INFO6003 Lab-04 Permissions

For this lab the student will explore permissions for Windows securable objects.

Requirements

- **2008-FOLusername** Server 2008 R2 VM from Lab-03
    - Password for the Domain Administrator account should be Windows12 at this point
- **W7-FOLusername** Windows 7 VM from lab-03
    - Password for the domain Administrator account should be Windows1 at this point
- **Win10-FOLusername** Windows 10 VM from lab-03
    - Password for the domain Administrator account should be Windows1 at this point

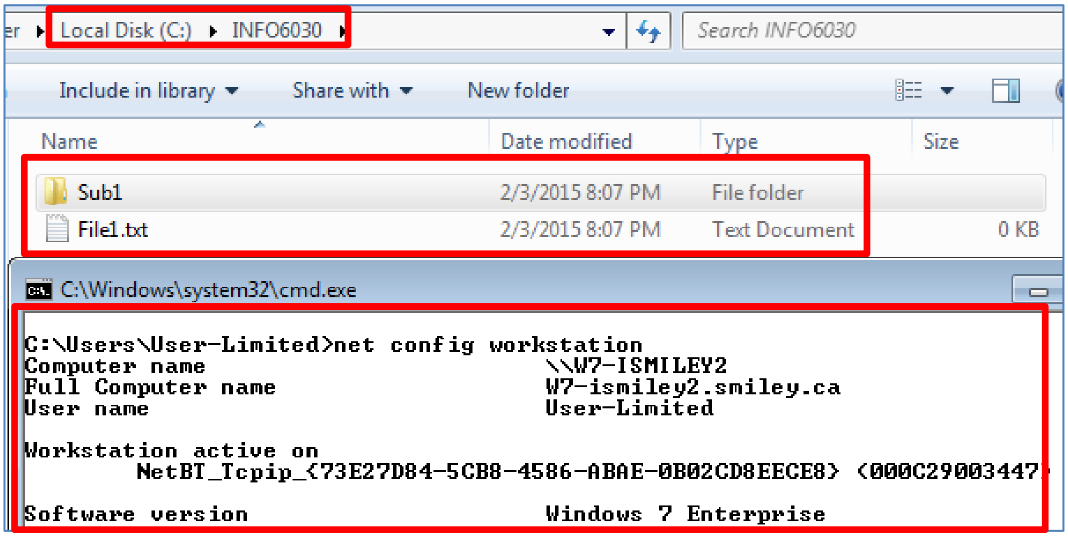
- Logon to each of the VMs as the **domain admin**, do a net config workstation and ping the other VM

Slide 1: net config workstation and ping for 2008-FOLusername VM
Slide 2: net config workstation and ping for W7-FOLusername VM
Slide 3: net config workstation and ping for W10-FOLusername VM

NTFS Permissions (On Windows 7 VM)

- For this portion we are going to logon to the W7 VM as a local user (switch user, other user)
- You need to use the following syntax to accomplish this
    - **User-Limited** (password should be Windows1)
- In the C: drive create a new folder named **INFO6003** (case sensitive, no spaces)
- Inside the INFO6003 folder, create a text document named **File1** (case sensitive, no spaces)
    - **Note: right click then choose, new and text document**
- Create a subfolder inside INFO6003 named **Sub1** (case sensitive, no spaces)
- Within Folder Options, then under view, choose to show extensions for known file types (search in start menu for folder options)

Slide 4: net config workstation and show INFO6003, Sub1 and File1



er ▸ Local Disk (C:) ▸ INFO6030 ▸
Search INFO6030
Include in library ▾
Share with ▾
New folder
C:\Windows\system32\cmd.exe

Name	Date modified	Type	Size
Sub1	2/3/2015 8:07 PM	File folder	
File1.txt	2/3/2015 8:07 PM	Text Document	0 KB

```
C:\Users\User-Limited>net config workstation
Computer name                        \\W7-ISMILEY2
Full Computer name                   W7-ismiley2.smiley.ca
User name                            User-Limited

Workstation active on
        NetBT_Tcpip_{73E27D84-5CB8-4586-ABAE-0B02CD8EECE8} (000C29003447

Software version                     Windows 7 Enterprise
```

- Move back to the C: drive and right-click on the folder INFO6003
- Choose **Properties** → **Security**

