Hide Files using Alternate Data Streams

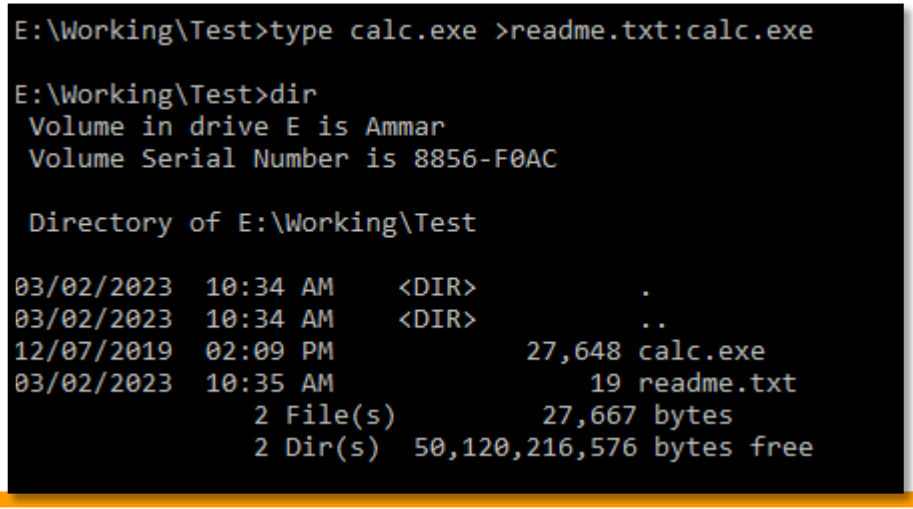
@mmar

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
```



Step-2

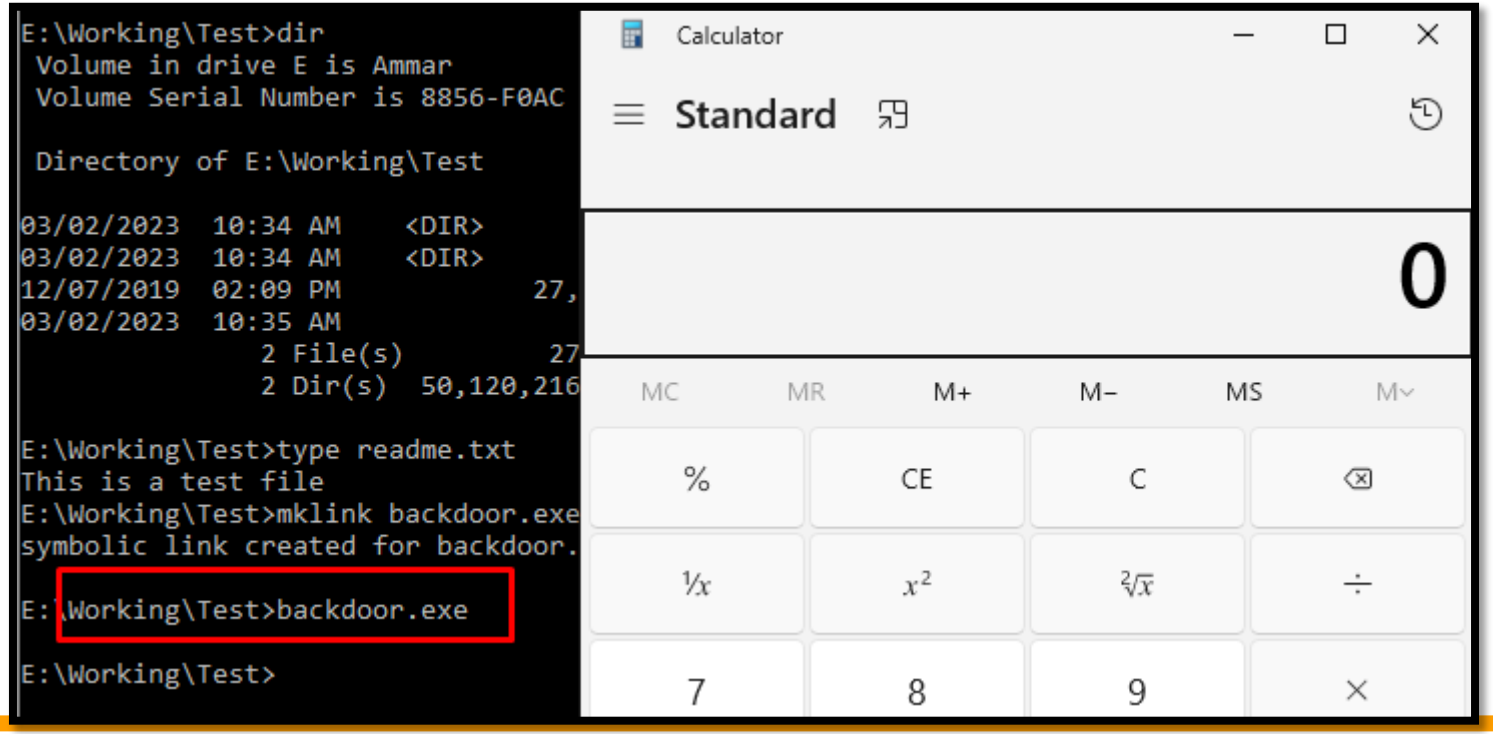
- Now create a link to the ADS file to create backdoor

```
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



DEMO

THANKS