**MCSE 1 Lecture 8**

**Sharing Resources**

**Share permissions vs NTFS Security permissions**

Each file and folder has two levels of permissions that control what operations a user can perform on files and folders. The two levels of permissions are **share permissions** and **NTFS permissions (security permissions).**

Every shareable resource, folder, files, printers, etc, has a **DACL (Discretionary Access Control List)** associated with it. The DACL contains two important pieces of information:

1. **ACEs (Access Control Entry)** – identifies who has access to the

resource

2. **Permissions** – lists what level of permission each ACE has

Figure 1 shows the share DACL and the NTFS DACL for a folder called **Accounting**.

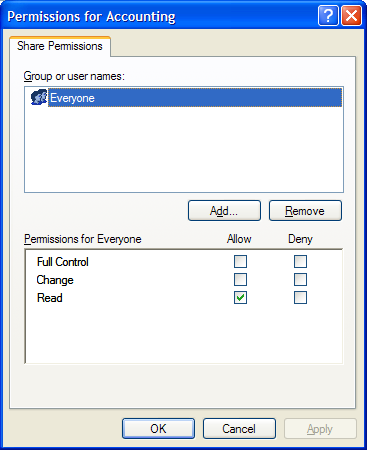
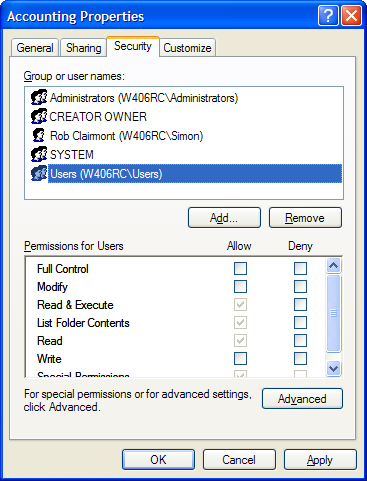


Fig. 1 Share DACL (left) and NTFS DACL (right) for the Accounting folder

**Why does each resource have two levels of permissions?**

If a user logs in locally, only the NTFS permissions apply. The Share permissions have no effect.

If a user tries to access a shared folder from another computer, both the share permissions and NTFS security permissions apply. You must assign the permissions at both levels so the user can perform whatever task he is meant to perform without granting him extra permissions. If a user has more permissions than he needs, he may be able to perform tasks that can cause problems with the data or applications on the network. He may accidently delete an application.

So what permissions are in effect if a user accesses a shared folder from another computer? You must combine the shared permissions with the NTFS permissions. The most restrictive permissions are the ones that are in effect.

For instance, if a user has CHANGE permission at the SHARED level but only Read & Execute permission at the NTFS level, the user’s effective permissions will be Read & Execute.

As another example, if a user has READ permission at the shared level and Modify permission at the NTFS level, the user will have an effective permission of Read & Execute.

When a user accesses a shared folder on 1 computer while logged into another computer, NTFS permissions are combined with Share permissions to create the user’s effective permissions. Table 1 shows what Share and NTFS permissions a user needs to perform basic tasks on files and folders.

|  |  |  |
| --- | --- | --- |
| **Share**  **Permissions** | **NTFS**  **Permissions** | **File Operation you wish to perform** |
| READ | READ | view the contents of a file |
| copy a file |
| READ & EXECUTE | run a program |
| CHANGE | WRITE | save changes to a document |
| MODIFY | rename a file / folder |
| create a file / folder |
| delete a file / folder |
| FULL | FULL | Take ownership |
| Assign permissions to other users |

Table 1 Effect of combining Share and NTFS permissions

In summary:

NTFS permissions always apply, whether the user accesses the resource locally while logged into the computer the resource is on, or remotely by logging into computer-A and accessing a resource on Computer-B through the network.

Share permissions only apply when a user accesses resources by logging into computer-A and accessing a resource on Computer-B through the network.

**SHARE permissions**

**Read**  – allows the user to open, run, and copy a file or folder

**Change**  – same as READ but also allows the user to delete, rename and

create files and folders in the SHARED folder.