- In the security tab, note the users and groups that have permissions to this folder.
    - As you click on each user you can see their permissions below
- Select **Advanced → Change Permissions…**
- Select **Administrators → Edit…**
- In the Permission Entry for INFO6003 dialog, select the **Deny** box opposite the Full control permissions (We are explicitly denying the Administrators Full Control)
- Click **OK → OK →** and **Read** the Windows Security Warning… Click **Yes**
- In the Advanced Security Settings window note that the permissions for the Administrators group is now denied full control and the explicit deny permission is moved to the top of the list
- Select **OK and OK.**

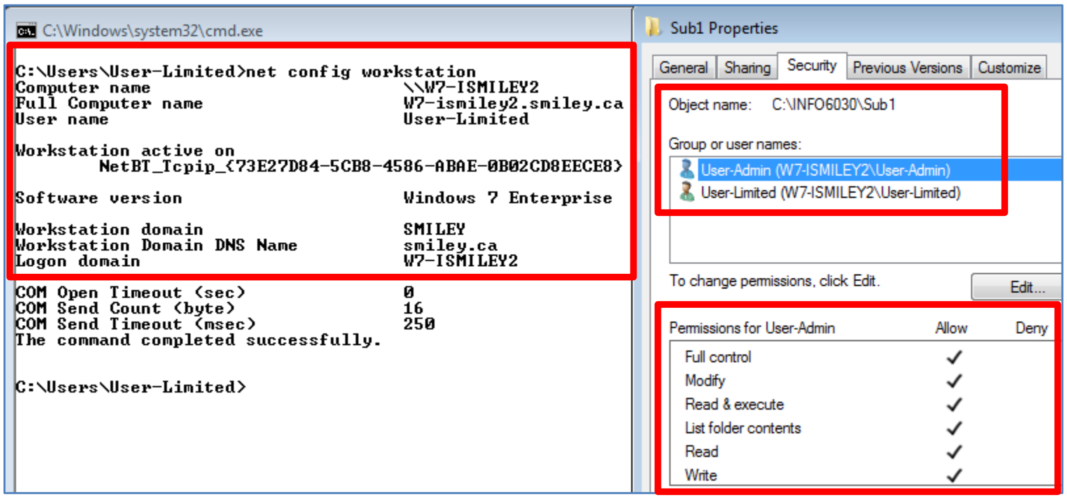
- Open the INFO6003 folder and look at the Properties for Sub1
- Choose **Properties → Security → Advanced**
- Note the Administrators group is denied access to the Sub1 folder and that this setting was inherited from the C:\INFO6003 folder. Additionally, they are allowed Full control from C:\

- **Log off as User-Limited and log back on as User-Admin**. Try to open the INFO6003 folder. *You should be denied access even though you're the administrator*!

- **Log on as User-Limited** and open INFO6003 folder and select the subfolder **Sub1**
- Choose **Properties → Security → Advanced → Change Permissions…**
- Remove the check mark from the box **Include inheritable permissions from this object's parent**
- **Play Close Attention** In the security warning select **Remove**. **(don't hit OK or apply after removing them)**
- All permissions should now be removed from the permissions entry window.
- Select **Add** then in the select object window enter **User-Admin → Check Names → OK.**
    - **You will be prompted for a domain admin password, even if you enter it, this is going to fail because we want to search locally, not on the domain. (close the dialogs)**
    - **Click on the Locations button and choose your local computer (cancel out of any dialogs)**
- In the Permissions Entry for Sub1 window check the box Allow **full control**. Click OK and Apply.

- **Repeat** this Procedure to allow full control for **User-Limited**.
- Click OK until you are back at the Sub1 Properties window.

Slide 5: Rearrange the windows to get the screen capture below



```
C:\Users\User-Limited>net config workstation
Computer name                        \\W7-ISMILEY2
Full Computer name                   W7-ismiley2.smiley.ca
User name                            User-Limited

Workstation active on
        NetBT_Tcpip_{73E27D84-5CB8-4586-ABAE-0B02CD8EECE8}

Software version                     Windows 7 Enterprise

Workstation domain                   SMILEY
Workstation Domain DNS Name          smiley.ca
Logon domain                         W7-ISMILEY2

COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.


C:\Users\User-Limited>
```

Object name: C:\INFO6030\Sub1

Group or user names:

User-Admin (W7-ISMILEY2\User-Admin)
User-Limited (W7-ISMILEY2\User-Limited)

To change permissions, click Edit.

