

INFO6003 Lab-05 Process Explorer & ABE

Preparation

- Windows 7 and Server 2008 R2 VMs from previous labs, on host only network
- **Before you power on** the VMs, you need to **ADD** a NAT network adapter to the W7 VM
 - VM settings, Add Network Adapter, NAT is the default
- Power on both VMs, then logon to the W7 VM with the **domain Administrator** account
 - At this point passwords should be Windows1 or Windows12
 - When prompted, set the new network as Public (this is Network Location Awareness)

Fine Tuning Commands

There are many times where we want to limit the output we are getting from a command. This is often the case during our labs, where you need to show me a variety of information in one screen capture. We are going to look at some options we can use to limit the output that is displayed to the screen.

Ping

- We can control the number of pings we send with the **-n count** option
- The syntax is **ping -n count (IP Address / DNS Name)**
 - **ping -n 2 google.ca**
- The command above will ping google twice

Pipe

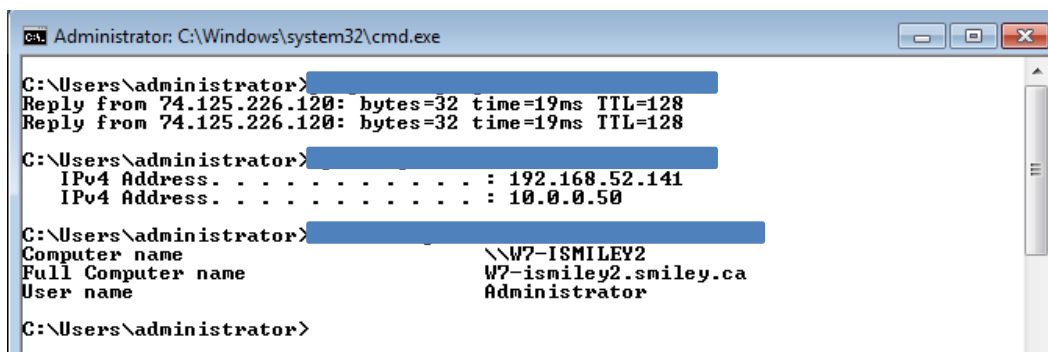
- If we want to further modify the output of the ping command, we can use the pipe command which will send the output of one command to another
- Command 1 | Command 2 (sends the output of command 1 to command 2)

Find

- We can use the pipe command with the find command to further filter the output
- In its default format we can search for a text string with the **find "string"** command
 - **ping -n 2 google.ca | find "TTL"**
- The command above will ping google.ca twice, then search the output for lines that include TTL and return only those lines to the screen

Slide 1:

- **Ping google.ca with two requests, and only show the replies**
- **Do an IP config only showing the lines that include your IP Addresses**
- **Do a net config workstation, only showing lines that include the string "name"**



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\administrator>ping 74.125.226.120
Reply from 74.125.226.120: bytes=32 time=19ms TTL=128
Reply from 74.125.226.120: bytes=32 time=19ms TTL=128

C:\Users\administrator>ipconfig
IPv4 Address. . . . . : 192.168.52.141
IPv4 Address. . . . . : 10.0.0.50

C:\Users\administrator>netconfig workstation
Computer name                \\W7-ISMILEY2
Full Computer name           W7-ismiley2.smiley.ca
User name                     Administrator

