




BUUCTF：秘密文件

原创

末初  于 2020-10-04 22:05:27 发布  1087  收藏

分类专栏：[CTF_MISC_Writeup](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/mochu7777777/article/details/108923251>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址：<https://buuoj.cn/challenges#%E7%A7%98%E5%AF%86%E6%96%87%E4%BB%B6>

Challenge 525 Solves ×

秘密文件

1

深夜里，Hack偷偷的潜入了某公司的内网，趁着深夜偷走了公司的秘密文件，公司的网络管理员通过通过监控工具成功的截取Hack入侵时数据流量，但是却无法分析出Hack到底偷走了什么机密文件，你能帮帮管理员分析出Hack到底偷走了什么机密文件吗？注意：得到的flag 请包上 flag{} 提交

 3752a571-a...

Flag

<https://blog.csdn.net/mochu7777777>

这题和BUUCTF：被偷走的文件一模一样的套路

首先筛选一下 `ftp` 的流量包

No.	Time	Source	Destination	Protocol	Length	Info
15	3.227840	172.16.80.153	172.16.66.100	FTP	148	Response: 220 HI, i know you are a hacker who is trying to hack me ,but can u find where is the flag?a
19	4.595768	172.16.66.100	172.16.80.153	FTP	64	Request: USER ctf
20	4.596664	172.16.80.153	172.16.66.100	FTP	85	Response: 331 Password required for ctf
22	5.275482	172.16.66.100	172.16.80.153	FTP	64	Request: PASS ctf
23	5.276235	172.16.80.153	172.16.66.100	FTP	120	Response: 230 Client :ctf successfully logged in. Client IP :172.16.66.100
39	6.515671	172.16.66.100	172.16.80.153	FTP	81	Request: PORT 172,16,66,100,30,158
43	6.517125	172.16.80.153	172.16.66.100	FTP	84	Response: 200 Port command successful.
45	6.521033	172.16.66.100	172.16.80.153	FTP	60	Request: LIST
46	6.521626	172.16.80.153	172.16.66.100	FTP	114	Response: 150 Opening ASCII mode data connection for directory list.
52	6.522290	172.16.66.100	172.16.80.153	FTP	78	Response: 226 Transfer complete.
89	15.938534	172.16.66.100	172.16.80.153	FTP	81	Request: PORT 172,16,66,100,30,162
93	15.940030	172.16.80.153	172.16.66.100	FTP	84	Response: 200 Port command successful.
95	15.944953	172.16.66.100	172.16.80.153	FTP	97	Request: RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
96	15.945708	172.16.80.153	172.16.66.100	FTP	114	Response: 150 Opening BINARY mode data connection for file transfer.
101	15.946804	172.16.66.100	172.16.80.153	FTP	78	Response: 226 Transfer complete.
133	17.882257	172.16.66.100	172.16.80.153	FTP	60	Request: QUIT
134	17.882890	172.16.80.153	172.16.66.100	FTP	63	Response: 220 Bye

<https://blog.csdn.net/mochu777777>

追踪流

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng

```

220 HI, i know you are a hacker who is trying to hack me ,but can u find where is the flag?a
USER ctf
331 Password required for ctf
PASS ctf
230 Client :ctf successfully logged in. Client IP :172.16.66.100
PORT 172,16,66,100,30,158
200 Port command successful.
LIST
150 Opening ASCII mode data connection for directory list.
226 Transfer complete.
PORT 172,16,66,100,30,162
200 Port command successful.
RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete.
QUIT
220 Bye

