThis.txt Properties

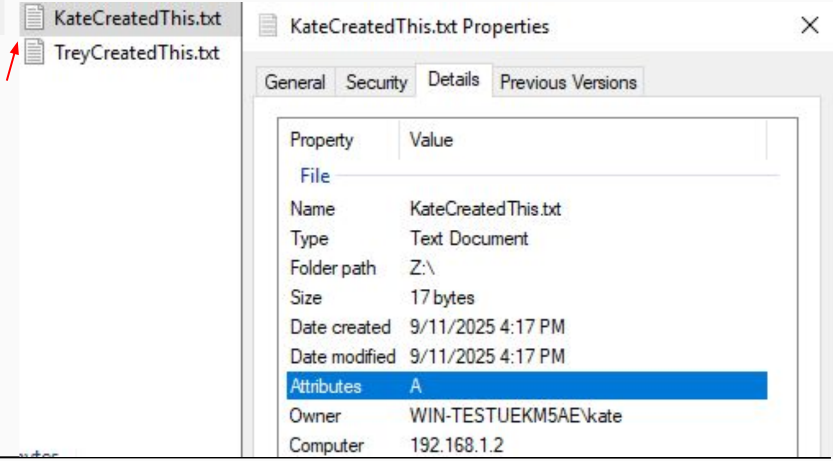
Property	Value
File	
Name	TreyCreatedThis.txt
Type	Text Document
Folder path	Z:\
Size	17 bytes
Date created	9/16/2025 4:02 PM
Date modified	9/16/2025 4:03 PM
Attributes	A
Owner	WIN-TESTUEKM5AE\atwood
Computer	192.168.1.2

Inside the shared folder on Trey's account, I created a .txt file tagged with my name. In the properties window you can see that the owner of the file is \atwood which is Trey's account name.

Now I'll repeat the steps on the last slide but for Kate's account this time and do the same thing.

Here's the folder again but this time I'm on Kate's account, as you can see the file I made on Trey's account "TreyCreatedThis.txt" is showing in the folder.

I created a new .txt file on Kate's account and you can see the owner of this file is \kate.



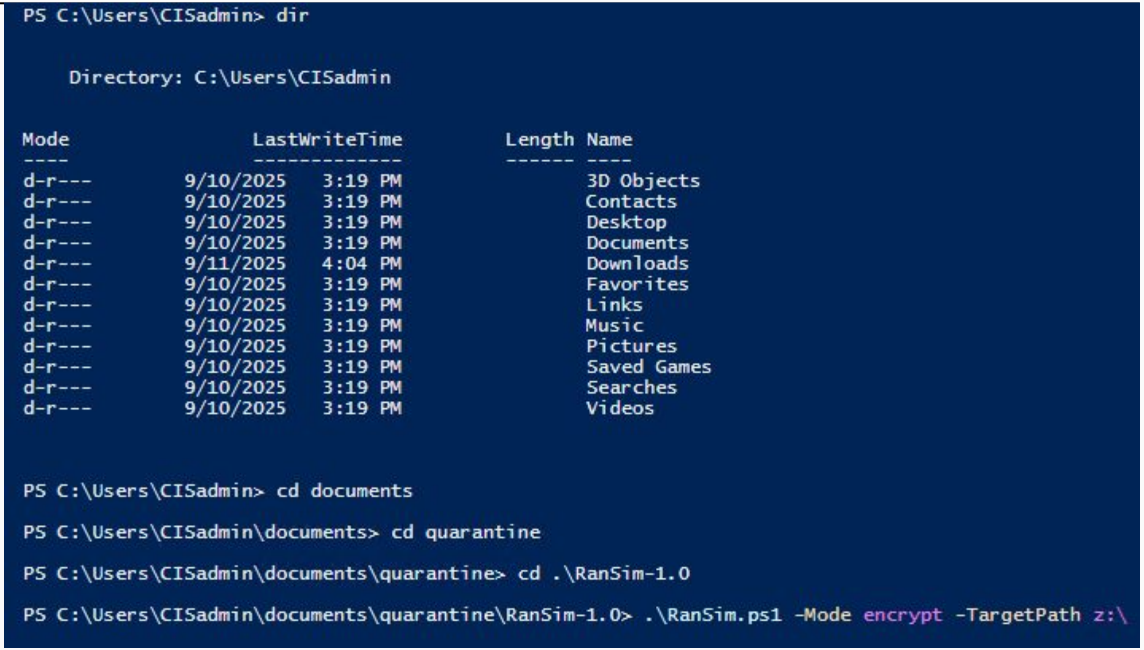
KateCreatedThis.txt Properties

Property	Value
File	
Name	KateCreatedThis.txt
Type	Text Document
Folder path	Z:\
Size	17 bytes
Date created	9/11/2025 4:17 PM
Date modified	9/11/2025 4:17 PM
Attributes	A
Owner	WIN-TESTUEKM5AE\kate
Computer	192.168.1.2