C:\Users\administrator>
```

Process Explorer & Security Tokens

- Every security principal is given a security token. You can view the tokens using Microsoft's Process Explorer tool. The tool is available for download from Microsoft.

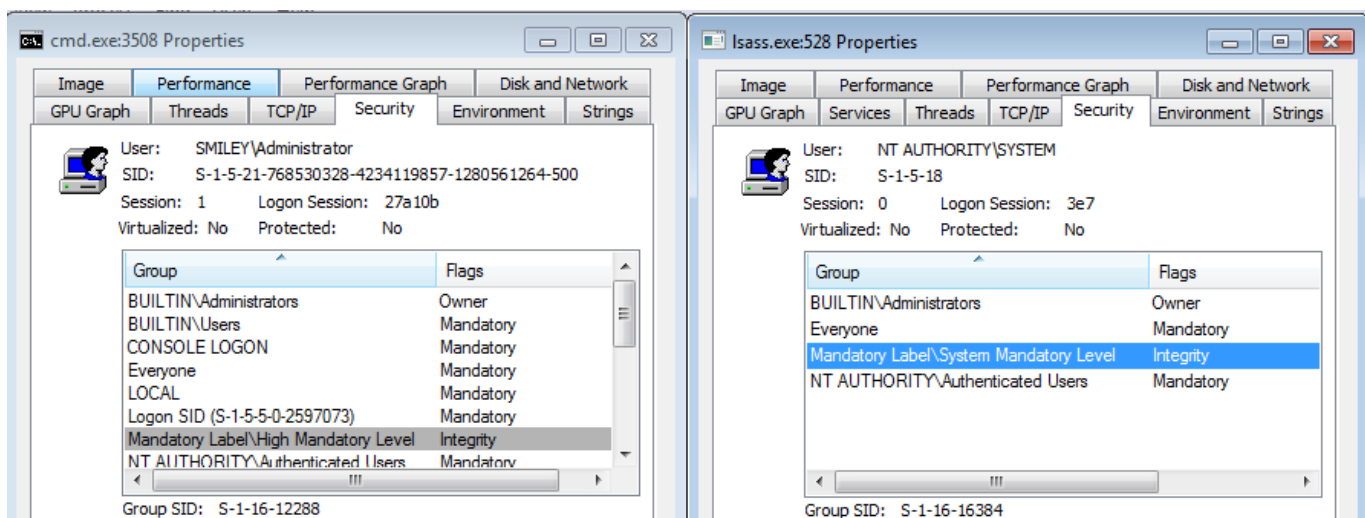
<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

- The program downloads as ProcessExplorer.zip
- Create a folder called **C:\PE** and extract the file there
 - Eula, Help File and Process Explorer Application
- Run procexp.exe.
 - The left hand panel shows the processes that are running.
 - Open a command prompt, leave it open in the background and go back to process explorer.
 - The cmd.exe process will be shown at the bottom of the list.
- Right click on cmd.exe and view its properties.
 - Select the **Security** tab to view the security token for Administrator: the user who started this process
 - This tab displays the Username, SID, Session information and contains two panels: one with group details and one with privilege details.
 - Note the assignment of special groups like BUILTIN\Administrators BUILTIN\Users and Everyone.
- Find the "Mandatory Label" entry
 - From the information you see, can you relate this back to the lab introduction?
- The bottom panel shows all the privileges granted to this user, quite a few for the domain admin.
 - Note that some are Default Enabled and some are Disabled.

Leave the cmd.exe properties window open for the next screen capture.

- Look at the security properties for the lsass.exe process
 - What integrity level is this process running at?
 - Notice the difference in the number of privileges that are Default Enabled

Slide 2: take a screen capture of the Security tab for the properties of cmd.exe and lsass.exe. Highlight the integrity level for both processes



Logon as **User-Limited** then:

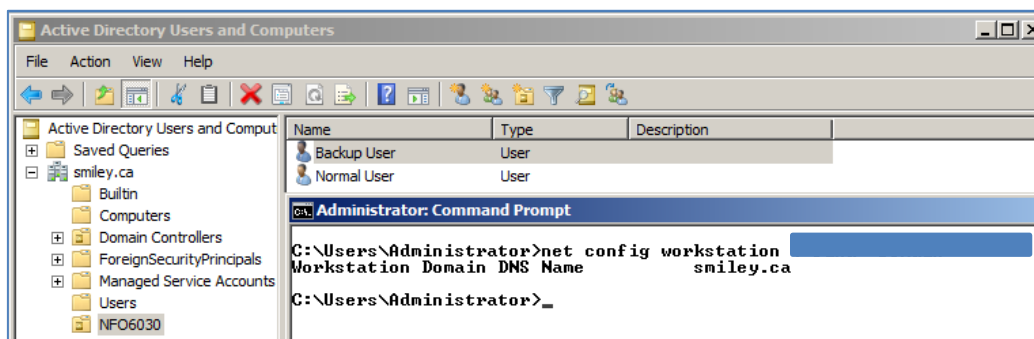
- Launch Process Explorer from the C:\PE folder
- View the security token for User-Limited. (use cmd.exe again)
- Notice that the list of Privileges is much shorter for the limited account user
- Also, what is the integrity level associated with this user?

Access Based Enumeration

Tasks to be completed on Server 2008 R2 VM

- Open “Active Directory Users and Computers”
- Start Menu, Administrative Tools, Active Directory Users and Computers
