NTFS数据流隐写

原创

m0re 于 2020-12-12 17:08:57 发布 1479 收藏 10
分类专栏： CTF 文章标签： NTFS
m0re

前言

最近做题遇到了几个是NTFS数据流隐写的题目，感觉很有趣，就深入的学习一下。知识面较浅。

什么是NTFS数据流？

> NTFS交换数据流（alternate data streams，简称ADS）是NTFS磁盘格式的一个特性，在NTFS文件系统下，每个文件都可以存在多个数据流，就是说除了主文件流之外还可以有许多非主文件流寄宿在主文件流中。它使用资源派生来维持与文件相关的信息。————百度百科

> NTFS交换数据流（alternate data streams，简称ADS）是NTFS磁盘格式的一个特性，在NTFS文件系统下，每个文件都可以存在多个数据流，就是说除了主文件流之外还可以有许多非主文件流寄宿在主文件流中。它使用资源派生来维持与文件相关的信息，虽然我们无法看到数据流文件，但是它却是真实存在于我们的系统中的。创建一个数据交换流文件的方法很简单，命令为“宿主文件：准备与宿主文件关联的数据流文件”。————百度百科

NTFS数据流隐藏文件的方法和实例

创建一个数据交换流文件的方法，命令为“宿主文件：准备与宿主文件关联的数据流文件”。
首先，分出一个很小的盘，来测试用。

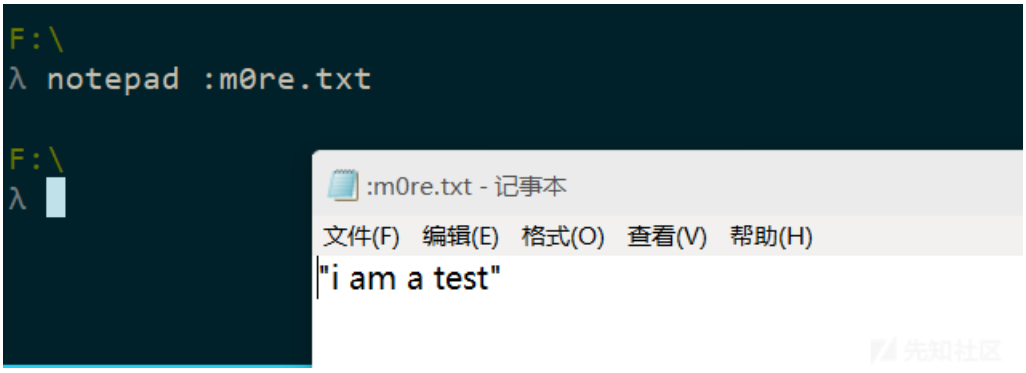
1.单文件流隐藏

先在F盘中新建一个空的文本文件，命名为m0re.txt，
创建一个NTFS数据流，

```
echo "i am a test" > :m0re.txt
```

已经成功的隐藏信息，查看方式有两种
一种是使用windows自带的notepad查看，命令如下

```
notepad :m0re.txt
```



第二种方法是使用工具，`lads.exe`

```
lads.exe /S
```

```
F:\
λ lads.exe  /S

LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory F:\ with subdirectories

      size  ADS in file
----------  ------------------------------
        16  F:\:m0re.txt
Error 5 opening F:\System Volume Information\

The following summary might be incorrect because there was at least one error!

        16 bytes in 1 ADS listed
```


扫描到这个文件存在NTFS数据流，然后用第一种方法显示出来。

2.关联文件流

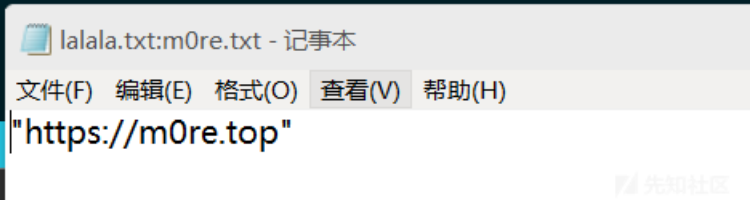
```
echo "https://m0re.top" > lalala.txt:m0re.txt
```

此时的m0re.txt是宿主文件，将信息内容隐藏到宿主文件中了，直接打开`lalala.txt:m0re.txt`查看数据流文件

```
F:\
λ echo "https://m0re.top" > lalala.txt:m0re.txt

F:\
λ
```

