NTFS Permissions
File and Directory Permissions:
NTFS permissions are largely the same. The following tables will break down each of the permissions types. The following table displays the different permissions for files.

Full Control	Read, write, modify, execute, change attributes, permissions, and take ownership of the file.
Modify	Read, write, modify, execute, and change the file's attributes.
Read & Execute	Display the file's data, attributes, owner, and permissions, and run the file (if it's a program or has a program associated with it for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

The following table displays the different permissions for directories.

Full Control	Read, write, modify, and execute files in the folder, change attributes, permissions, and take ownership of the folder or files within.
Modify	Read, write, modify, and execute files in the folder, and change attributes of the folder or files within.
Read & Execute	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
List Folder Contents	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

The Read & Execute and List Folder Contents folder permissions appear to be exaclty the same, however, they are inherited differently, thus are different permissions. Files can inherit the Read & Execute permissions but can't inherit the List Folder Contents permission. Folders can inherit both.

So you may be wondering what is really different from NT 4.0. NT 4.0 gave the options of granting access or not specifying. Windows 2000 has the new option of denying a user or users a particular permission. For example, if you wanted to make sure that Bob is unable to read any file, then simply deny him read permissions. Permissions are cumulative, except for Deny, which overrides everything.

The next table shows what happens to files when they are copied or moved within or across NTFS partitions.

Moving within a partition	Does not create a new file - simply updates location in directory. File keeps its original permissions.
Moving across a partition	Creates a new file and deletes the old one. Inherits the target folders permissions.
Copying within a partition	Creates a new file which inherits permissions of target folder.

Files moved from an NTFS partition to a FAT partition do not retain their attributes or security descriptors, but will retain their long filenames.

As with NT 4.0, Windows 2000 also supports special access permissions which are made by combining other permissions. The following tables will show special access permissions and how the recipe to make them.

File Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X
Create Folders/Append Data	X	X			X
Write Attributes	X	X			X
Write Extended Attributes	X	X			X
Delete Subfolders and Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				
Synchronize	X	X	X	X	X

Folder Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read
Traverse Folder/Execute File	X	X	X	X	
List Folder/Read Data	X	X	X	X	X
Read Attributes	X	X	X	X	X
Read Extended Attributes	X	X	X	X	X
Create Files/Write Data	X	X			
Create Folders/Append Data	x	x			
Write Attributes	X	X			
Write Extended Attributes	X	X			
Delete Subfolders And Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				
Synchronize	X	X	X	X	X

Remember that file permissions override the permissions of its parent folder. Anytime a new file is created, the file will inherit permissions from the target folder.

Share Permissions:
Shares are administered through the MMC, My Computer or through Explorer and permissions can be set on a share in the "Share Permissions" tab. Share level permissions only apply when a file or folder is being accessed via the network and do not apply to a user logged into the machine locally. The following are the different share-level permissions:

Read	View files and subdirectories. Execute applications. No changes can be made.
Change	Includes read permissions and the ability to add, delete or change files or subdirectories
Full Control	Can perform any and all functions on all files and folders within the share.

These permissions are identical to NT 4.0, however, there is one new change. As we discussed above the Deny permission can also be applied to shares. The Deny permission overrides all others. When folders on FAT and FAT32 volumes are shared, only the share level permissions apply as these systems do not support file and directory permissions. When folders on NTFS volumes are shared, the effective permission of the user will be the most restrictive of the two. This means that if Bob is trying to access a file called *mystuff* located on *myshare* and he has share permissions of read and file permissions of full control, his effective permissions would be read. Conversely, if his share permissions are full control and his file permissions are read, he will still only have read permissions to *mystuff*

When comparing either Share or NTFS permissions, the least restrictive always wins out. When comparing both Share and NTFS permissions, take the least restrictive of each category and then the more restrictive of those two