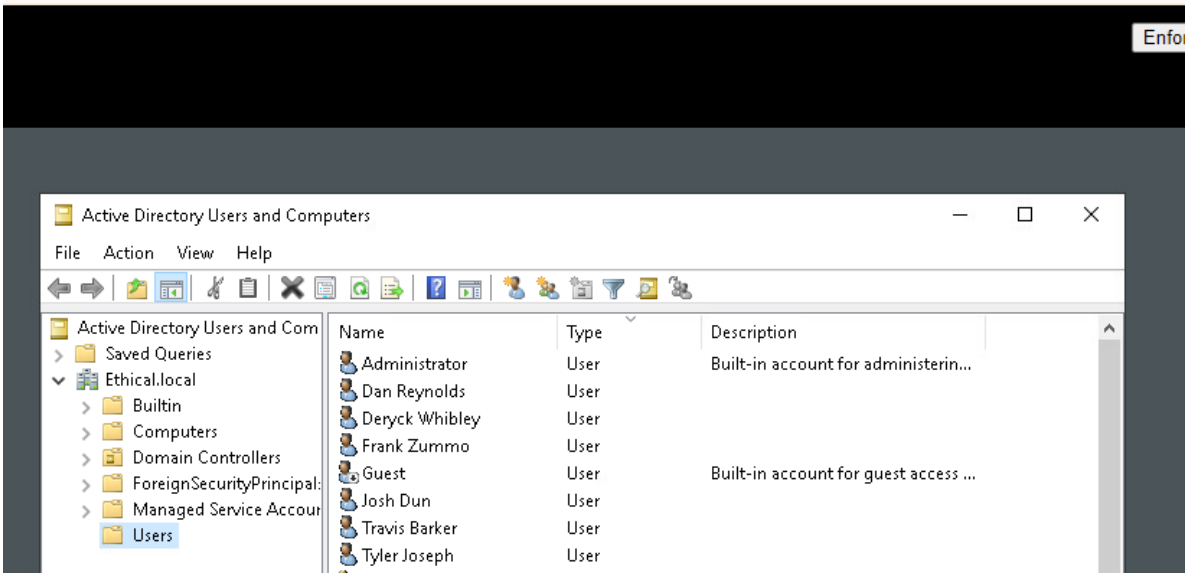
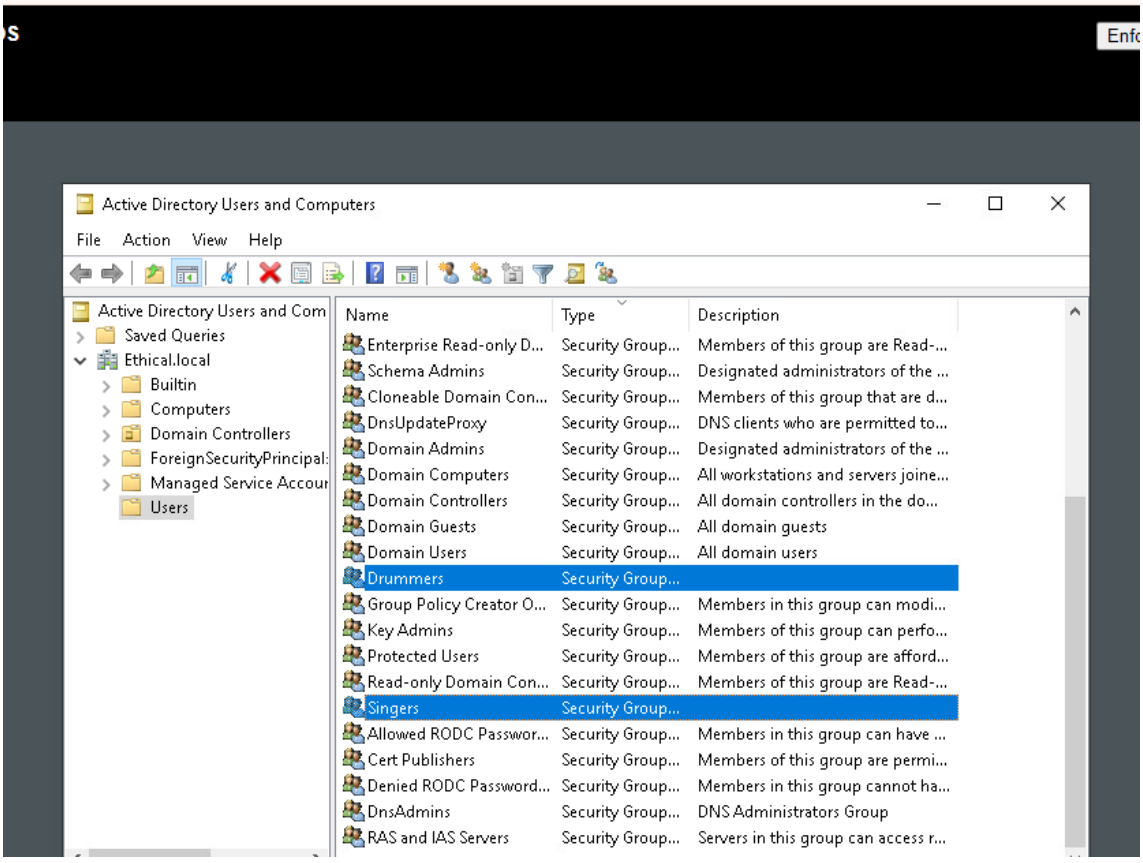
For my implementation I implemented CIS Control 06 which is Access Control Management. I used Windows Active Directory (AD) to create users and put those users into groups. Putting users into groups allows me to display the use of Role Based Access Control which is an important part of access control management. Using AD functions also allows centralized management which is another important aspect. There is only one device or virtual machine (VM) being used for this implementation so there is no inventory to create of devices and all the users and groups can be seen on AD already.