Now that we have everything setup and permissions are given to all the users, I’m going to simulate a Ransomware attack on the shared folder.

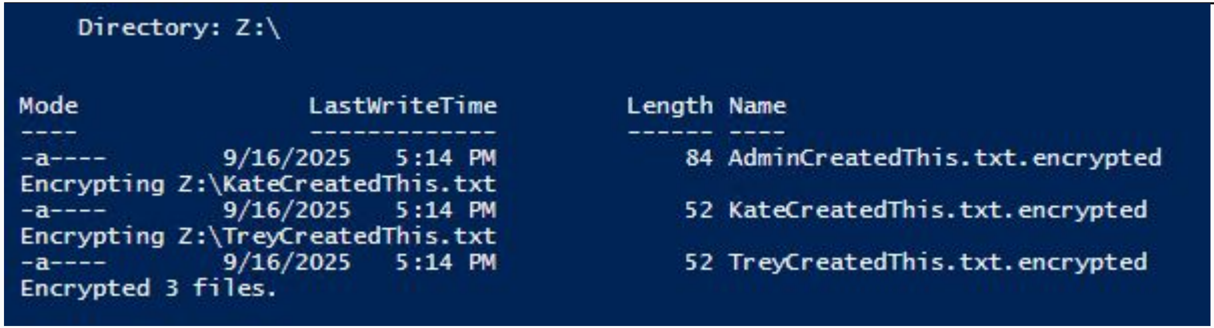
Using a program called RanSim, I’m going to simulate what It would look like if a hacker had gotten access to one of the users accounts, and deployed a ransomware on the system.

To do this I’m going to use Powershell on the Azure Machine.



```
PS C:\Users\CISadmin> dir


    Directory: C:\Users\CISadmin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/10/2025   3:19 PM                3D Objects
d-r---         9/10/2025   3:19 PM                Contacts
d-r---         9/10/2025   3:19 PM                Desktop
d-r---         9/10/2025   3:19 PM                Documents
d-r---         9/11/2025   4:04 PM                Downloads
d-r---         9/10/2025   3:19 PM                Favorites
d-r---         9/10/2025   3:19 PM                Links
d-r---         9/10/2025   3:19 PM                Music
d-r---         9/10/2025   3:19 PM                Pictures
d-r---         9/10/2025   3:19 PM                Saved Games
d-r---         9/10/2025   3:19 PM                Searches
d-r---         9/10/2025   3:19 PM                Videos


PS C:\Users\CISadmin> cd documents

PS C:\Users\CISadmin\documents> cd quarantine

PS C:\Users\CISadmin\documents\quarantine> cd .\RanSim-1.0

PS C:\Users\CISadmin\documents\quarantine\RanSim-1.0> .\RanSim.ps1 -Mode encrypt -TargetPath z:\
```

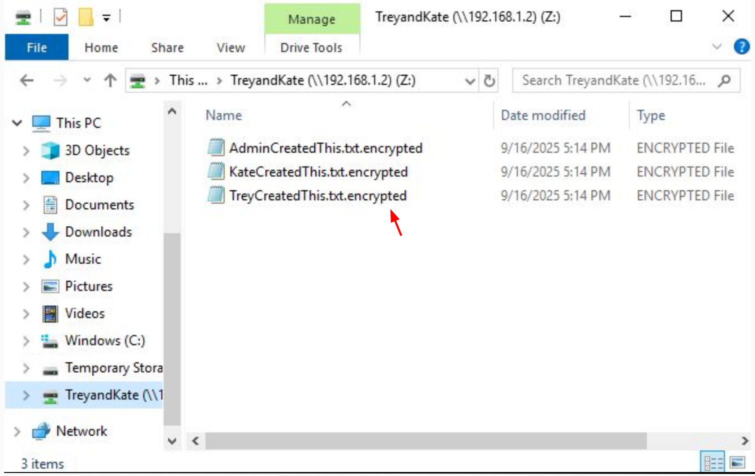
In Powershell we navigate to the RanSim-1.0 folder, and execute the command “.\RanSim.ps1 -Mode encrypt -TargetPath z:\”. This command will encrypt every file we have in the “z:\” folder which is our shared folder.