**Full Control –** same as CHANGE but also allows the user to take ownership,

change the DACL list, and delete files regardless of file

permissions

**NTFS permissions**

**List Folder Contents –** allows user to see what’s in the folder

(this permission does not appear for files)

**Read** - allows the user to open and copy the files or folder

**Read & Execute** – allows the user to do everything Read allows plus the user

can run programs.

**Write**  - allows user to make changes to documents; and save the changes.

**Modify** – allows the user to do anything with the files and folders. This includes,

Read, Write, Read & Execute, plus the user can delete, rename and

create documents and folders.

**Full Control** – same as Modify, but in addition, allows the user to take ownership

and assign permissions in the DACL.

Figure 1 shows the default permissions when you create and share a folder.

You should rarely leave the default permissions in place. To tighten up security, remove the default group **Everyone** on the share permissions. Then assign new permissions that meet the level of access you want to grant the users.

**Groups**

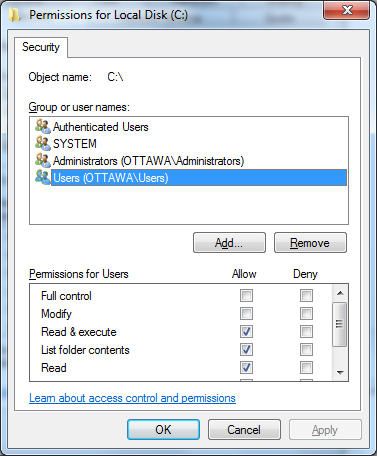
Whenever possible, create groups and add user accounts to the groups. Quite often a group of users that perform the same tasks will require the same level of access to a handful of folders.

If there are 20 architects who all need the same level of access to 10 different folders, it is more efficient to add the 20 users to a group called architects and then add the architects group to the DACLs of the 10 folders. This is much quicker than adding 20 individual accounts each time to 10 folders. Using groups, we have 10 assignments and without groups we would have 200 assignments to make!

Another advantage is, Mike who is an architect joins the engineering department. It is easy to remove his user account from the architects group and add it to the engineers group. Mike would instantly be denied access to the resources that the architects have and immediately gain all the permissions to folders that the engineers have.

**Special built-in groups**

Figure 2 shows the DACL for drive C:. The groups that show up as ACEs in the DACL were placed there when the operating system was installed. Therefore, these are the default groups who have access to the hard drive.



**Authenticated Users**

This group contains all users who login with the exception of the **Guest** account.

**Everyone**

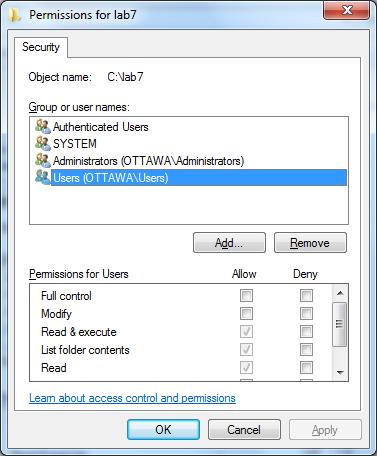
This group is the same as the Authenticated Users group except it does contain the **Guest** account.

You cannot modify or view the members of the two groups mentioned above. The membership of these groups is under the control of the operating system. They do not contain the anonymous users **IUSR\_** and **IWAM\_** which are accounts used in IIS (WEB services).

Fig. 2 DACL of drive C:

**Users group**

This group is the same as the Authenticated Users group because the Authenticated Users group is a member of this group. The difference between users and authenticated users is, the administrator can modify the membership list of this group, but he cannot view or change the membership of the Authenticated users group.

**Inherited Permissions**

NTFS permissions are assigned at the root level of the hard drive and then trickle down or are inherited by folders and their sub-folders and then to the files found in those folders.

Figure 3 shows the default permissions on a folder found in the root of C:. If you compare the DACL of this folder with the DACL of drive C: in figure 2 you will see they are the same.