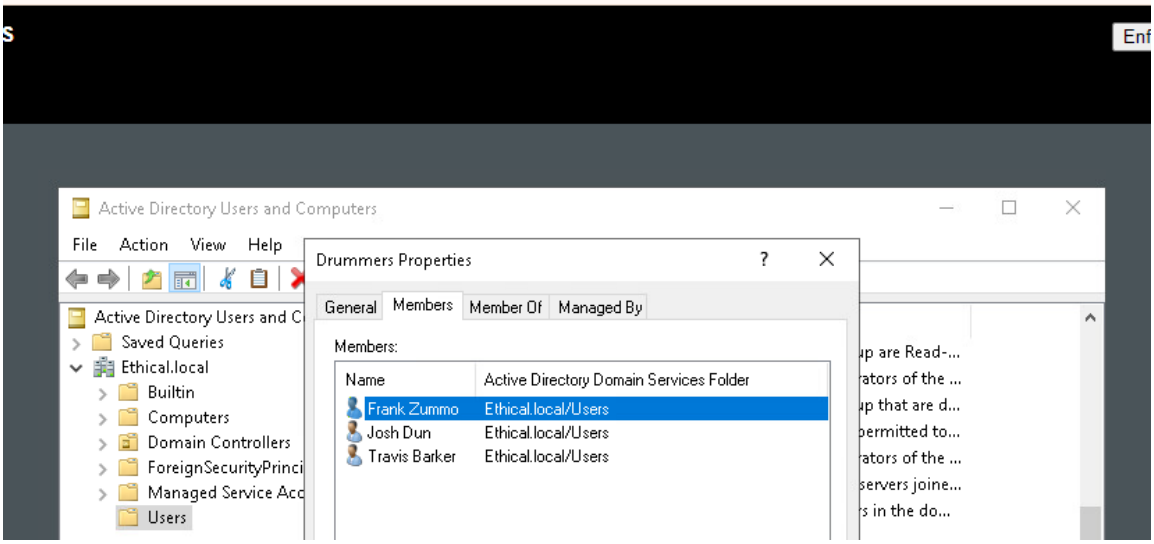
Using AD allows for an easy way to grant and remove access to users as needed. If a new user needs to be created an account can be created for them and they can be assigned to the group based off who they are, and this group will control what the user can and cannot access. When that user leaves their account can quickly be disabled to remove their access from the systems and prevent them from being able to access the account. Disabling an account allows for its resources to be saved and files the account created can still be accessed as needed while the user can no longer user their account.

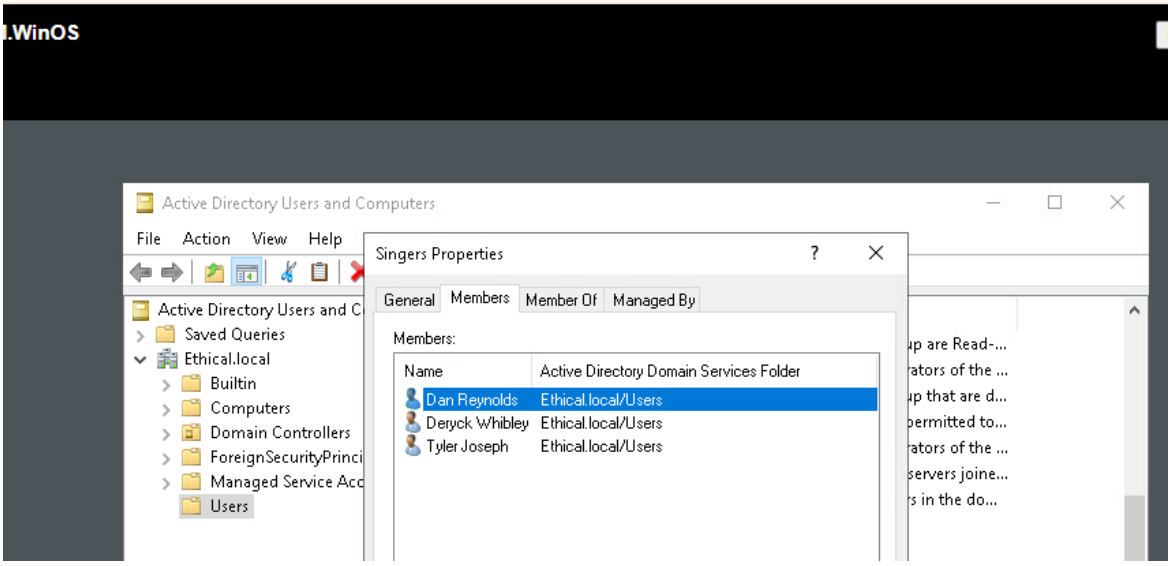
For the implementation of this control the VM that was created has no internet access. This limits the ability to implement MFA which is another very important aspect of access control management.

In my implementation I have created multiple users. The users are the names of members of bands. Some users are singers and some users are drummers and they have been added to a Singers or Drummers group based off what they are. This will allow the singers and drummers to have access to separate resources and files on the systems.

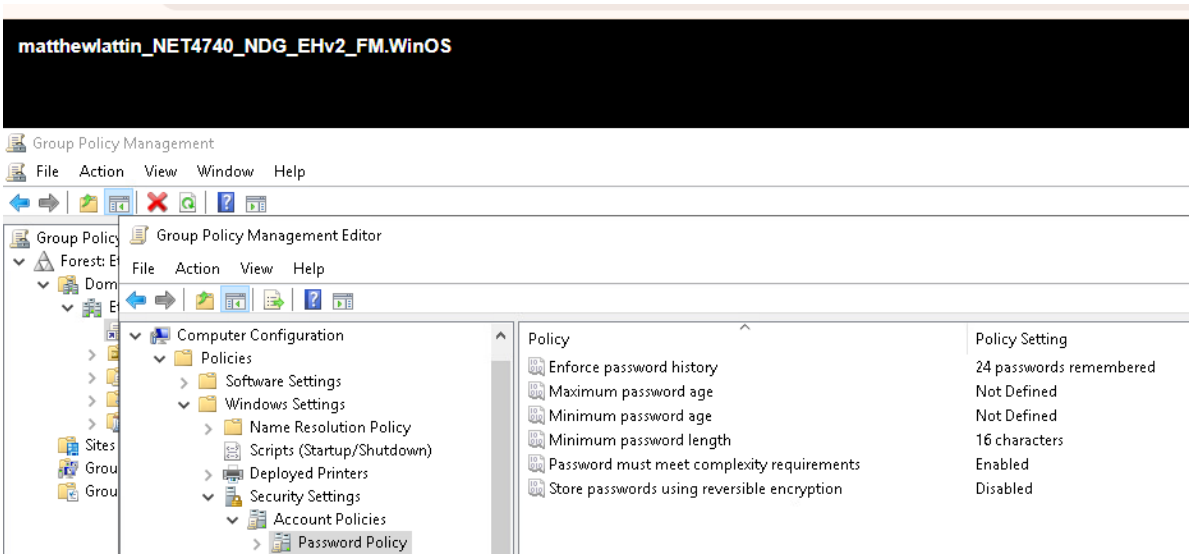

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
Ethical.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name Type Description
Administrator User Built-in account for administerin...
Dan Reynolds User
Deryck Whibley User
Frank Zummo User
Guest User Built-in account for guest access ...
Josh Dun User
Travis Barker User
Tyler Joseph User

