Exploit #1 – Cover Tracks with Alternate Data Streams

Open theWin7 VMware image and login as account name **User**

Open File Explorer and from the **security** folder create a new sub folder named **ads**.

Copy **felix.exe** & **plane.jpg** from the ***c:\security*** folder to the ***c:\security\ads*** folder Open notepad.

Enter your name and favourite professor as the text message. Save the file with name **info6001.txt** to the ***c:\security\ads*** folder.

Open a command prompt

Change to the **ads** directory

C:\User\User> **cd \security\ads**

View the contents of the ADS directory C:\security\ads> **dir**

Note the size & time stamp of the yourFOLname.txt file

____ .

Note the size & time stamp of the felix.exe file

____ .

Note the size & time stamp of the plane.jpg file

____ .

Hide the info6001.txt text file behind the plane.jpg file in the security folder

C:\security\ads> **type info6001.txt > c:\security\ads\plane.jpg:hide.txt**

The output of the type command is now redirected to the alternate data stream space behind the ***plane.jpg*** file in the windows folder and indexed with the name hide.txt

Delete info6001.txt from the ads folder

C:\ security\ads> **delete info6001.txt**

Retrieve hide.txt and rename as yourFOLname.txt

C:\ security\ads> **more < c:\security\ads\plane.jpg:hide.txt>** ***yourFOLname.txt***

At the command prompt enter the following 2 commands

C:\ security\ads> **dir**

*View the **ads** folder and the text file **yourFOLname.txt** will now be listed*

C:\ security\ads> **type** ***yourFOLname.txt***

*View the contents to ensure this is the same text as entered and saved to the file **info6001.txt***

1. ***Take a screen capture of the command prompt showing the output of the last 2 commands***

Hide the executable program felix.exe in the ***yourFOLname*.txt** data stream
C:\security\ads> **type felix.exe > *yourFOLname.txt*:felix.exe** The program ***felix.exe*** is now hidden behind the text file View the **ads** folder and the text file **yourFOLname.txt** C:\security\ads> **dir**

Note: The size of the yourFOLname.txt has not changed

Note: The time stamp on the file has been updated

Execute the hidden program
Felix can be executed from behind the ***yourFOLname.txt*** file

First create a symbolic link to the felix.exe program in the ***c:\security\ads*** folder
C:\security\ads> **mklink hack.exe *yourFOLname.txt*:felix.exe**

To run the felix program start the file name for the symbolic link C:\security\ads> **start .\hack.exe**

You should see Felix the cat walking across your screen

2. Take a screen capture showing the command prompt & Felix

Use task manager to view the running process

Note that the file yourFOLname.txt has not been displayed
Running felix.exe from its hidden location did not cause the parent file to be executed

Use task manager to close the felix program

Hide the executable program felix.exe in the plane.jpg data stream
C:\security\ads> **type felix.exe > plane.jpg:felix.exe**

Open the plane.jpg file C:\security\ads>
plane.jpg

Did felix run?

Do you see the cat on the desktop?

Note: The size of the plane.jpf file has not changed

Note: The time stamp on the plane.jpg file has been updated

Open Task Manager
Is felix.exe listed as a running process?

Note: Opening the parent program **will not run** the program hidden behind in the alternate data stream

Exploit #2 – Cover tracks with Tini
To avoid virus program detection, change the tini binary code and file name

Make sure **tini.exe** has been **stopped** before proceeding. The code will be locked if the program is running.

From the security folder open the Tini folder and find the Hex Editor installer program **hexedfull** Double click to **Run** the installer program.
After the install wizard is finished close the wizard and open hexedfull.exe
Start → Programs → hexedfull.exe

From the hexedfull.exe program select **File → Open** (browse to the directory with tini.exe)

In the program change the port that Tini will listen for a connection from 7777 to 8888
Decimal 7777 = 1E61 in Hexadecimal
Edit → Find in the **Bytes** window box type in **1e** then click OK
The editor will find the line with 1E 61
If not scroll down to line 430
Overwrite the **1E61** with **22B8** (0x22B8 = 8888 in decimal)

Save as a different file name that might evade detection
File → Save as ***yourfirstname*.exe**

Run *yourfirstname*.exe

From a command prompt run the command **netstat –nao** to verify a program is now running and listening on port **8888**

3. Take a screen capture of the netstat command make sure the process id (PID) is included

The file could be copied to any folder and file on the system and remain undetected as a backdoor Trojan installed on their computer.