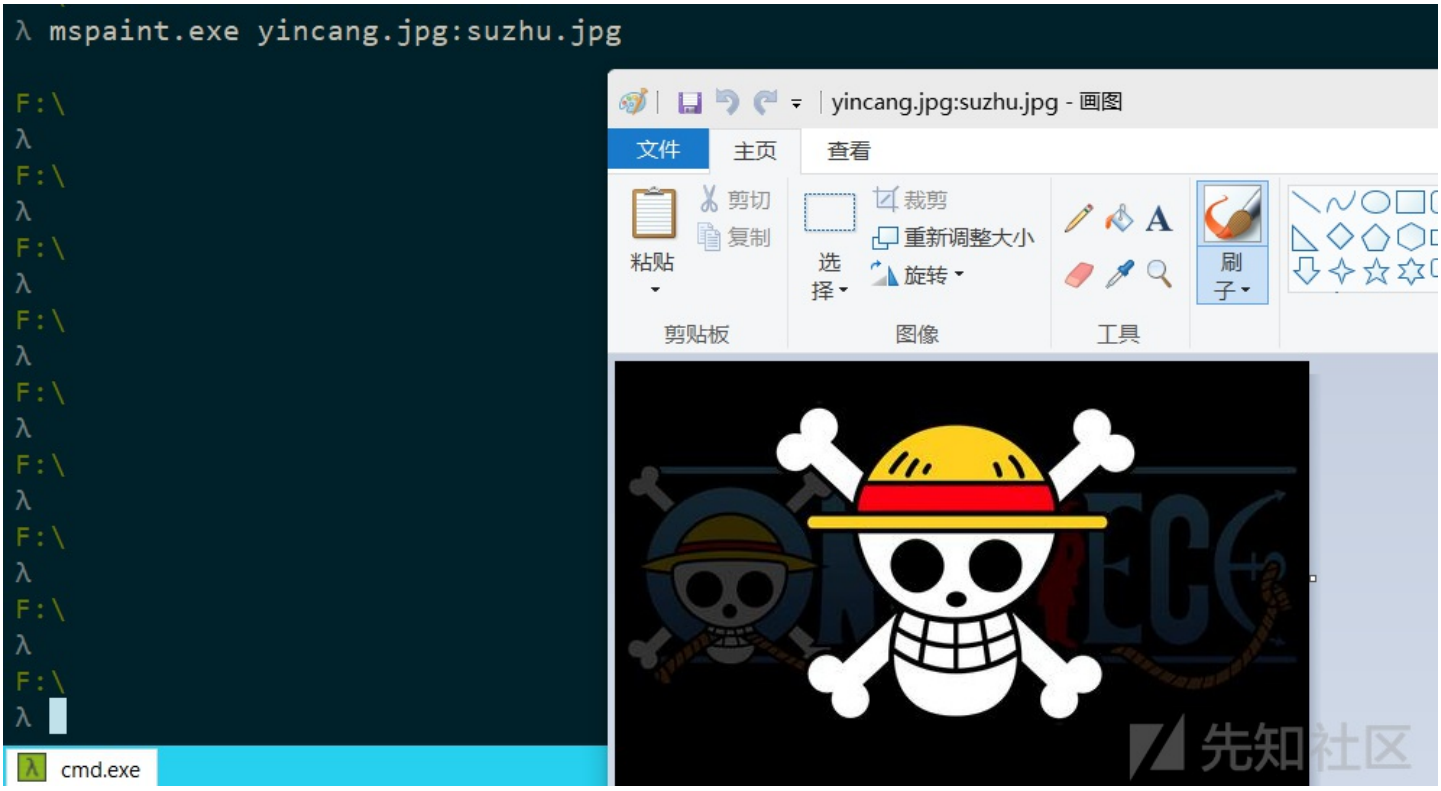

这里需要注意的是这个不是将数据写入到文件中，而是创建了NTFS数据流，信息都在数据流当中。这个`lalala.txt:m0re.txt`就是创建的流文件。

```
F:\
λ notepad lalala.txt:m0re.txt

F:\
λ
```