The only difference is the check marks in the bottom half of the folder’s DACL are greyed-out indicating the permissions were inherited

and cannot be modified. Fig. 3 This folder has inherited permissions

If you wish to change the permissions on this folder you must break the inheritance as shown in figure 4. To break the inheritance, clear this box.

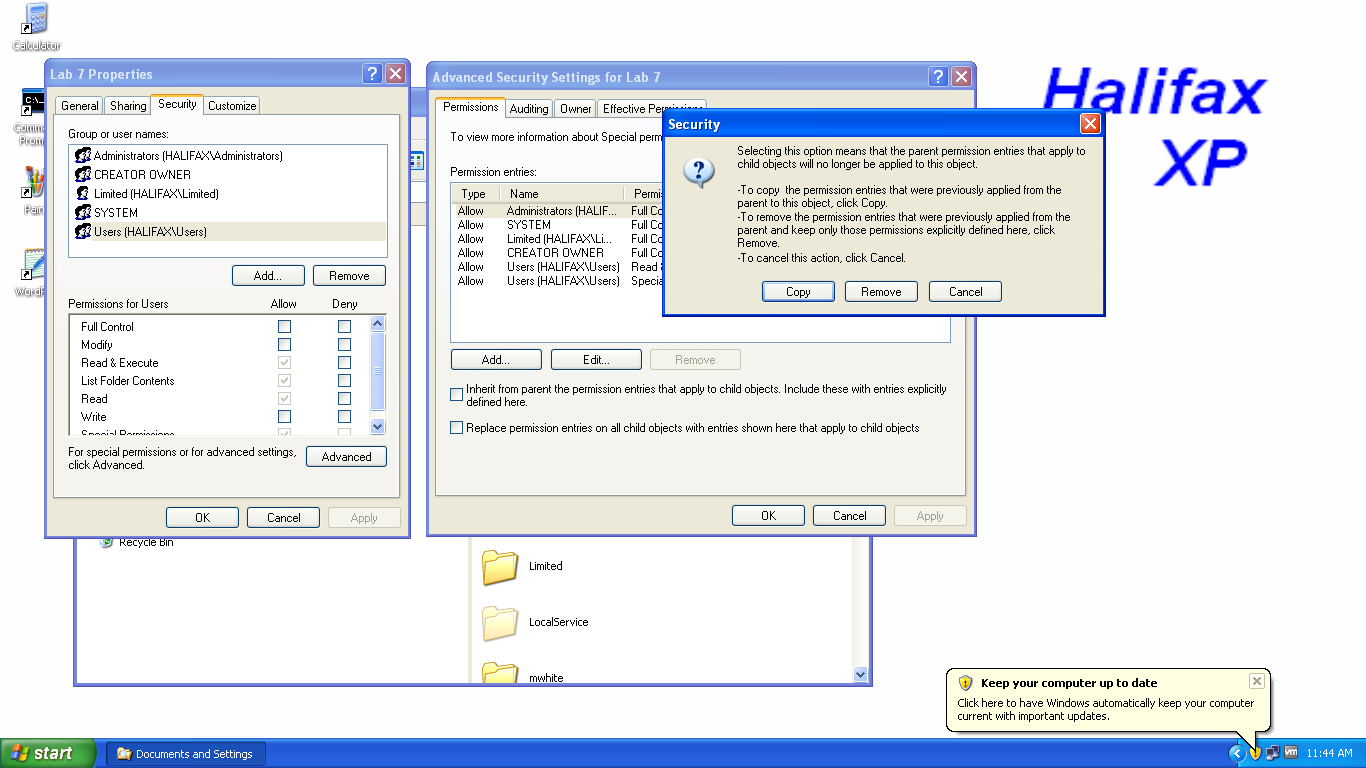
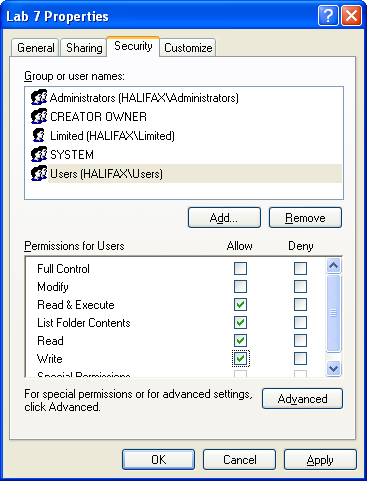


Fig. 4 Breaking the inheritance on a folder

When you clear the box in figure 4, you will be given the option to remove all the permissions or copy them as they appeared through inheritance.