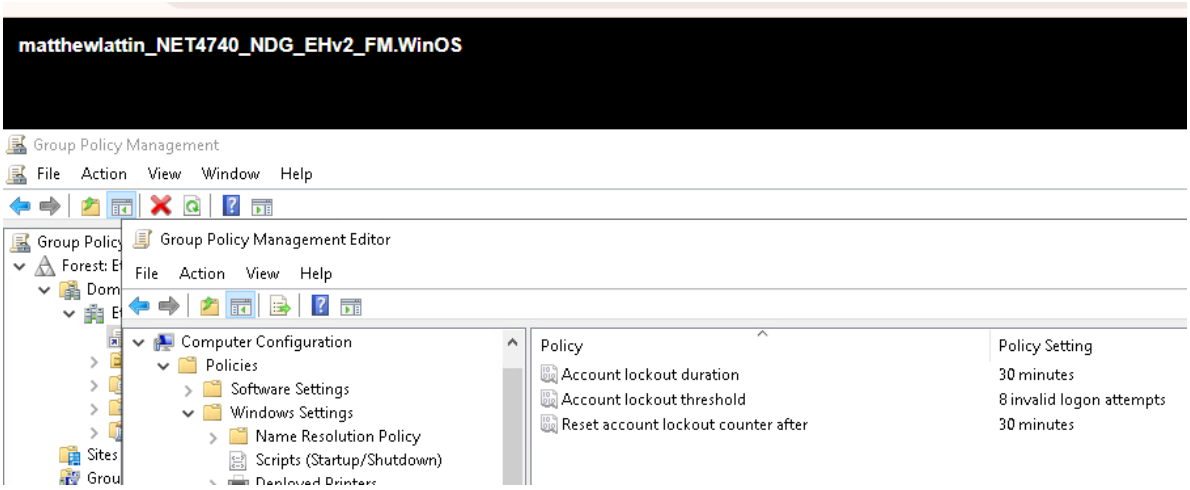

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
Ethical.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name Type Description
Enterprise Read-only D... Security Group... Members of this group are Read-...
Schema Admins Security Group... Designated administrators of the ...
Cloneable Domain Con... Security Group... Members of this group that are d...
DnsUpdateProxy Security Group... DNS clients who are permitted to...
Domain Admins Security Group... Designated administrators of the ...
Domain Computers Security Group... All workstations and servers joine...
Domain Controllers Security Group... All domain controllers in the do...
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Drummers Security Group...
Group Policy Creator O... Security Group... Members in this group can modi...
Key Admins Security Group... Members of this group can perfo...
Protected Users Security Group... Members of this group are afford...
Read-only Domain Con... Security Group... Members of this group are Read-...
Singers Security Group...
Allowed RODC Passwor... Security Group... Members in this group can have ...
Cert Publishers Security Group... Members of this group are permi...
Denied RODC Password... Security Group... Members in this group cannot ha...
DnsAdmins Security Group... DNS Administrators Group
RAS and IAS Servers Security Group... Servers in this group can access r...



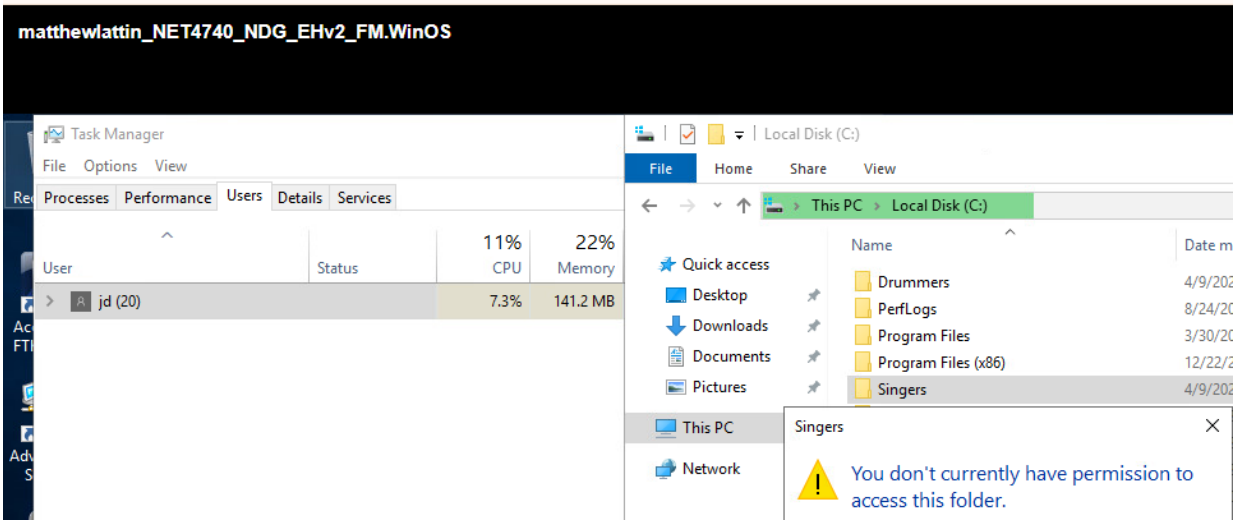


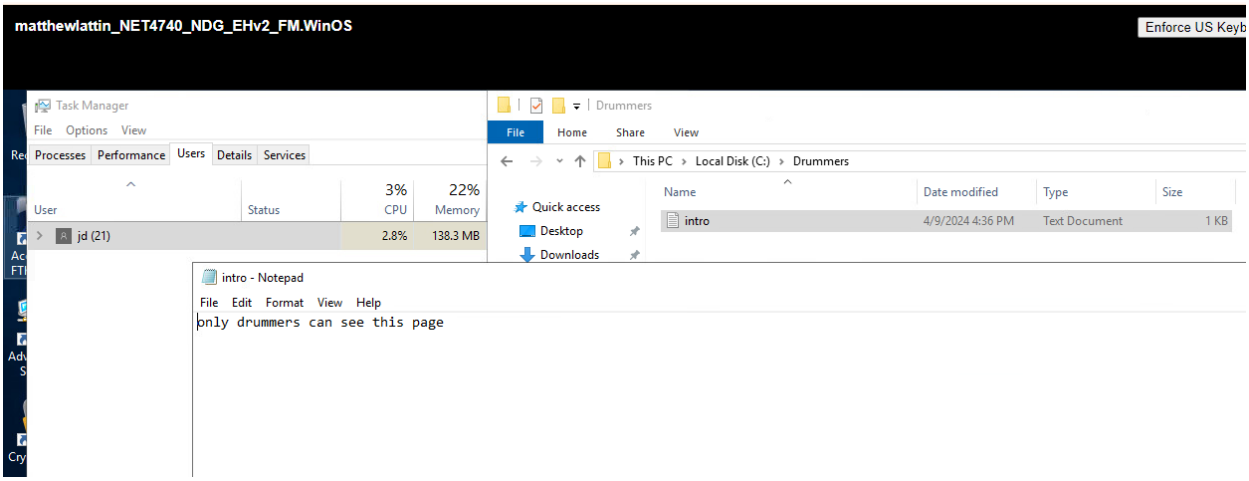
The pictures above show the users and groups that were created. They also show the members of the groups that have been added so far. A strong password policy has also been created. This will make logins more secure and limiting the number of attempts before locking an account will make brute forcing a password less likely to happen.