当然不止可以隐藏文本数据，还可以隐藏其他的文件，比如exe可执行文件，pyc文件等
这里使用type命令，来隐藏文件。

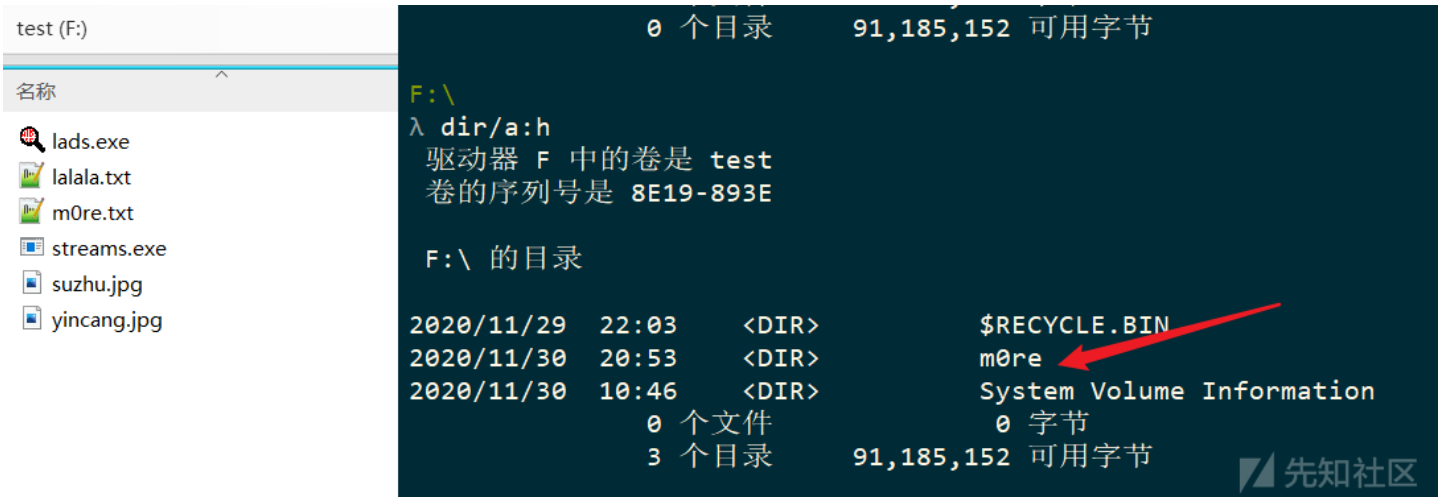
```
type yincang.jpg >yincang.jpg:suzhu.jpg    #隐藏图片到另一张图片中
#查看方式使用windows自带的mspaint.exe
mspaint.exe yincang.jpg:suzhu.jpg
```



了解：windows系统隐藏文件夹和查看方法

隐藏：`attrib m0re +a +s +h`

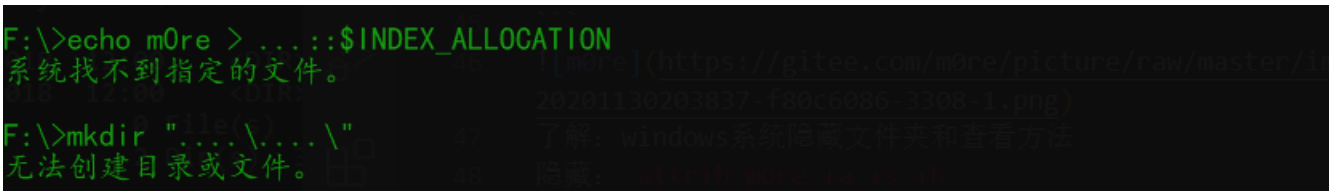
查看：`dir/a:h`



1.创建...文件夹

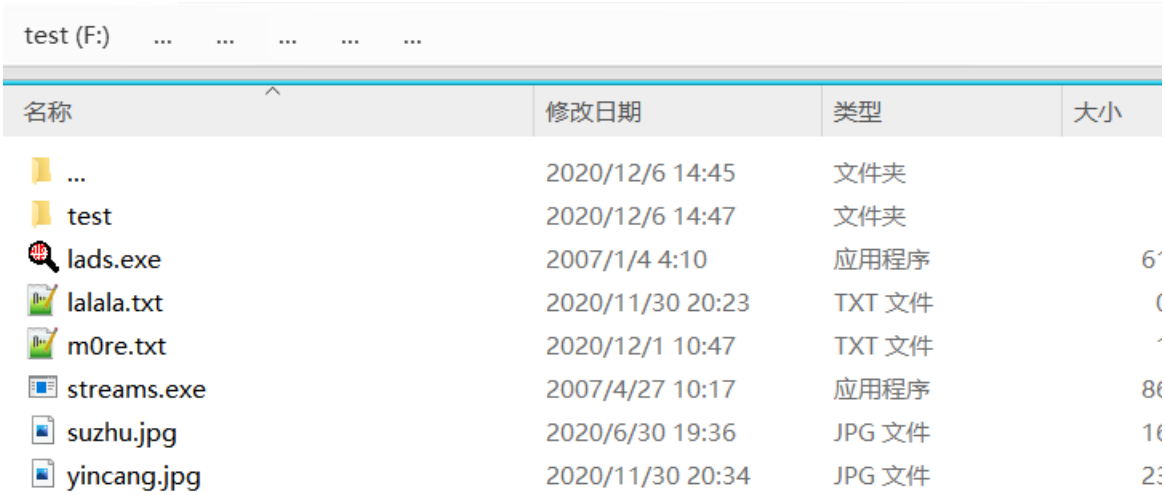
我们都知道，在windows系统中是无法创建以点命名的目录。所以一般是无法创建...的目录文件的。

```
...::$INDEX_ALLOCATION
mkdir "...\...\"
```



```
F:\>dir
 驱动器 F 中的卷是 test
 卷的序列号是 8E19-893E

 F:\ 的目录

2020/12/06  14:45    <DIR>          ...
2007/01/04  04:10            61,952 lads.exe
2020/11/30  20:23                 0 lalala.txt
2020/12/01  10:47                15 m0re.txt
2007/04/27  10:17            87,424 streams.exe
2020/06/30  19:36            15,545 suzhu.jpg
2020/12/06  14:41    <DIR>          test
2020/11/30  20:34            22,771 yincang.jpg
               6 个文件        187,707 字节
               2 个目录     89,636,864 可用字节
```