Figure 5 shows the results of copying the permissions when the inheritance is broken. You can see the permissions assigned to Users is no longer greyed-out. As a matter of fact, if you compare figure 5 with figure 4, you can see the administrator has added the write permission.

**Shared Folder**

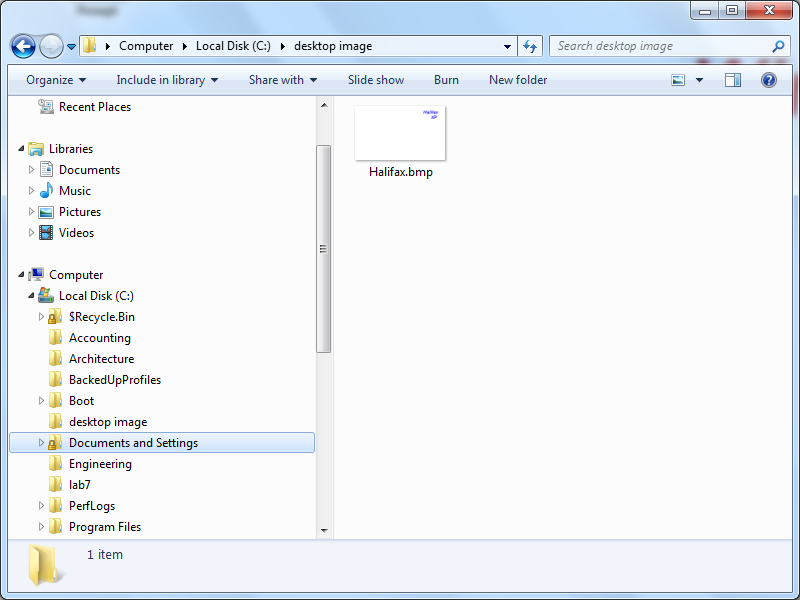
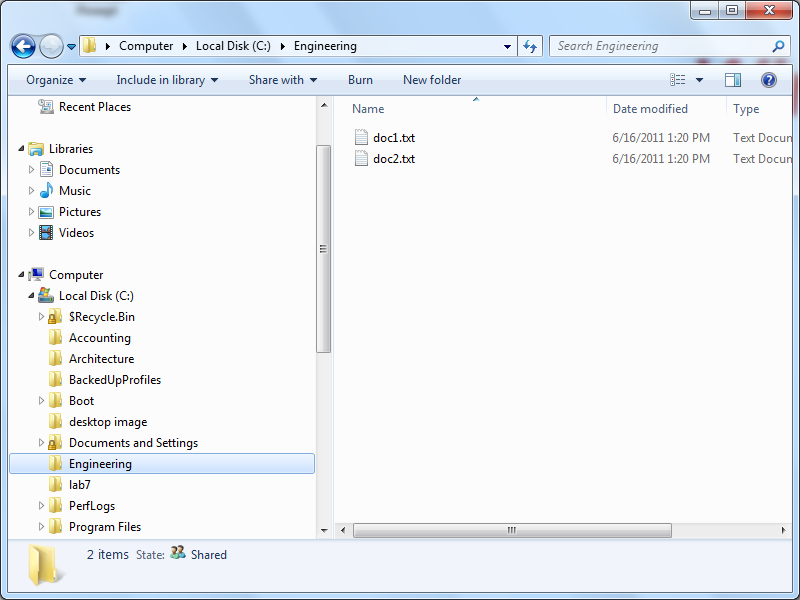
If you want users on another computer to access files and folders on your computer, you must share the folders.

