DAC Demo

# Demo 1

* Create another user on the system
* Create a text file in C:\Users\Public
* Go back to the original user and try to access the file. An access denied message should come up.

Reference: C:\Users\Public\non-admin1\_demo\_file.txt

MAC Demo

Tools Needed: ProcessExplorer

# Demo 1 – Labels

* Open notepad and create a text file with something in it. Save it as test.txt in somewhere the user has access to.
* Open a command prompt and change directory to where the original test.txt file was created (in Demo 1).
* Show the current integrity level (no label means it is inherited for the user which is medium)

icacls test.txt

* Now change the integrity level to high

icacls test.txt /setintegritylevel h

* Open Notepad and attempt to make a change and save over it [Should get and error]
* From the Start Menu right click on Notepad and "Run as Administrator"
* Attempt to modify and save the text file again.

# Demo 2 - Notepad

* Open notepad and create a text file with something in it. Save it as test.txt in somewhere the user has access to.
* Use explorer to copy that file to c:\windows\system32 and click continue at the dialog box. This dialog box is the gateway to the change in integrity.
* Open the file, modify it, and try to save it. It will show a dialog. Try to save it over the itself in system32. You will get a permission denied.
* Run: icacls c:\windows\system32\test.txt
* You will not see any mandatory access label because it is inherited as "High". If you look at properties for the file the user still has ownership of it.
* In the start menu find notepad. Right click and select "Run as Administrator". This should start Notepad
* Do the same for Process Explorer and run it using "Run as Administrator"
* Look at the Notepad process listed in process explorer. It should show the integrity as "High". Note if you don't see this column then add it under the view menu.
* Open the c:\windows\system32\test.txt in the Notepad running as Administrator. You should be able to modify it and save it.

# Demo 3 - Process Explorer

* Open Process Explorer (without "Run as Administrator"). Note that many processes are missing information in the "Integrity" column. This is because Process Explorer itself isn't allowed to read the integrity level of other processes.
* Open a second Processes Explorer by right clicking and select "Run as Administrator"
* Compare the two. One is running with administrative privileges with an Integrity of "High"

# Demo 4 - Location Matters

* Open Windows Explorer and copy you test.txt file to C:\Windows\System32
* A dialog box will come up asking for administrative permissions. This is because System32 is treated as High integrity
* Double click on the file to have it open in Notepad
* Modify the file and try to save it. It will not let you save it over the existing file. This is because notepad is running at the Medium Integrity Level
* Open a Command Prompt and run

cd \windows\system32

icacls test.txt

* Note that it doesn't show a Integrity Level since it is inherited
* Go to the Start Menu and Find Notepad. Right click on it and "Run as Administrator"
* Now open the test.txt file and try to save some kind of modification you make to it. It should work because both the process and the file are at the same Integrity Level
* Go back to the Command Prompt and run

cd %USERPROFILE%\AppData

icacls LocalLow

* Notice the Mandatory Label is low for that directory

# Demo 5 - Low Integrity Applications

* Open a Command Prompt and do

cd \windows\system32

copy calc.exe calc\_low.exe [Should fail]

* This fails because the Command Prompt is running at a different integrity level
* Find the Command Prompt on the Start Menu and right click to "Run as Administrator"
* Now do the same commands

cd \windows\system32

copy calc.exe calc\_low.exe [Should Work]

* This works. Now modify the calc\_low.exe to have a low integrity label

icacls calc\_low.exe /setintegritylevel l

* Open Windows Explorer and head over to c:\windows\system32
* Double click on calc\_low.exe
* Windows gives you a warning since the file is of low integrity

Reference File:

MAC = C:\Program Files\demo\MAC\_MIC\_Demo.txt

# References

http://security.stackexchange.com/questions/65375/what-is-a-visible-example-for-a-mandatory-access-control-mac

https://msdn.microsoft.com/en-us/library/bb625965.aspx

https://msdn.microsoft.com/en-us/library/bb625960.aspx

https://msdn.microsoft.com/en-us/library/bb625963.aspx

Protecting Objects in MS: https://www.microsoftpressstore.com/articles/article.aspx?p=2228450&seqNum=3

Windows Integrity: https://blogs.technet.microsoft.com/yuridiogenes/2011/04/13/exploring-the-windows-security-survival-guide-integrity/