山东省ctf比赛之你真的很不错writeup

原创

Akong3916 于 2019-11-03 23:48:58 发布 499 收藏

分类专栏： CTF 文章标签： CTF 工具类 简单的工具使用

本文链接：https://blog.csdn.net/weixin_42861453/article/details/102877092

一、题目介绍

对于这么刺激好看的视频。。刚开始也没想法，后面发了个提示，“使用WinRAR解压”

突然 想起来前几天做的bugku的一道题

题目后面有NTFS，不知道什么意思，然后百度

专门用“winRAR”解压缩之后才可以产生流文件，后面找了一下别人写的介绍NTFS文件流的博客！

转载 **Windows中隐藏文件的捷径---------NTFS文件流(ADS)**

2019-06-12 13:33:42 weixin_34274029 阅读数 116

原文链接：https://my.oschina.net/dake/blog/196651

一、

1.在任一NTFS分区下打开CMD命令提示符，输入echo abcde>>a.txt:b.txt，则在当前目录下会生成一个名为a.txt的文件，但文件的大小为0字节，打开后也无任何内容，只有输入命令：notepad a.txt:b.txt 才能看见写入的abcde

2.在上边的命令中，a.txt可以不存在，也可以是某个已存的文件，文件格式无所谓，无论是.txt还是.jpg|.exe|.asp都行；
b.txt也可以任意指定文件名以及后缀名。（可以将任意文本信息隐藏于任意文件中，只要不泄露冒号后的虚拟文件名(即b.txt)，别人是根本不会查看到隐藏信息的）

3.包含隐藏信息的文件仍然可以继续隐藏其它的内容，对比上例，我们仍然可以使用命令echo 12345>>a.txt:c.txt 给a.txt建立新的隐藏信息的流文件，使用命令notepad a.txt:c.txt 打开后会发现12345这段信息，而abcde仍然存在于a.txt:b.txt中丝毫不受影响。

----------华丽不对称的分割线

二、隐藏文件

1.与上面大同小异，命令格式为type 文件名+后缀>>任意文件:任意文件名+原文件后缀，
比如：type 1.jpg>>2.abc:1.jpg
就是将1.jpg的内容写入到2.abc:1.jpg这个流文件中，2.abc可以随便换，1.jpg也可以随便，但是为了好记还是选择跟要隐藏的文件一样，最好是使用正常的文件，这样隐蔽性更强。

2.打开隐藏文件时注意，如果使用系统自带的，直接输入程序名就可以了，例如用画图工具打开2.abc:1.jpg是mspaint 2.abc:1.jpg
使用第三方软件打开的话则需要完整路径，例如用ACDSee9打开2.abc:1.jpg是ACDsee9.exe 盘符:/2.abc:1.jpg

注意：同样道理，其他文件也可以这样隐藏，只要打开时根据后缀名找对应的程序就行了，而且也可以像隐藏信息那样隐藏多个文件。
画图工具：mspaint
可执行程序exe：start

三、隐藏木马

1.与隐藏文件同理，type muma.exe>>2.jpg:muma.exe，将muma.exe写入到2.jpg:muma.exe这个流文件中，
打开的时候则：start 流文件绝对路径，上例是：start c:/2.jpg:muma.exe ；
不然会提示参数不正确。

---------- 华丽不对称的分割线

注意事项：

1.流文件不能直接通过网络传输，必须使用WinRAR在压缩时勾上高级选项中"保存文件流数据"才行。

2.制作好的流文件大小跟原文件是一样的，只在压缩后才包含隐藏文件的大小，说明NTFS文件流仍然会占用磁盘空间。

3.流文件只能在NTFS分区储存和运行(压缩"保存文件流数据"也可储存到FAT32，但解压出来的文件依然是丢失了数据流的文件)，一旦放到其它的文件系统中，即使再放回来，NTFS数据流也会丢失。

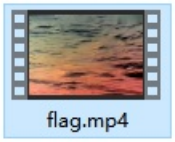
转载于:https://my.oschina.net/dake/blog/196651