It is easy to tell which folders are shared when you open the Windows Explorer on an XP Machine. There is a little hand under Fig. 5 Inheritance has been broken

the folder representing a person handing

data so someone else as if they were sharing the data with the other person.

With Windows 7, Windows 8, and Windows 10 it is not so easy. Microsoft tried to improve the user experience by not congesting the windows with too much information that a novice user would not need. The hand under the folder was one of the things to get axed. Now when you view the folders in Windows 7/8/10, the only way you can tell if a folder is shared or not is to click on it and check the status bar to see if it says “shared”



Documents and Settings is not a shared folder

Engineering is a shared folder

Fig. 6 With Windows 7/8/10 a shared folder is indicated as “shared” in the status bar

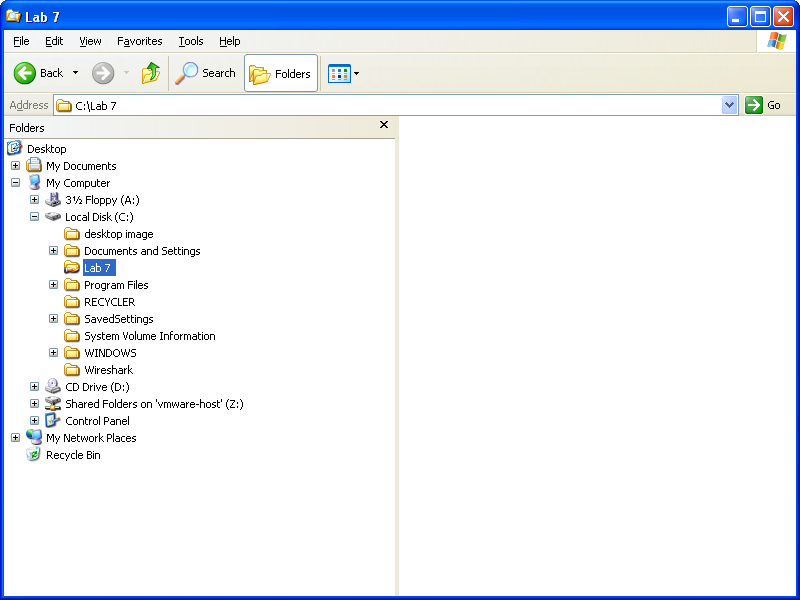
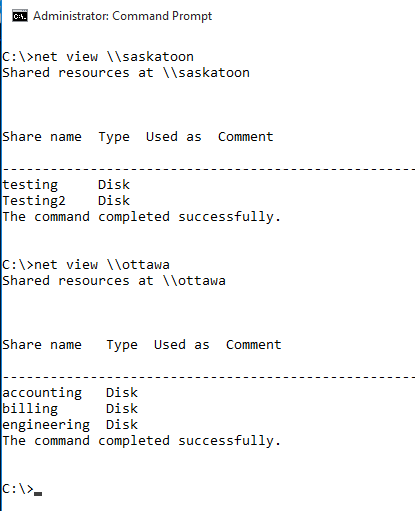


Fig. 7 XP indicates a shared folder by placing a hand under the folder

There is no problem telling which folders are shared in XP although, if there are shared folder inside other folders they will not be any easier to find than with Windows 7/810.

Regardless of the operating system, there is an easy way to find all the shared folders. Open a command prompt window and type:

**net view \\<host-name>**

The net view command is shown in figure 8.

The command works on the local machine as well as on a remote machine.

Fig. 8 Using the net view command to discover

the shared resources on Ottawa

and Saskatoon.

**Authenticating Local User Accounts in a Peer-to-Peer network**

When a user logs into a local account on a computer, the **SAM** authenticates his username and password. It then issues him a session ticket which allows the user to access resources on the computer he logged into. Figure 9 shows the SAM database. It is found in the **C:\Windows\system32\config** folder.