```

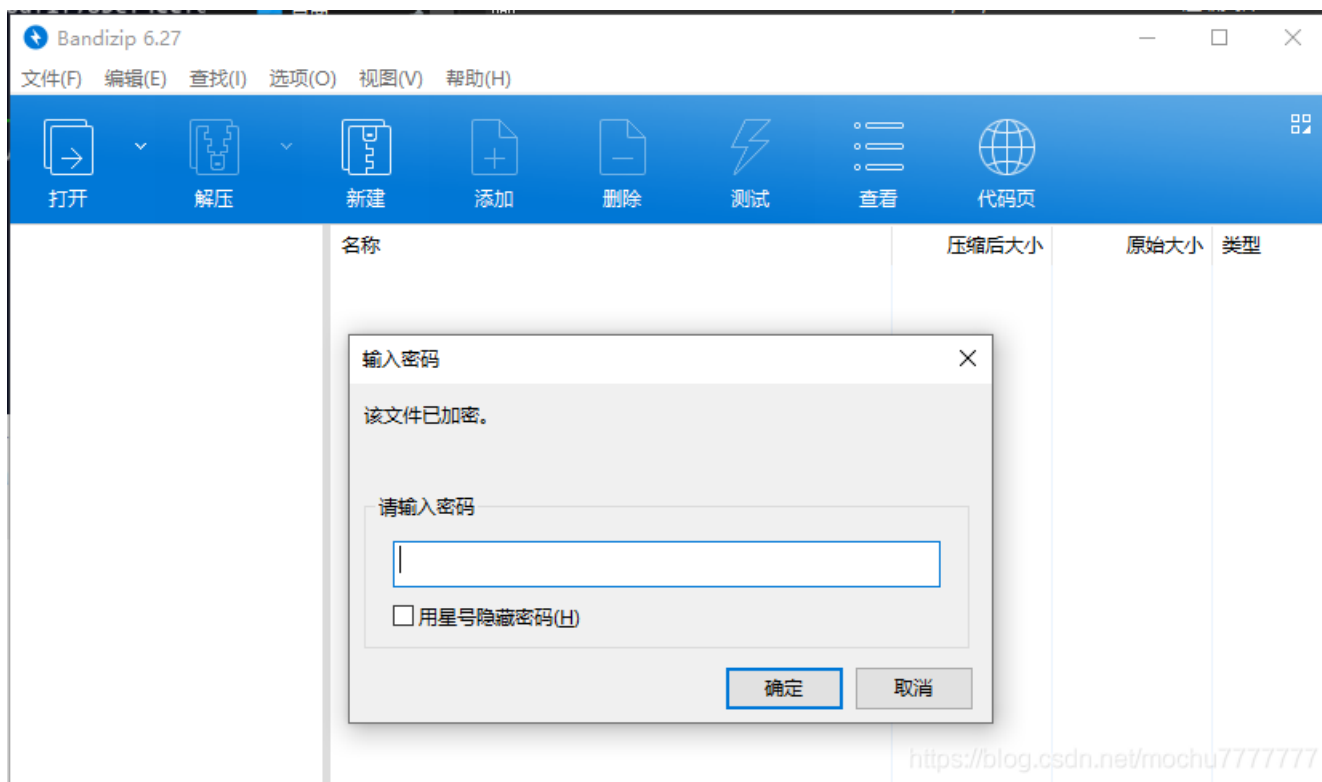
<https://blog.csdn.net/mochu777777>

发现传输了一个 rar 文件，使用 foremost 分离

```
m0c1nu7@Seanz7:/mnt/c/Users/Administrator$ cd Downloads/
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ ls
305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng 3752a571-aeb0-4881-9133-c983fe028fff.rar desktop.ini
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ foremost 305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng
Processing: 305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng
|*|
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ ls
305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng 3752a571-aeb0-4881-9133-c983fe028fff.rar desktop.ini output
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ tree output/
output/
├── audit.txt
├── rar
└── 00000031.rar

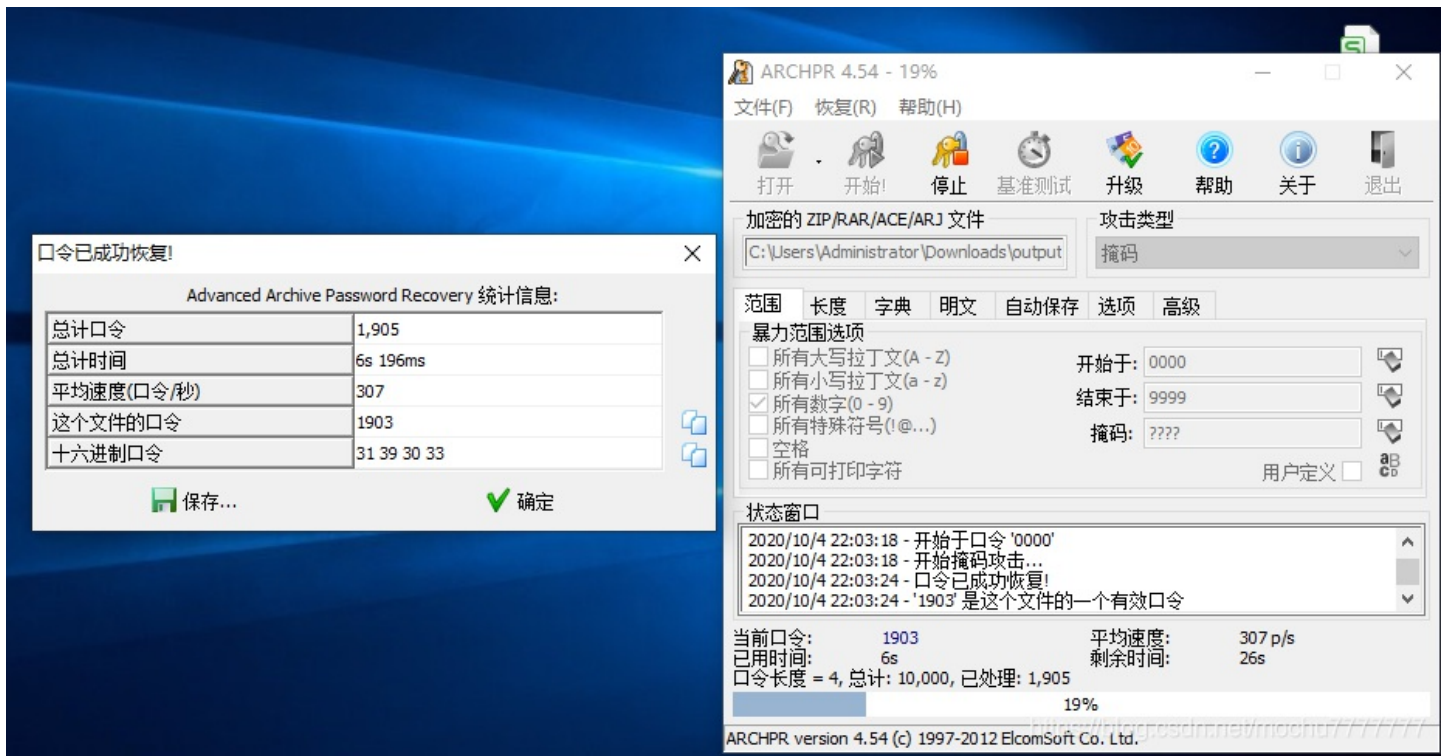
1 directory, 2 files
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ |
```

<https://blog.csdn.net/mochu777777>



<https://blog.csdn.net/mochu777777>

尝试 ARCHPR 四位数掩码爆破



密码: 1903

解压得到flag

```
flag{d72e5a671aa50fa5f400e5d10eedeaa5}
```



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)