Permissions for User-Admin	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

- Close your various windows, then **log off as User-Limited** and log on as **User-Admin**
- Try to access the Sub1 folder through Windows explorer.
- **Why is access denied to INFO6003**?
- Try to access the Sub1 folder via the command prompt with the following command:
    - **cd C:\INFO6003\Sub1**
- **Was access still denied?**

- **Log off as User-Admin and log on as User-Limited**
- In **Computer Management**, expand Local Users & Groups and select the **Groups folder.**
- To view the group's memberships, right click on the **Administrators** group and select Properties.
- When the window opens it will show the users that are members of the Administrators group. In this case it should be **Administrator, FOLusername\Domain Admins, User** and **User-Admin.**
- Close the window, then select the Users group and view the membership. Note **User-Admin** is part of both groups.
- Close the Computer Management window.

- You should be logged on as **User-Limited** at this point.

- Create a new folder called **Secure1** off of C:\ (case sensitive and no spaces)
- **Deny** the **Users** group **Full Control**. **(You may have to refer to previous instructions)**
- Note that the Administrators group still has Full Control.
- **Log off and log on as User-Admin.** If you try to access the Secure1 folder, access will be denied even though User-Admin is a member of the Administrators group that inherited the allow full control permission.
- User-Admin is also a member of the group Users that was explicitly denied full control and because the deny was listed first that action was taken and the allow permission was never read or executed.

Access Control Lists

- Logon as **User-Limited**

- The **icacls** command can be used to view the individual Access Control Entry (ACE) lines of the Discretionary Access Control List (DACL) and set permissions for a file from the command line.
- To view the permissions for File1.txt in the INFO6003 folder
    - Open a command prompt
    - Change to the INFO6003 folder and type the command:
    - **icacls File1.txt**
- The output shows the individual access control entry (ACE) lines with subject and permissions

- View the permissions for the Sub1 folder in the INFO6003 folder
    - **icacls sub1**

- Note that when used on a folder, the inheritance permissions are shown along with the special permissions to the folder for each ACE.
    - CI – Container Inherit
    - OI – Object Inherit
    - F – Full Control
- Type the command **icacls** by itself to show the options and arguments for the command.
- Find the portion that talks about the canonical ordering of the ACE entries
    - It is a bit more than half way through the output.

  - What does this mean?

Using icacls to Change Permissions

- From the command line, Deny the Users group all access to File1.txt
  - **icacls File1.txt /deny Users:F**
- Now view the ACL: **icacls File1.txt**
- There will now be a new entry at the top of the list for BUILTIN\Users: (N)
- Use the /? Option with icacls to see what (N) represents.

- Execute the following command:
  - **icacls File1.txt /inheritance:r**
  - Now view the ACL: **icacls File1.txt**

- **What just happened?** You can use the help file to break the commands down if you can't figure them out.

Registry Permissions

- Logoff User-Limited and login using the **User-Admin** account
- Run the **regedit** program from the Start Menu.
- When the Registry Editor opens
- Navigate to HKEY_LOCAL_MACHINE → SAM →SAM, right-click the lower SAM folder and select **Permissions**
- Note that the System is the only account that has full control over the key. Click Advanced, select the Administrators group and click **Edit**. Notice the Administrators group only has the **Write DAC** and **Read Control** special permissions.

Why is this not a good idea?

Leave this window open for now to get the next screenshot.