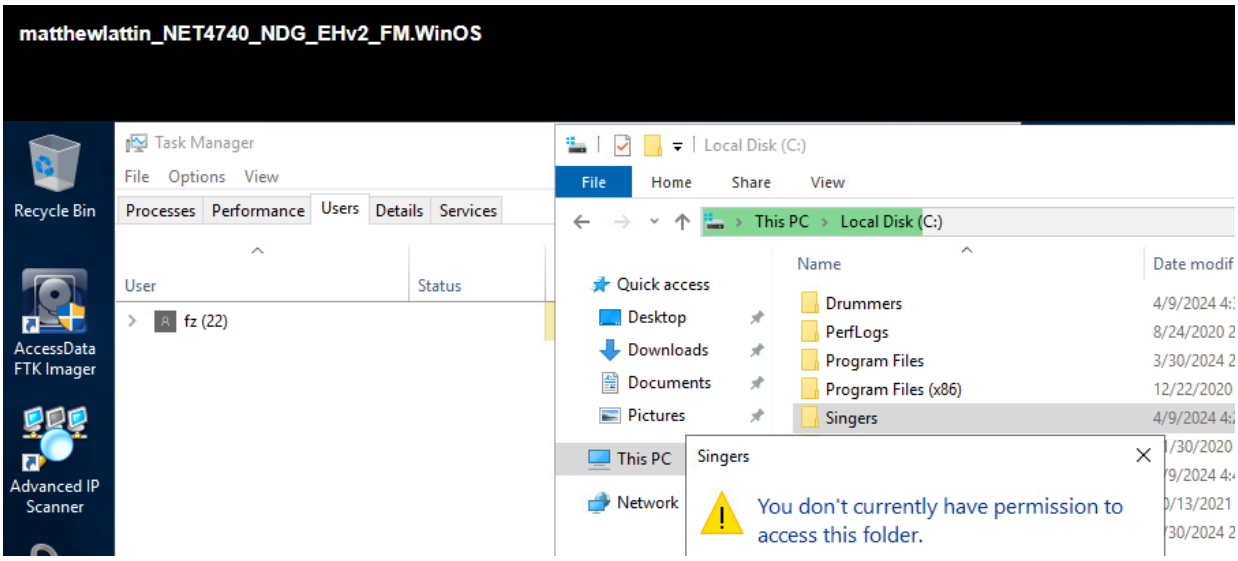


For file sharing I have set it up so there is a file for drummers and a file for singers and we can see that a drummer doesn't have access to the singer's folder. JD is a drummer account and is the account used to test this access.

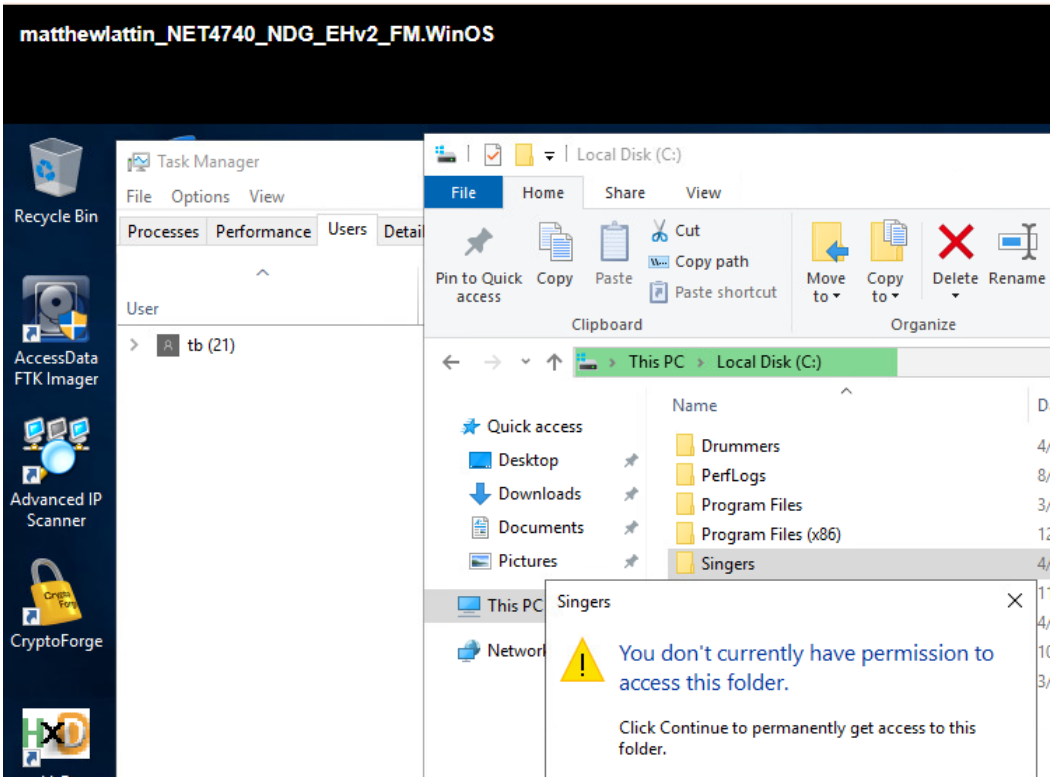




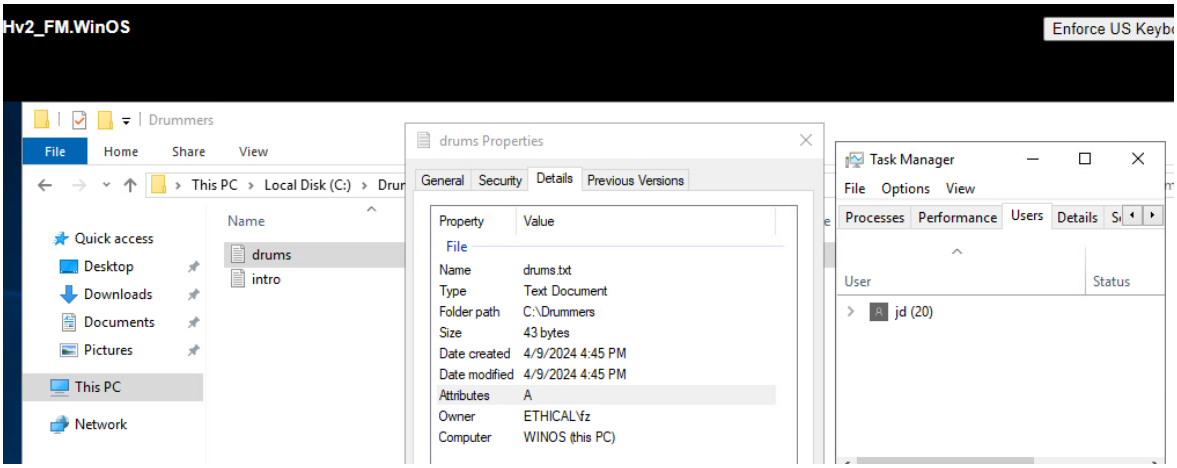
Testing another drummer, fz, shows that the singer folder still cannot be accessed by a drummer.



Testing the drummer account tb we can see that singers also cannot be accessed showing that access control was granted properly based on the Drummers group which means role based access control is successful for the drummers group.