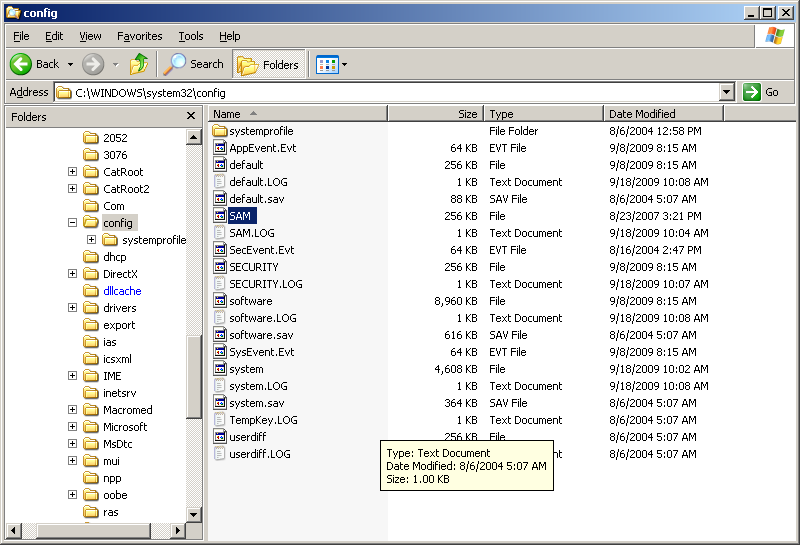


Fig. 9 The Security Accounts Management database (SAM)

If the user tries to access a shared folder on another computer, that computer must first authenticate the user. This means the user requires the same username and password on the computer where the folder is found. When the user is authenticated on the second computer, the second computer issues the user a **session ticket** which allows him to access resources on the second computer.

If the user does not have an account on the other computer, he will be required to supply the username and password of an account that exists on the remote host.

If the user changes his password and then logs in on the first computer, he will not be authenticated by the second computer because the second computer is still working with his old password. Therefore, when a user changes his account on 1 computer in a peer-to-peer network, he must make the same change to his account on the other computers.

There are 3 methods to authenticate to another computer to gain access to that computer’s resources.

1. have an account with the identical username and password set up on the

remote computer.

2. supply a username and password of a user on the remote computer when

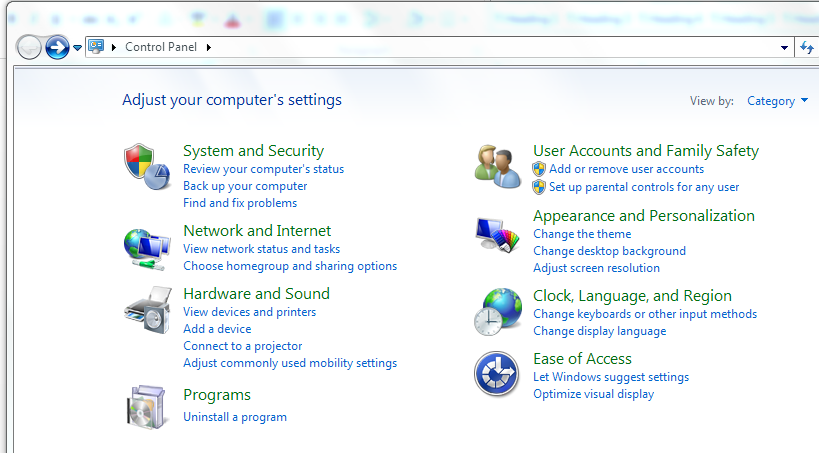
challenged to enter a username and password.

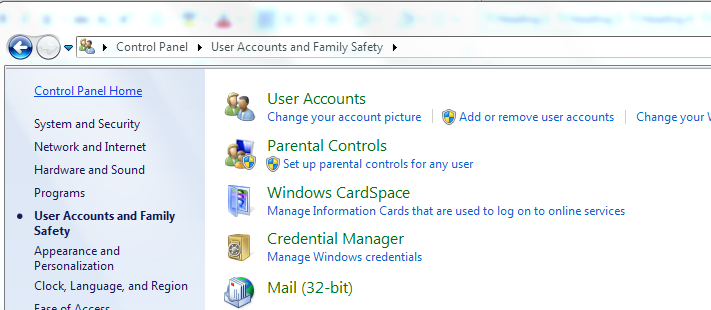
3. For Windows 7/810, go into **Control Panel**, **User Accounts**, click on the **Advanced** tab, **Manage Passwords** button**, Add a Windows Credential**. See fig. 10. Anyone can add passwords for their account in Windows 7/810.