- Click on the **Users** Container (**found under your domain**). Note the 2 Built-in **user** accounts.
- What is the description for the Domain Admins group? Who are its members?
 - Note: this can be found through the properties (do some searching).
- Create two new users in an OU called INFO6003 with the following steps.
 - Right click on your domain name and choose to create a new Organizational Unit called **INFO6003**
 - Right click the INFO6003 OU, then **new>User**
 - Use the following values:
 - First Name: **Normal**
 - Last Name: **User**
 - Full Name: **Normal User**
 - User logon name: **n_user**
 - Click next, set the password to **Windows1**, and check the “password never expires” box.
- Perform this same tasks to **create Backup User**. (first name **Backup**, last name **User**, logon name **b_user**)

Slide 3: Show all the information in the screen capture below: INFO6003 OU, users in INFO6003 OU and net config workstation lines that include “Domain”

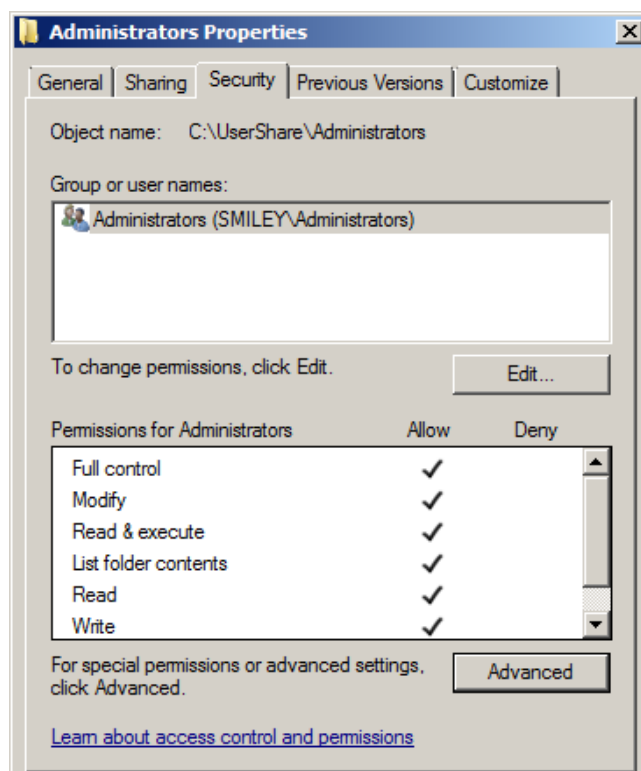



- In the Left Pane, select the **Builtin** Container. Take a few minutes and look over the names and descriptions of the built-in security groups.
- Double click the **Backup Operators** group – This is potentially a very dangerous group.
- Select the **Members** tab, click add, then type **Backup User** into the object selection window. You can use check names to make sure you have the right user. Click OK and OK to add the user to the group.

- Open My Computer and create a folder named **C:\UserShare**.

- Create three folders inside the UserShare folder:
 - **Administrators**
 - **BACKUP-USER**
 - **NORMAL-USER**

- Edit the permissions for the Administrators, NORMAL-USER and BACKUP-USER folders, explicitly giving only the group Administrators and users: Normal User and Backup User access to **their own folders only. (Full Control)**
- Note: You will need to go into the advanced security settings for the folders, **remove** inheritable permissions, and then add the appropriate user.
- When done, your security settings should be similar to the one on the right, only one user for each folder.



- Example for Administrators on right 
- At the command prompt navigate to the **UserShare** directory

Slide 4: include the output of net config workstation only returning lines with “name” and the output of the icacis * command