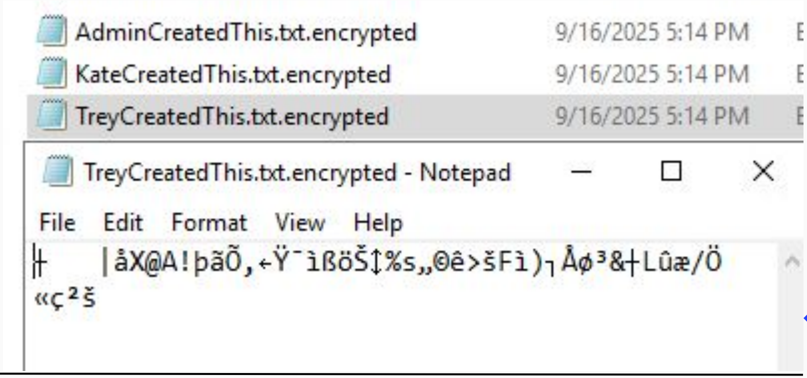
```
    Directory: Z:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/16/2025   5:14 PM             84 AdminCreatedThis.txt.encrypted
Encrypting Z:\KateCreatedThis.txt
-a----         9/16/2025   5:14 PM             52 KateCreatedThis.txt.encrypted
Encrypting Z:\TreyCreatedThis.txt
-a----         9/16/2025   5:14 PM             52 TreyCreatedThis.txt.encrypted
Encrypted 3 files.
```

After we execute that last command we see this, the three files that were inside our shared folder are now tagged with .encrypted instead of .txt.

This is what it looks like to us in the file explorer. We no longer have .txt files that are plaintext, instead we have encrypted files that when you open them are not longer readable, and we have no idea what it means anymore



Name	Date modified	Type
AdminCreatedThis.txt.encrypted	9/16/2025 5:14 PM	ENCRYPTED File
KateCreatedThis.txt.encrypted	9/16/2025 5:14 PM	ENCRYPTED File
TreyCreatedThis.txt.encrypted	9/16/2025 5:14 PM	ENCRYPTED File



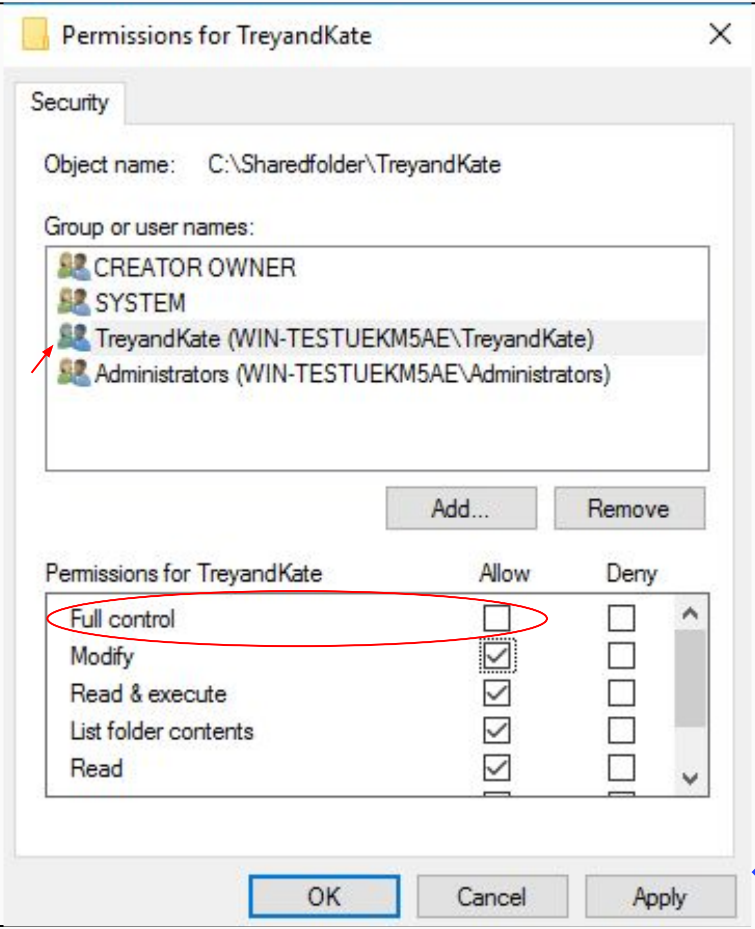
AdminCreatedThis.txt.encrypted	9/16/2025 5:14 PM	E
KateCreatedThis.txt.encrypted	9/16/2025 5:14 PM	E
TreyCreatedThis.txt.encrypted	9/16/2025 5:14 PM	E

```
╫    |åX@A!þãÕ,←Ÿ¯ìßöŠ↨%s„0ê>šFì)┐Åø³&┼Lûæ/Ö
«ç²š
```