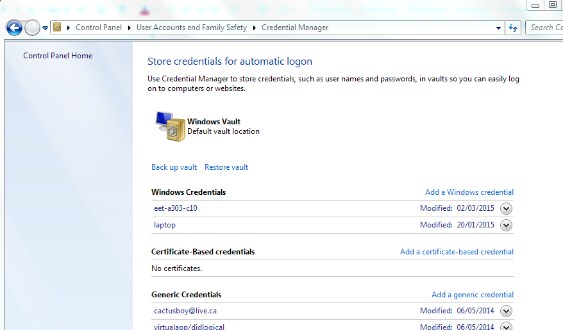
You can add the credentials of any user on any computer. When you try to

access resources on that remote computer, it will work seamlessly since your

computer will supply the credentials you saved as shown in figure 10.







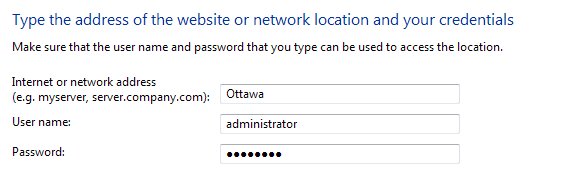


Fig. 10 Adding credentials for Ottawa on the Saskatoon computer

**Finding out what groups a user belongs to**

There are a couple of commands a user can issue to find out what groups he is a member of. You can use **gpresult /R**. See figure 11.

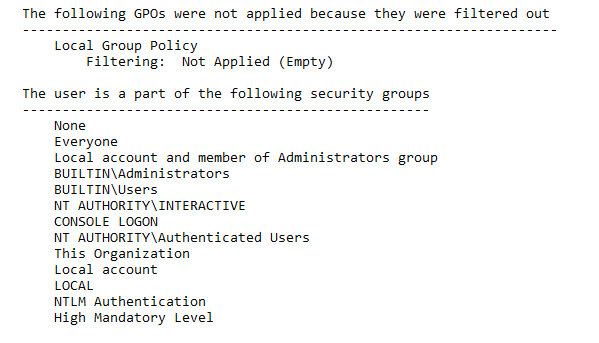


Fig. 11 **gpresult /R** shows the groups a user belongs to

You can also type **Whoami /groups > group-list.txt**. The output of the whoami command is piped to a text file because the DOS window in too narrow to display the wide lines. The output is too hard to read. The output displays fine if it is piped to a text file. See figure 12.

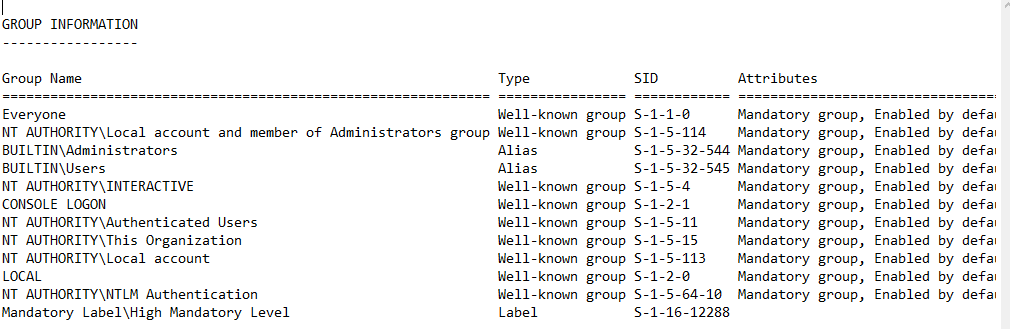


Fig. 12 The output of **whoami /groups > group-list.txt** shows the user’s groups