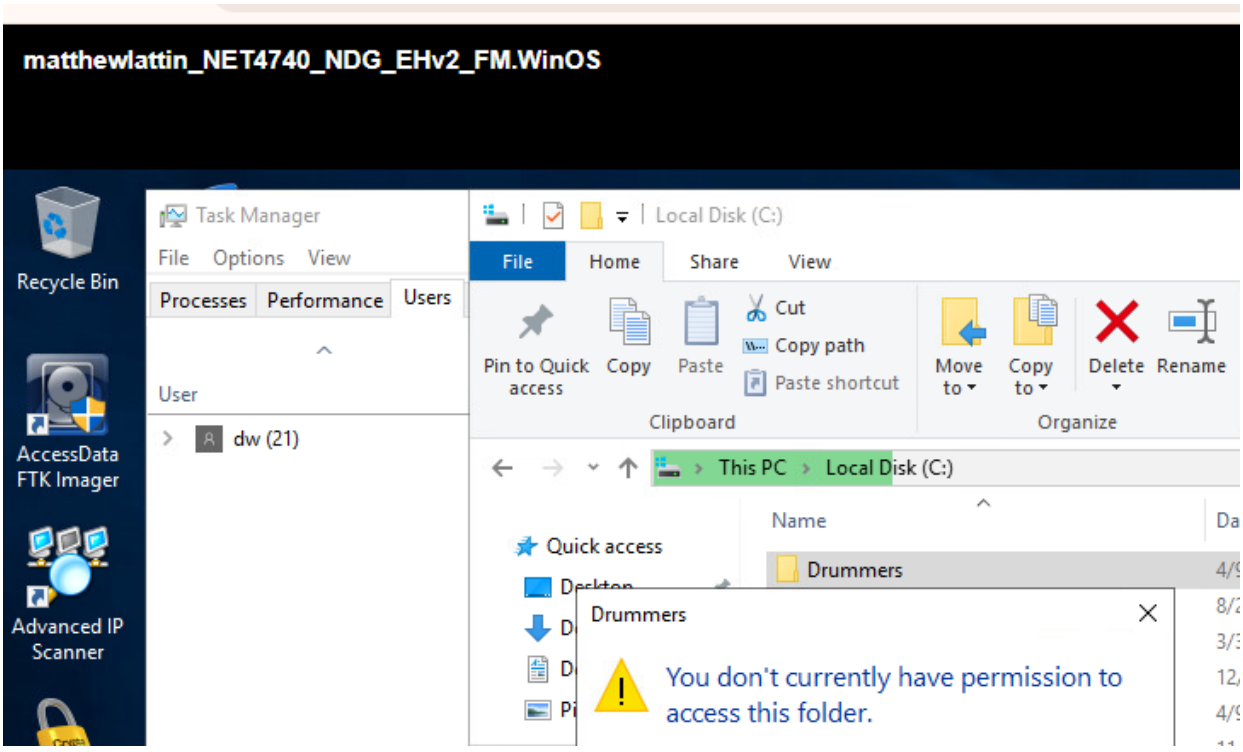


Logging back in as jd we can see that a file created by fz is visible to jd.

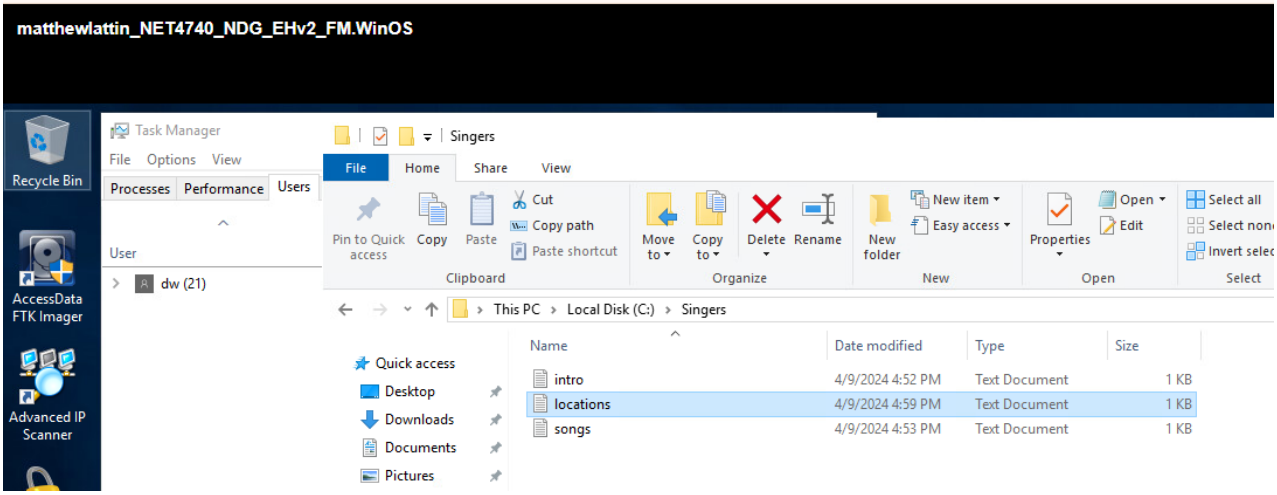


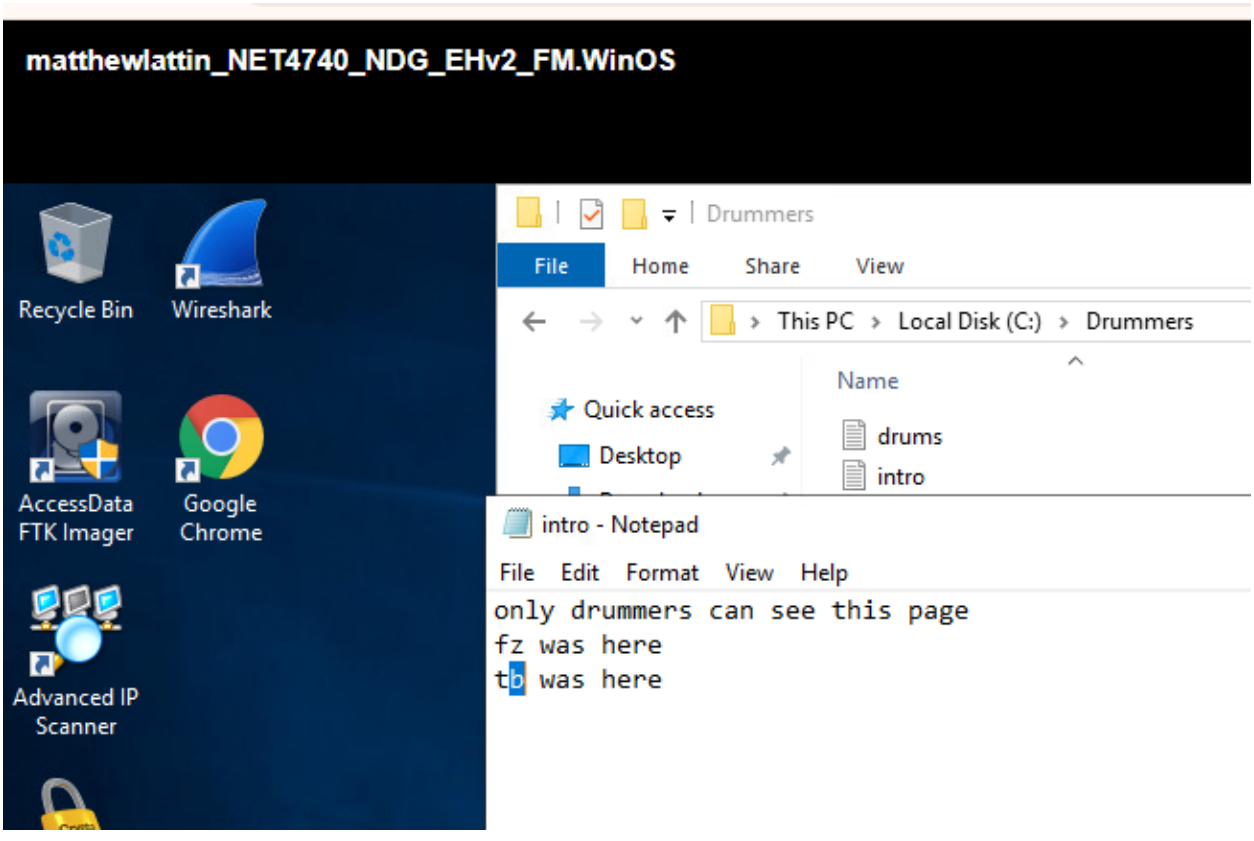
The file intro was created by jd and edited by the other drummers accounts and we can see those changes when logged back in as jd.