简单来说就是用winRAR解压之后可以得到它里面隐藏的文件。说不定就是最终想要的东东~

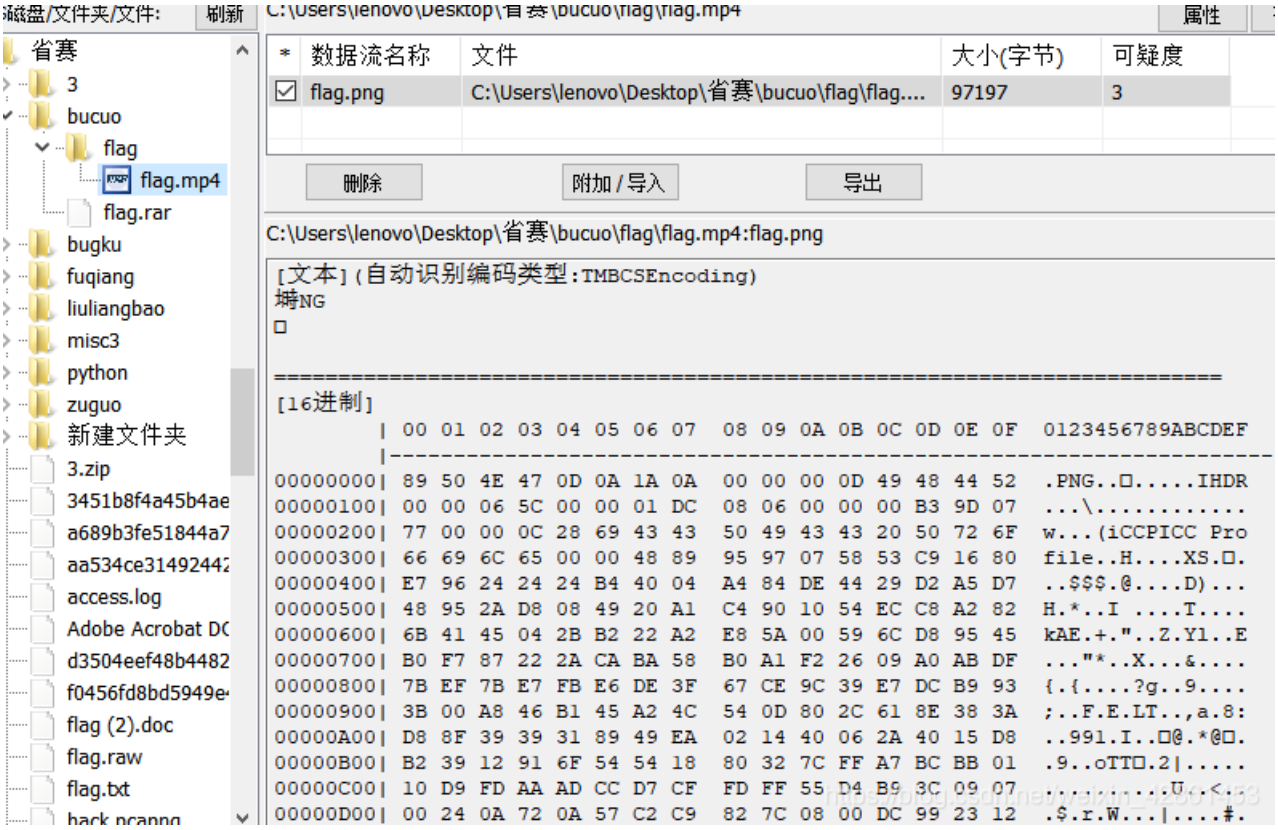
二、题目解答：

1、解压文件

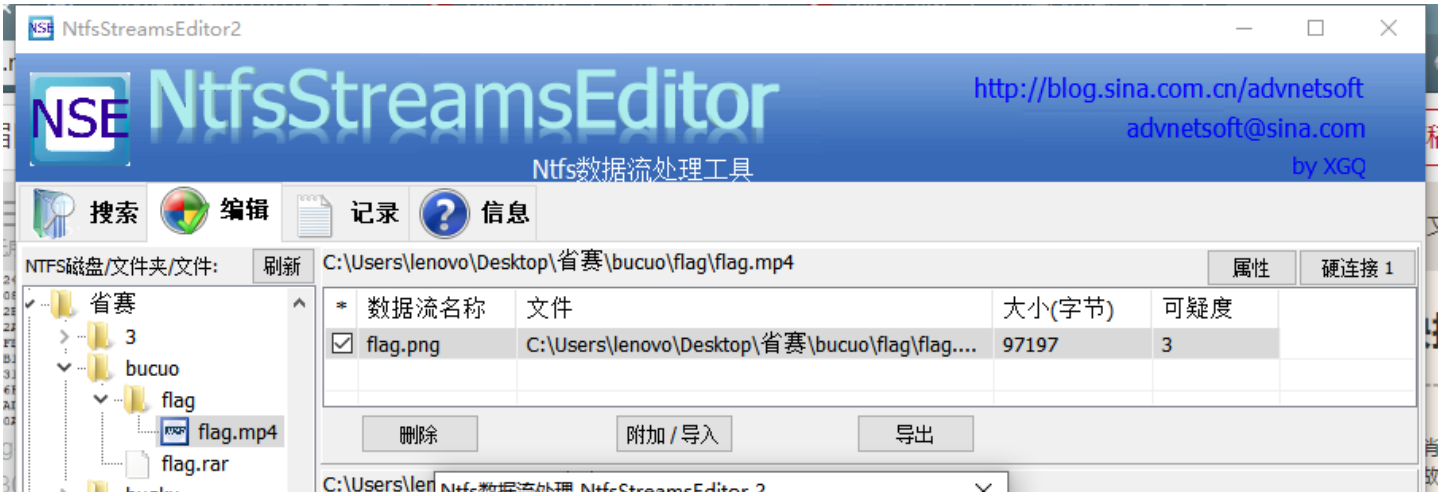
得到flag中的MP4文件

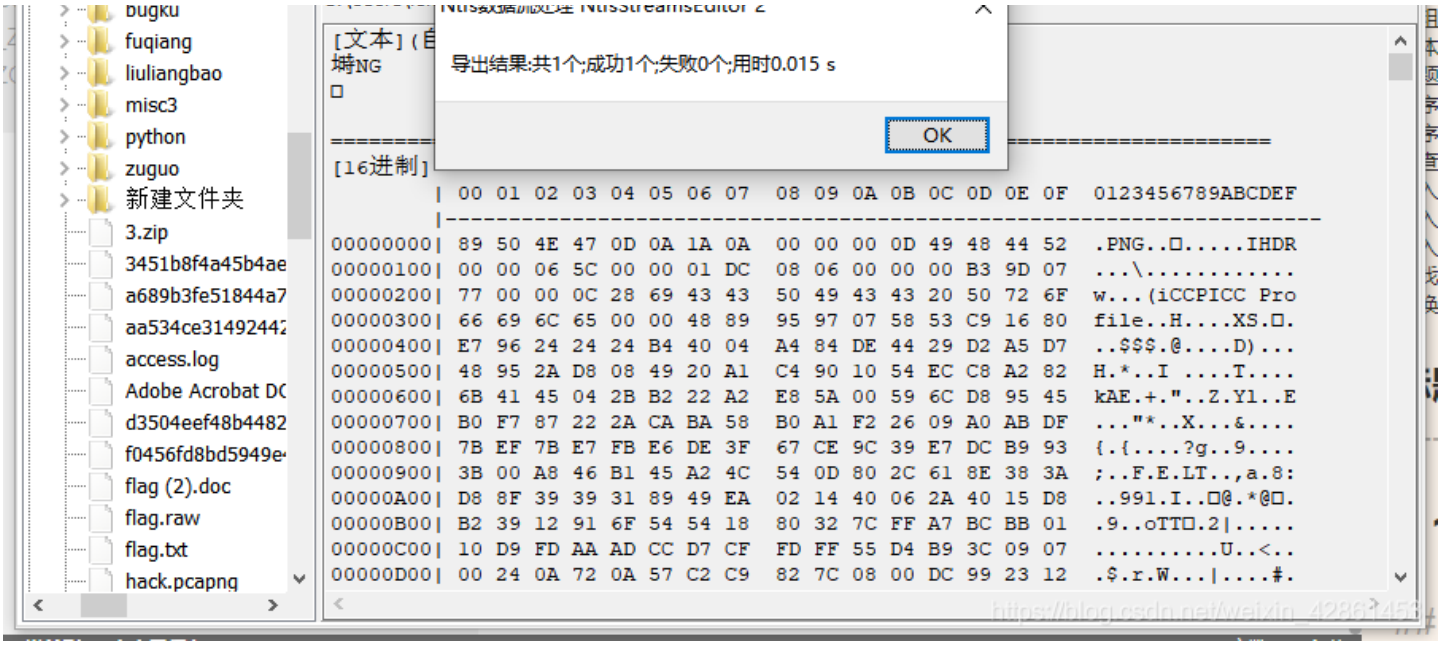


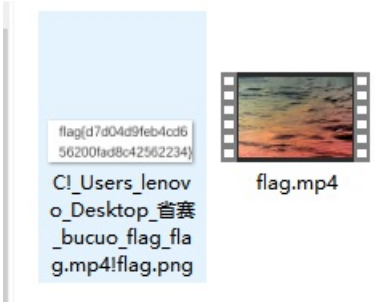
用ntfs数据流处理工具NtfsStreamsEditor打开解压缩的文件



点击文件下面的导出




bugku
fuqiang
liuliangbao
misc3
python
zuguo
新建文件夹
3.zip
3451b8f4a45b4ae
a689b3fe51844a7
aa534ce3149244
access.log
Adobe Acrobat DC
d3504eef48b4482
f0456fd8bd5949e
flag (2).doc
flag.raw
flag.txt
hack.pcapng
导出结果:共1个;成功1个;失败0个;用时0.015 s
OK
[16进制]