```

Administrator: Command Prompt
c:\UserShare>net config workstation
Computer name          \2008-ISMILEY2
Full Computer name     2008-ismiley2.smiley.ca
User name              Administrator

c:\UserShare>icacis *
Administrators BUILTIN\Administrators:(OI)(CI)(F)
BACKUP-USER SMILEY\b_user:(OI)(CI)(F)
NORMAL-USER SMILEY\n_user:(OI)(CI)(F)
Successfully processed 3 files; Failed processing 0 files
c:\UserShare>_

```

Other than the domain, the permissions output from the **icacis** command should match the screen capture above **Exactly** before you move on.

Research Access Based Enumeration on Microsoft TechNet.

[http://technet.microsoft.com/en-us/library/dd772681\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd772681(v=WS.10).aspx)

Now that you know what ABE is and how to use it from your research, enable ABE on the **UserShare** folder. (If you paid attention in class you have already researched how to do this)

- The steps to enable ABE are well laid out on TechNet, here is the short form:
 - Turn sharing on for the UserShare folder (advanced)
 - Open Share and Storage Management
 - From the advanced properties for UserShare enable ABE

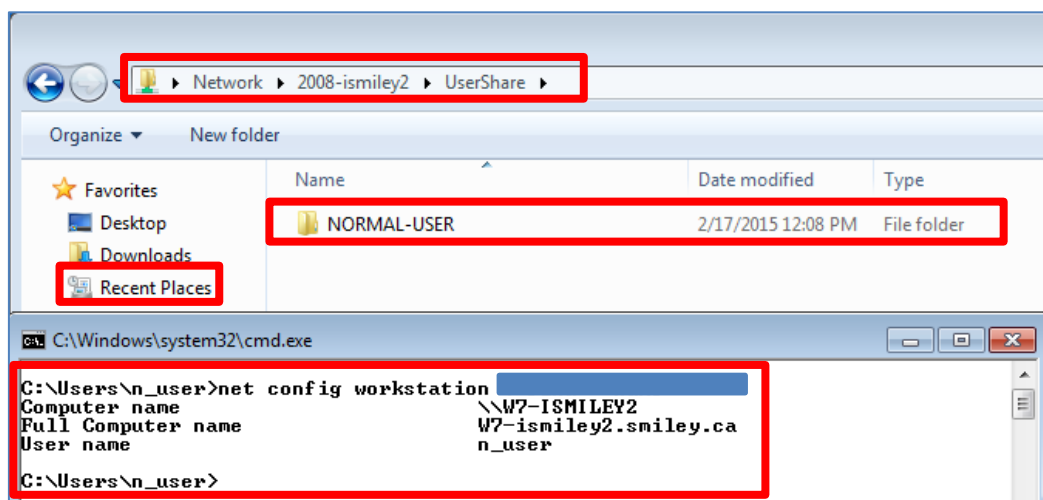
If you need more guidance than that, go back to the TechNet site.

- Logon to the W7 VM as **Normal User** (make sure you are using the logon name)
- On the W7 VM use Windows Explorer to go to: **\\2008-FOLusername\UserShare**
 - (You type this into the address bar of file explorer, not IE)

Slide 5: Take a screen capture that matches the following layout, including the output of the net config workstation command, only returning lines with “name”

Note: YOUR COMMAND PROMPT CAN'T BE HIGHER THAN THE WORDS “Recent Places”

- This is because I need to be able to see any possible folders in UserShare



Slide 6: Generate the same screenshot for Backup User

Why is Backup User's output different than the output for Normal User?

Slide 7: Generate a screenshot of your new Windows Server 2016 after you have tried to do PDC promo.

Why should you not complete the process?

Note that you must do a snap shot image of your Network before you add the Server 2016 to the domain.

This is for bonus marks but all students must show me that they tried to complete the task.

Read this site for help

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>