Testing dw, a singer we can see that access to Drummers is denied.

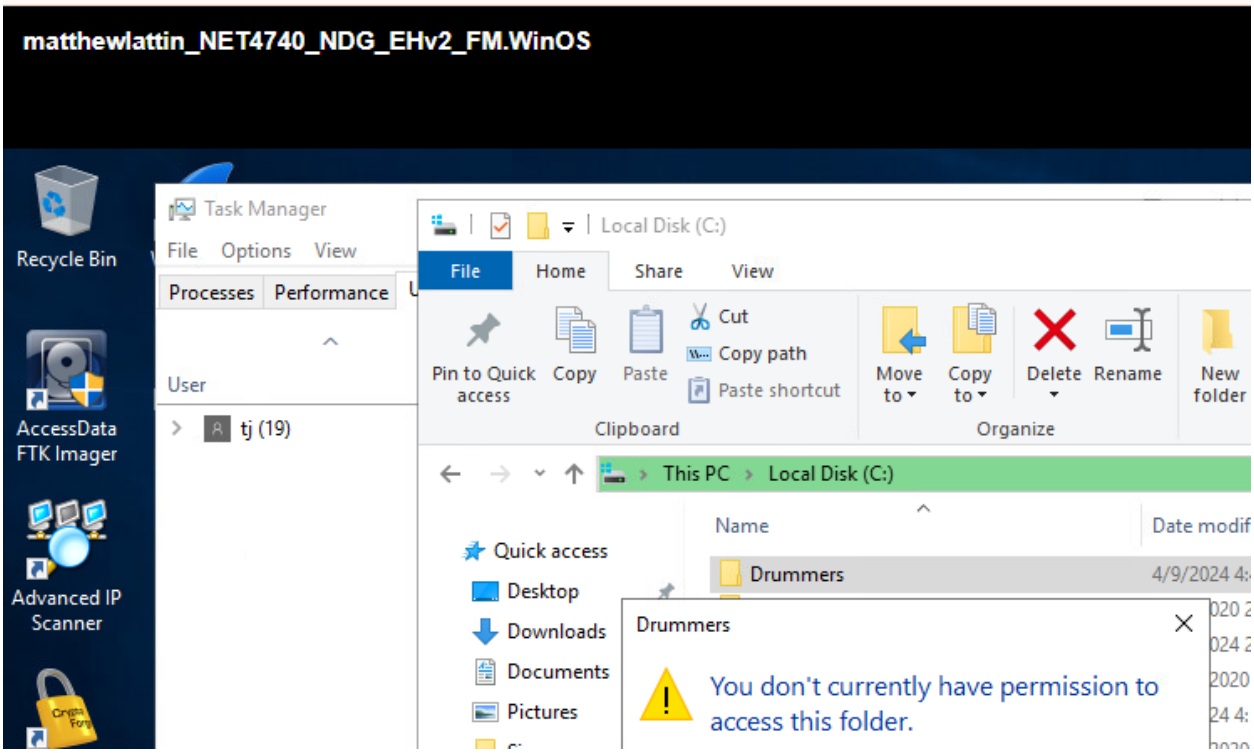


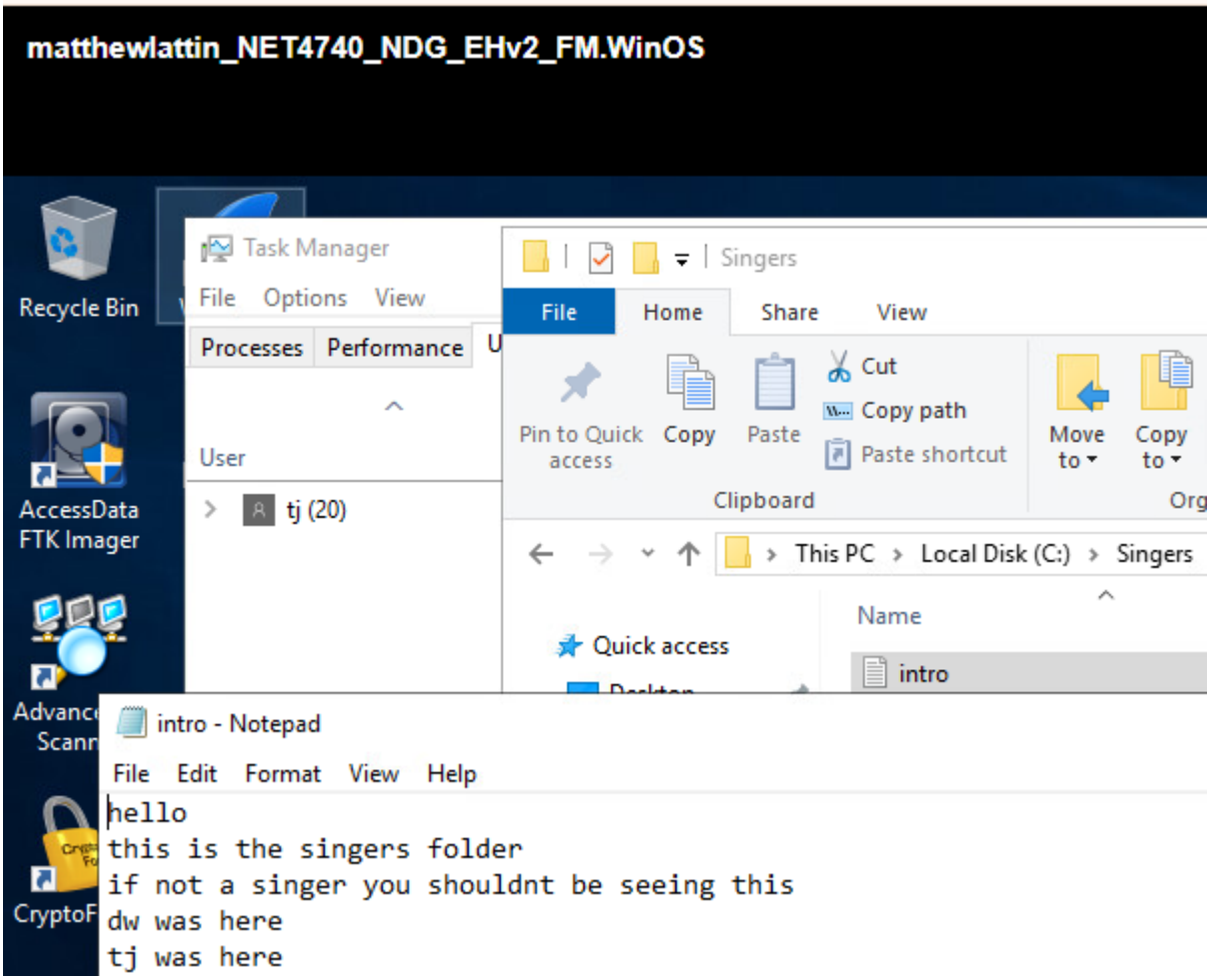
Singers can be accessed by dw which is what is supposed to happen.



