

Hide Files using Alternate Data Streams

@mmar



The NTFS file system includes support for alternate data streams. A file stream is a sequence of bytes that contains data about a file, such as keywords or the identity of the user who created the file. Think of a data stream as a file within a file — a hidden file residing within a legitimate one. Each stream has its own disk space allocation, its own actual size (bytes in use) and its own file locks.

Step-1

- ❖ Copy calc from system32 folder to your test folder, Now create a text file and append the cal.exe to the file

```
type calc.exe >readme.txt:calc.exe
```

```
E:\Working\Test>type calc.exe >readme.txt:calc.exe

E:\Working\Test>dir
Volume in drive E is Ammar
Volume Serial Number is 8856-F0AC

Directory of E:\Working\Test

03/02/2023  10:34 AM    <DIR>          .
03/02/2023  10:34 AM    <DIR>          ..
12/07/2019  02:09 PM                27,648 calc.exe
03/02/2023  10:35 AM                 19 readme.txt
                2 File(s)        27,667 bytes
                2 Dir(s)  50,120,216,576 bytes free
```

Step-2

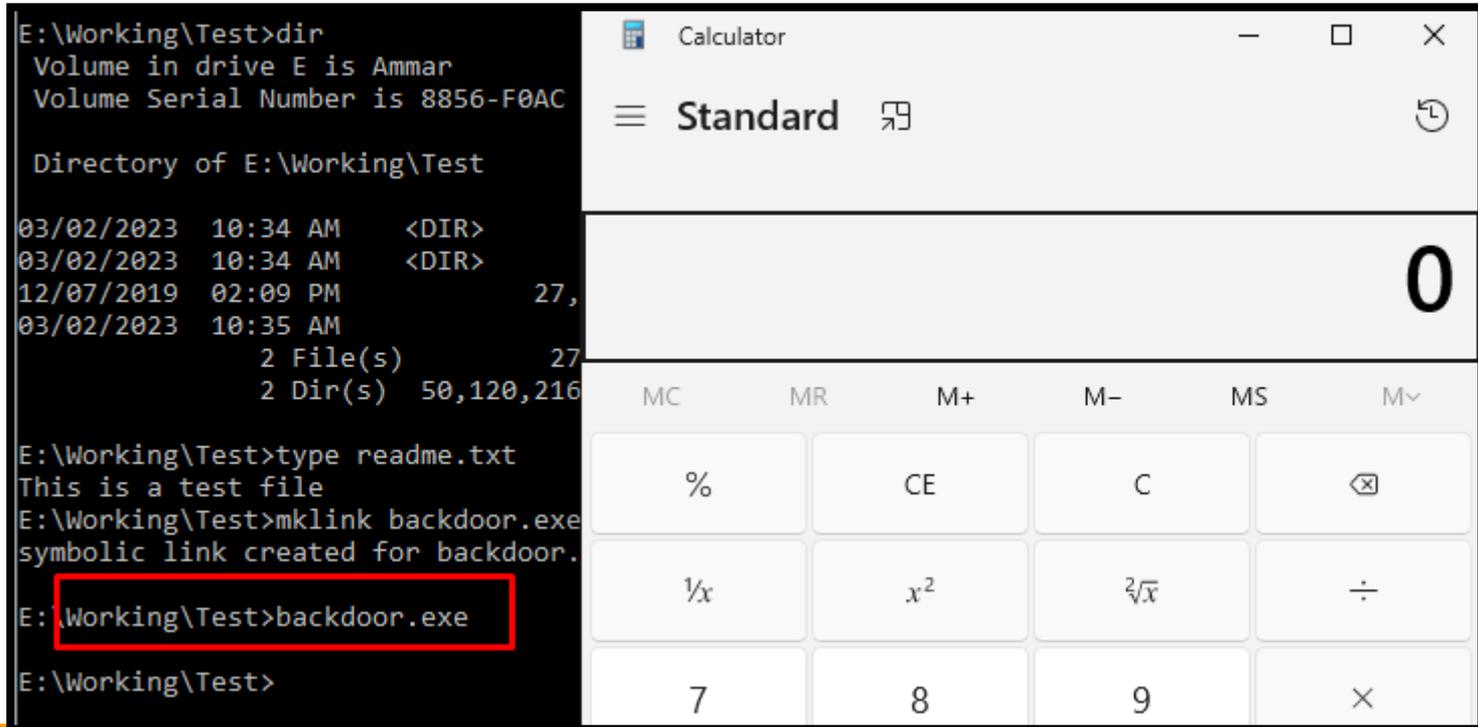
- ❖ Now create a link to the ADS file to create backdoor

```
mklink backdoor.exe readme.txt:calc.exe
```

```
E:\Working\Test>type readme.txt  
This is a test file  
E:\Working\Test>mklink backdoor.exe readme.txt:calc.exe  
symbolic link created for backdoor.exe <=> readme.txt:calc.exe
```

Step-4

- ❖ Opening the backdoor link will open the hidden file



The image shows a Windows command prompt window on the left and a Windows calculator window on the right. The command prompt shows the following commands and output:

```
E:\Working\Test>dir
Volume in drive E is Ammar
Volume Serial Number is 8856-F0AC

Directory of E:\Working\Test

03/02/2023  10:34 AM    <DIR>
03/02/2023  10:34 AM    <DIR>
12/07/2019  02:09 PM                27,
03/02/2023  10:35 AM
                2 File(s)          27
                2 Dir(s)  50,120,216

E:\Working\Test>type readme.txt
This is a test file
E:\Working\Test>mklink backdoor.exe
symbolic link created for backdoor.

E:\Working\Test>backdoor.exe

E:\Working\Test>
```

The calculator window is titled "Calculator" and is in "Standard" mode. The display shows the number "0". The calculator interface includes a menu icon, a "Standard" mode selector, a refresh icon, and a grid of buttons for mathematical operations and constants.

DEMO



THANKS