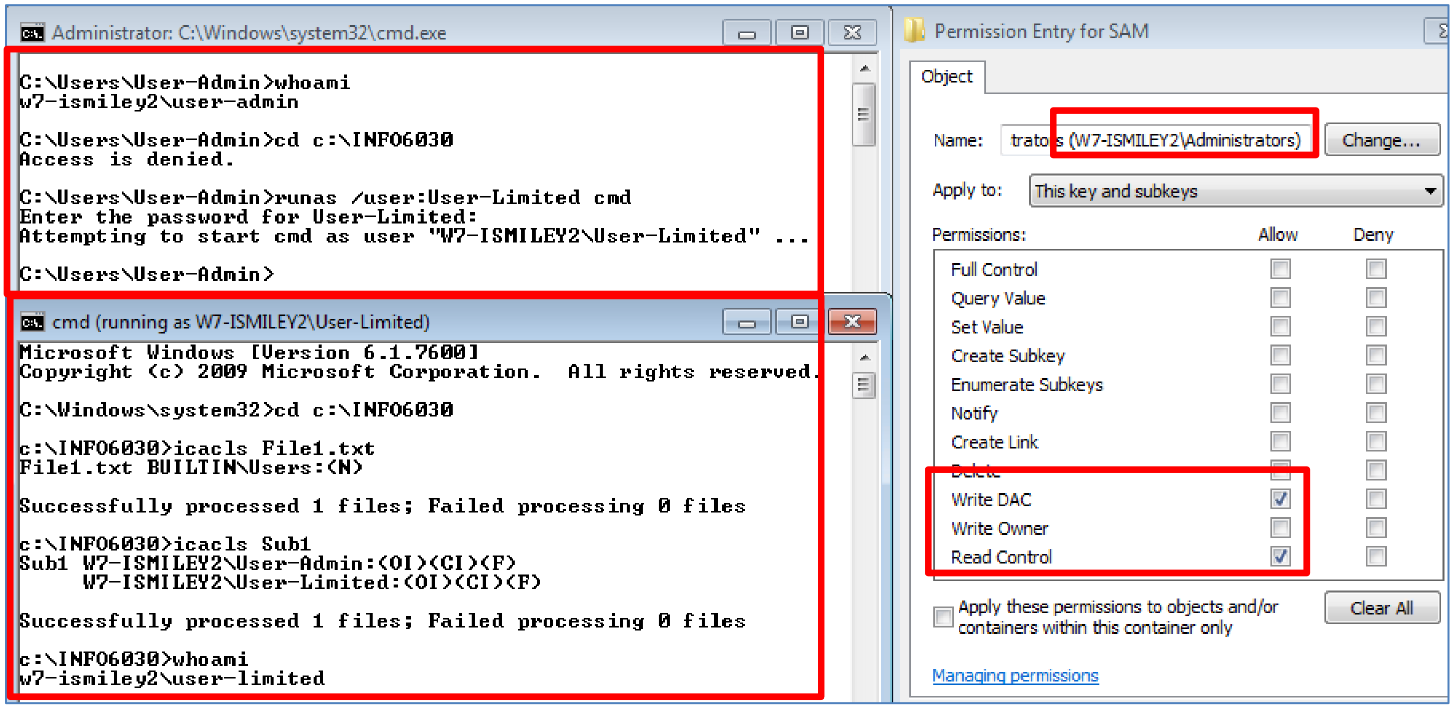
Running a Process with the Security Token of another User

- Open a command prompt and type the following two commands
  - **whoami**
  - **cd c:\INFO6003**
- Administrators are still denied access to the directory unfortunately, but we can run a command window as another user. Run the command:
  - **runas /user:User-Limited cmd**
- Enter User-Limited's password to open a second command window running with the security token of User-Limited!

- In the new command window, run the following three commands:
- **cd c:\INFO6003**
- **icacls File1.txt**
- **icacls Sub1**
- **whoami**

The details for getting the final screenshot are on the next page

Slide 6: Arrange the open windows to get the final screen capture
You will need to change the size of your CMD windows to get it all to fit.
Make sure you show all the highlighted information.


Administrator: C:\Windows\system32\cmd.exe
cmd (running as W7-ISMILEY2\User-Limited)
Permission Entry for SAM
Object

```
C:\Users\User-Admin>whoami
w7-ismiley2\user-admin

C:\Users\User-Admin>cd c:\INFO6030
Access is denied.

C:\Users\User-Admin>runas /user:User-Limited cmd
Enter the password for User-Limited:
Attempting to start cmd as user "W7-ISMILEY2\User-Limited" ...

C:\Users\User-Admin>
```

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd c:\INFO6030

c:\INFO6030>icacls File1.txt
File1.txt BUILTIN\Users:(N)

Successfully processed 1 files; Failed processing 0 files

c:\INFO6030>icacls Sub1
Sub1 W7-ISMILEY2\User-Admin:(OI)(CI)(F)
     W7-ISMILEY2\User-Limited:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

c:\INFO6030>whoami
w7-ismiley2\user-limited
```

Name: trators (W7-ISMILEY2\Administrators) Change...

Apply to: This key and subkeys

Permissions:	Allow	Deny
Full Control	□	□
Query Value	□	□
Set Value	□	□
Create Subkey	□	□
Enumerate Subkeys	□	□
Notify	□	□
Create Link	□	□
Delete	□	□
Write DAC	☑	□
Write Owner	□	□
Read Control	☑	□

□ Apply these permissions to objects and/or containers within this container only

Clear All

Managing permissions

Login from Win10 guest with Domain Admin account and browse to the server 2008 to create a Data folder. Share it with Full control. Give user-limited NTFS read only. Give user-Admin NTFS read / write.

Slide 7: Create a screen shot that shows each user with their permissions.

Power down your VMs and take snapshots called After Lab-04

1) **File share security options include?**

2) **Why do we use file share on the network?**

3) **If both file share and NTFS security are on a folder which security is applied to the user who has access?**