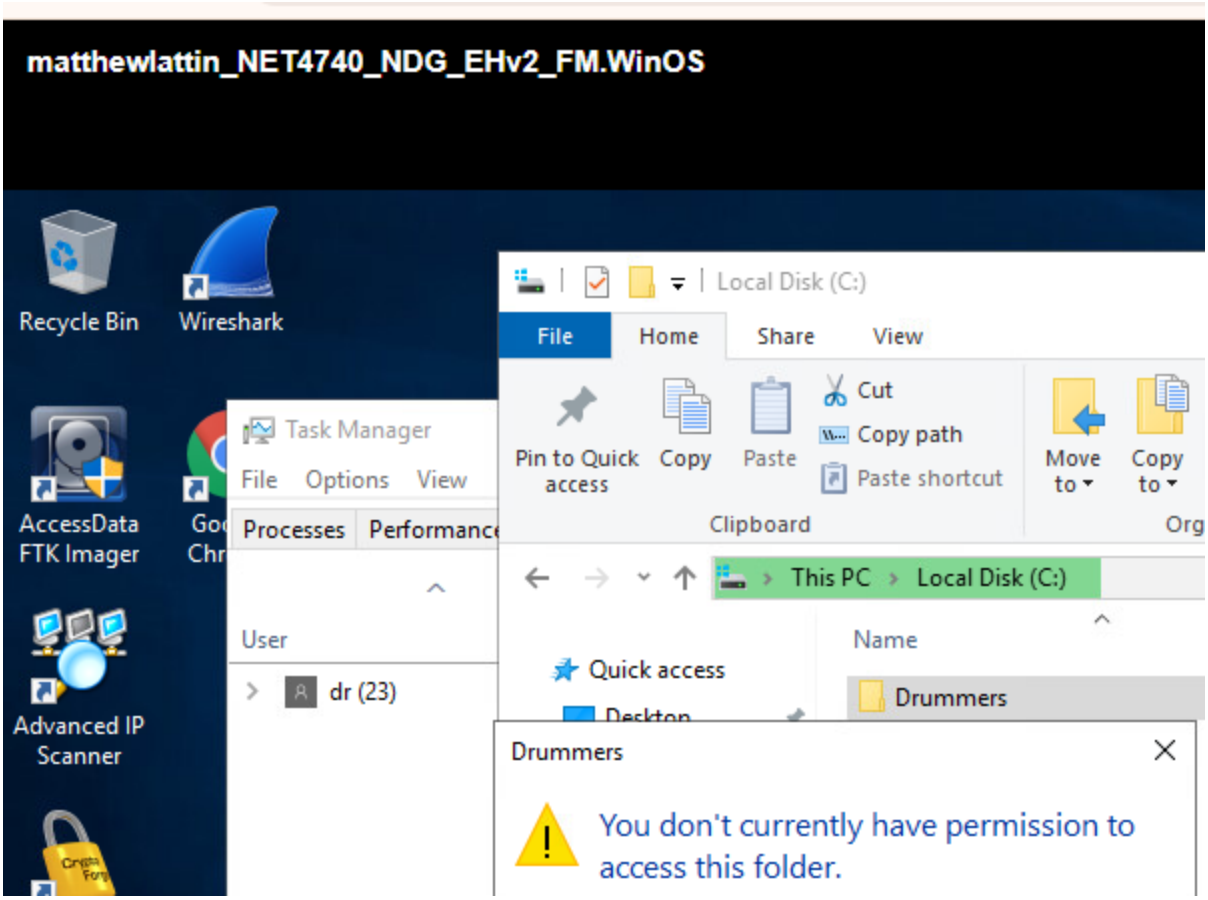


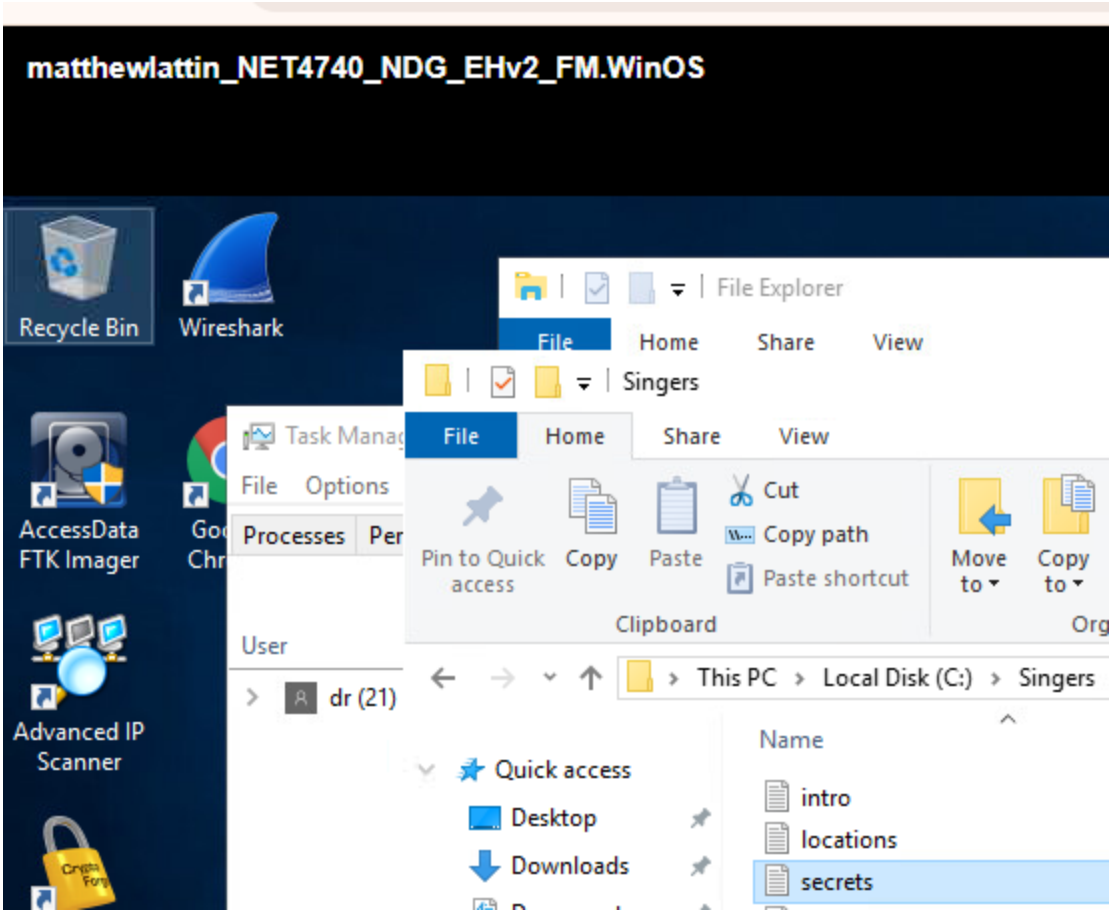
Testing tj, another singer, we can see the same results come for what folders can be accessed.