Now that we were just hit with a ransomware attack, we need to revisit our permissions that were given to the group that was hit with the attack.

Looking over the current permissions that the group has in the shared folder, I'm going to disable the groups access to have "full control" over the folder and instead give them just "modify" permissions. With the group having "full control" the users within the group can read, write, modify, and **take ownership** of the files or folders. They're able to change the files / folders permissions, and adjust other groups permissions within the shared folder. Disabling their "full control" permissions and replacing it with just the "modify" permission allows them to still access, read, write, modify, and delete files in the folder but limits them to not be able to change the permissions or ownership of the files in the folder.

Now even if we were hit with another ransomware attack, they would still gain access to create, edit, or delete files, but they won't be able to take over our shared folder completely and delete it or do whatever they want with our information.



Object name: C:\Sharedfolder\TreyandKate

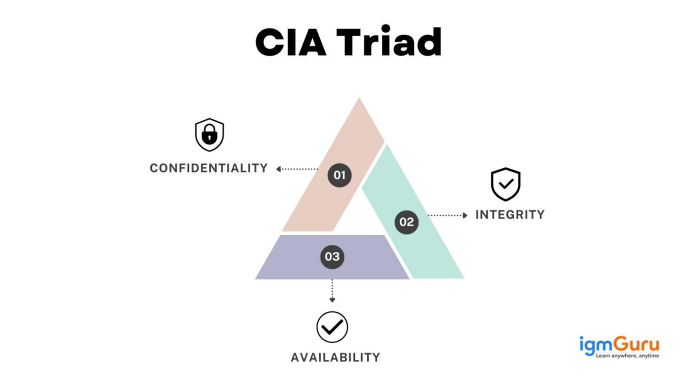
Group or user names:

- CREATOR OWNER
- SYSTEM
- TreyandKate (WIN-TESTUEKM5AE\TreyandKate)
- Administrators (WIN-TESTUEKM5AE\Administrators)

Permissions for TreyandKate	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

Keeping the idea of the users necessity to still get their job done, there are falloffs that we are just going to have to accept. Having to toggle each users permissions when they need to edit or access something in the shared folder is tedious and in the real world isn't probable.

Having to accept the fact that there are going to have vulnerabilities is part of it, the CIA Triad is something that you have to keep in mind all the time, Confidentiality, Integrity, and Availability are things that have to be measured together and prioritize based on how you want your systems set up.



In a real world scenario when a company is setting up these folders and permissions to their employees, there are things that are going to have to be accepted as a vulnerability.

In a ransomware attack the easiest fix is having everything on a folder that is backed up. This folder could be within the same folder that was compromised by the attack, but by changing permissions of the users you can allow them only permissions to read the files. No matter who the user is, an administrator of the system, a manager, or a new employee with the base permissions, none of them have any permissions to change the files in the backup folder. Since they all have read only permissions, the ransomware can't encrypt the files since the account they used to get into the system doesn't have access to the files in the first place.

Finding an equal median of Confidentiality, Integrity, and Availability is one of the hardest tasks to do when creating a new system from the ground up, whether it be constricted by the budget, or certain guidelines to follow, finding a balance between everything is super challenging. But the idea of **Least Privilege** is to only give users what they absolutely need access to, nothing more or nothing less. This prevents a situation where a ransomware attack will be crippling to a company, allowing the hacker to change permissions, ownership of the files and to delete everything since they are the new owner of the folders. Small things like the idea of least privilege are important fixes to large problems.