| 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00000000| 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 .PNG..□.....IHDR
00000100| 00 00 06 5C 00 00 01 DC 08 06 00 00 00 B3 9D 07 ...\............
00000200| 77 00 00 0C 28 69 43 43 50 49 43 43 20 50 72 6F w...(iCCPICC Pro
00000300| 66 69 6C 65 00 00 48 89 95 97 07 58 53 C9 16 80 file..H....XS.□.
00000400| E7 96 24 24 24 B4 40 04 A4 84 DE 44 29 D2 A5 D7 ..$$$.@....D)...
00000500| 48 95 2A D8 08 49 20 A1 C4 90 10 54 EC C8 A2 82 H.*..I ....T....
00000600| 6B 41 45 04 2B B2 22 A2 E8 5A 00 59 6C D8 95 45 kAE.+."..Z.Yl..E
00000700| B0 F7 87 22 2A CA BA 58 B0 A1 F2 26 09 A0 AB DF ..."*..X...&....
00000800| 7B EF 7B E7 FB E6 DE 3F 67 CE 9C 39 E7 DC B9 93 {.{....?g..9....
00000900| 3B 00 A8 46 B1 45 A2 4C 54 0D 80 2C 61 8E 38 3A ;..F.E.LT..,a.8:
00000A00| D8 8F 39 39 31 89 49 EA 02 14 40 06 2A 40 15 D8 ..991.I..□@.*@□.
00000B00| B2 39 12 91 6F 54 54 18 80 32 7C FF A7 BC BB 01 .9..oTT□.2|.....
00000C00| 10 D9 FD AA AD CC D7 CF FD FF 55 D4 B9 3C 09 07 ....U..<..
00000D00| 00 24 0A 72 0A 57 C2 C9 82 7C 08 00 DC 99 23 12 .$.r.W...|....#.


flag{d7d04d9feb4cd656200fad8c42562234}
C!_Users_lenovo_Desktop_省赛_bucuo_flag_flag.mp4!flag.png
flag.mp4

得到flag图片。