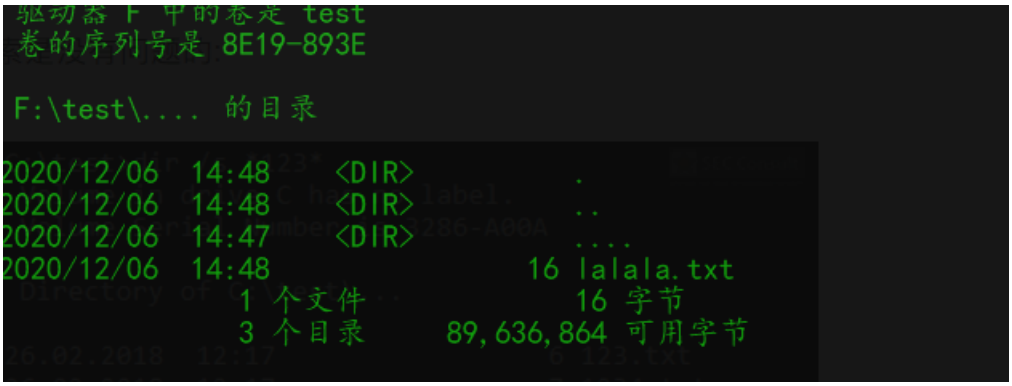
怎么进入这个文件夹呢？在资源管理器中是进不去的。



无法仅使用名称进入文件夹(例如:`cd …`或`cd …\`或`cd …\…`不起作用)，必须使用`cd …\…\`的语法。进入文件夹之后可以在这个文件夹里创建文件。

在cmd中进入，使用命令进入，但是无法通过GUI(`explorer.exe`)进入，而且删除不了，无法进行删除操作。(PS:后悔了，早知道给虚拟机里实验了。55555)

```
F:\test>cd ....\....\

F:\test\....>echo m0resixsixsix > lalala.txt

F:\test\....>dir
 驱动器 F 中的卷是 test
 卷的序列号是 8E19-893E

 F:\test\.... 的目录

2020/12/06  14:48    <DIR>          .
2020/12/06  14:48    <DIR>          ..
2020/12/06  14:47    <DIR>          ....
2020/12/06  14:48                16 lalala.txt
               1 个文件             16 字节
               3 个目录     89,636,864 可用字节

F:\test\....>dir
```



CTF例题实战

找了几个NTFS流数据隐写的题目。

[ACTF新生赛2020]NTFS数据流

题目来源——BUUCTF
wp不写了，就是那两个工具的使用，关键在于理解知识。
这个是使用NtfsStreamsEditor工具扫描。
有两点，需要注意
1.解压需要使用winrar解压软件。
2.需要在win7系统中进行搜索。

猫片(安恒)

这个题目在bugkuCTF的misc分类中。最后会使用工具就OK。

喵喵喵

题目来源——BUUCTF，最后有个步骤是NTFS隐写。

总结

这次学到几点冷知识，有所收获，NTFS隐写也掌握了基本的原理及应用。

参考文章

https://xz.aliyun.com/t/2539
https://www.qingsword.com/qing/812.html
https://tyrant-k.github.io/2020/06/24/%E7%A1%AC%E7%9B%98%E5%8F%96%E8%AF%81-%E5%88%9D%E6%8E%A2NTFS%E9%9A%90%E5%86%99/
https://blog.csdn.net/alone_map/article/details/51851071
https://www.cnblogs.com/liuzhenbo/p/10925120.html
ww.cnblogs.com/liuzhenbo/p/10925120.html](https://www.cnblogs.com/liuzhenbo/p/10925120.html)