matthewlattin_NET4740_NDG_EHv2_FM.WinOS
Recycle Bin
AccessData FTK Imager
Advanced IP Scanner
Task Manager
File Options View
Processes Performance
User
tj (19)
Local Disk (C:)
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
New folder
Organize
This PC › Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date modif
Drummers
4/9/2024 4:
Drummers
You don't currently have permission to access this folder.

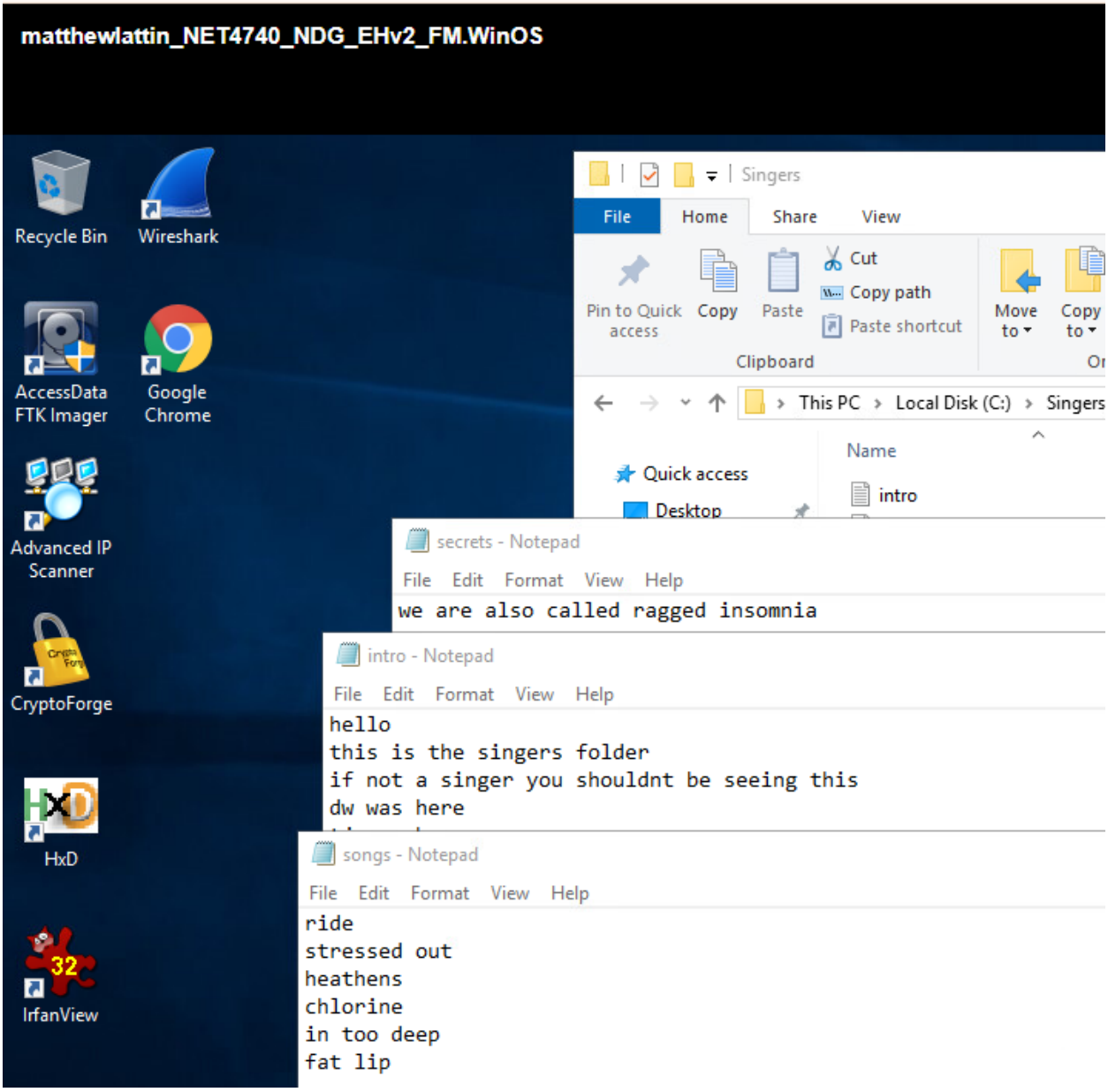


Testing the final singer, dr, we get the same results where we can access only the singers folder and can add changes to files and add files to the folder that will be accessible to other members of the singers group.


matthewlattin_NET4740_NDG_EHv2_FM.WinOS
Recycle Bin
Wireshark
AccessData FTK Imager
Advanced IP Scanner
Task Manager
File Options View
Processes Performance
User
dr (23)
Local Disk (C:)
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
This PC › Local Disk (C:)
Quick access
Name
Drummers
Drummers
You don't currently have permission to access this folder.



Testing the tj account one more time shows all the changes can be viewed. The tj account created the folder and shared it to the singers group, this shows that role based access control was successfully implemented with the singers and that role based access control allows for sharing of folders and files among users in a group.



Role based access control was implemented centrally using AD which is another important aspect of access control management. The only thing that wasn't able to be accomplished was MFA and this is because of the lack of internet connection limiting testing abilities of MFA and limiting ability to test remote desktop connections which is one location where MFA should be used. Ways that MFA could be implemented for logging into accounts would include using an app like DUO, using smartcards, or using metrics. These methods would cover the other aspects

of authentication outside of something you know which is a username and password combination. Biometrics would be something you are and a smartcard would be something you have and these would be effective ways of implementing MFA which I was not able to accomplish.