

# Buuctf 秘密文件

原创

Dexret 于 2021-11-25 16:27:01 发布 659 收藏

分类专栏: [Buuctf Misc](#) 文章标签: [加密解密](#) [安全 misc](#)

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/Dexret/article/details/121540740>

版权



[Buuctf Misc](#) 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

下载该文件, 发现该文件为一个数据包

利用wireshark打开该文件

No.	Time	Source	Destination	Protocol	Info
1	0.00000000	172.16.66.100	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
2	0.58606700	172.16.66.100	223.5.5.5	DNS	Standard query PTR 100.66.16.172.in-addr.arpa
3	0.58958600	223.5.5.5	172.16.66.100	DNS	Standard query response, No such name
4	0.59490900	172.16.66.100	223.5.5.5	DNS	Standard query PTR 230.255.235.232.in-addr.arpa
5	0.59871100	223.5.5.5	172.16.66.100	DNS	Standard query response, No such name
6	1.22823870	172.16.66.100	223.5.5.5	DNS	Standard query PTR 5.5.5.223.in-addr.arpa
7	1.22823500	223.5.5.5	172.16.66.100	DNS	Standard query response PTR public1.alidns.com
8	2.61625500	172.16.66.100	223.5.5.5	DNS	Standard query A teredo.ipv6.microsoft.com
9	2.62055100	223.5.5.5	172.16.66.100	DNS	Standard query response, No such name CNAME teredo.ipv6.microsoft.com.nsatc.net
10	2.70221400	0c:da:41:9e:cc:91	LLDP_Multicast	LLDP	Chassis Id = 0c:da:41:9e:cc:84 Port Id = GigabitEthernet1/0/8 TTL = 120 System Name = 8F02-A12
11	3.00586700	172.16.66.100	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
12	3.22650500	172.16.66.100	172.16.80.153	TCP	7837 > ftp [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
13	3.22692500	172.16.80.153	172.16.66.100	TCP	ftp > 7837 [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1460 WS=0 SACK_PERM=1
14	3.22697100	172.16.66.100	172.16.80.153	TCP	7837 > ftp [ACK] Seq=1 Ack=1 win=8192 Len=0
15	3.22784000	172.16.80.153	172.16.66.100	FTP	Response: 220 Hi, I know you are a hacker who is trying to hack me ,but can u find where is the flag?
16	3.22790500	172.16.66.100	172.16.80.153	TCP	7837 > ftp [ACK] Seq=1 Ack=95 win=8096 Len=0
17	3.85643100	172.16.66.100	223.5.5.5	DNS	Standard query PTR 193.80.16.172.in-addr.arpa
18	3.86058100	223.5.5.5	172.16.66.100	DNS	Standard query response, No such name
19	4.59576800	172.16.66.100	172.16.80.153	FTP	Request: USER ctf
20	4.59666400	172.16.80.153	172.16.66.100	FTP	Response: 331 Password required for ctf
21	4.59677800	172.16.66.100	172.16.80.153	TCP	7837 > ftp [ACK] Seq=11 Ack=126 win=8064 Len=0

Frame 20: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)  
Ethernet II, Src: 0c:da:41:9e:cc:85 (0c:da:41:9e:cc:85), Dst: 20:89:84:32:73:c5 (20:89:84:32:73:c5)  
Internet Protocol, Src: 172.16.80.153 (172.16.80.153), Dst: 172.16.66.100 (172.16.66.100)  
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 7837 (7837), Seq: 95, Ack: 11, Len: 31  
File Transfer Protocol (FTP)

```
0000  20 89 84 32 73 c5 0c da 41 9e cc 85 08 00 45 00  ..2s... A....E.
0010  00 47 5f e6 40 00 7f 06 b0 ac ac 10 50 99 ac 10  .G..@... ..P...
0020  42 64 00 15 1e 9d 04 b0 0a b6 50 34 f9 a5 50 18  Bd..... .P4..P.
0030  ff f5 bc c6 00 00 33 33 31 20 50 61 73 73 77 6f  ....33 1 Passwo
0040  72 64 20 72 65 71 75 69 72 65 64 20 66 6f 72 20  rd requi red for
0050  ctf
```

结合题意, 发现该题需要我们查询被盗取的文件是什么

过滤ftp数据包

305df1f78bef4ccfd2a3bd0fe4a6cd7.pcapng - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: ftp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
15	3.22784000	172.16.80.153	172.16.66.100	FTP	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	4.59576800	172.16.66.100	172.16.80.153	FTP	Request: USER ctf
20	4.59666400	172.16.80.153	172.16.66.100	FTP	Response: 331 Password required for ctf
23	5.27623500	172.16.80.153	172.16.66.100	FTP	Request: PASS ctf
23	5.27623500	172.16.80.153	172.16.66.100	FTP	Response: 230 Client :ctf successfully logged in. Client IP :172.16.66.100
39	6.51567100	172.16.66.100	172.16.80.153	FTP	Request: PORT 172,16,66,100,30,158
43	6.51712500	172.16.80.153	172.16.66.100	FTP	Response: 200 Port command successful.
45	6.52103300	172.16.66.100	172.16.80.153	FTP	Request: LIST
46	6.52162600	172.16.80.153	172.16.66.100	FTP	Response: 150 opening ASCII mode data connection for directory list.
52	6.52229800	172.16.80.153	172.16.66.100	FTP	Response: 226 Transfer complete.
89	15.93853400	172.16.66.100	172.16.80.153	FTP	Request: PORT 172,16,66,100,30,162
93	15.94003000	172.16.80.153	172.16.66.100	FTP	Response: 200 Port command successful.
95	15.94495300	172.16.66.100	172.16.80.153	FTP	Request: RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
96	15.94570800	172.16.80.153	172.16.66.100	FTP	Response: 150 opening BINARY mode data connection for file transfer.
101	15.94608400	172.16.80.153	172.16.66.100	FTP	Response: 226 Transfer complete.
133	17.88225700	172.16.66.100	172.16.80.153	FTP	Request: QUIT
134	17.88289000	172.16.80.153	172.16.66.100	FTP	Response: 220 Bye

Frame 20: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)

Ethernet II, Src: 0c:da:41:9e:cc:85 (0c:da:41:9e:cc:85), Dst: 20:89:84:32:73:c5 (20:89:84:32:73:c5)

Internet Protocol, Src: 172.16.80.153 (172.16.80.153), Dst: 172.16.66.100 (172.16.66.100)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 7837 (7837), Seq: 95, Ack: 11, Len: 31

File Transfer Protocol (FTP)

```

0000  20 89 84 32 73 c5 0c da 41 9e cc 85 08 00 45 00  ..2s... A.....E.
0010  00 47 5f e6 40 00 7f 06 b0 ac ac 10 50 99 ac 10  .G..@... ..P...
0020  42 64 00 15 1e 9d 04 b0 0a b6 50 34 f9 a5 50 18  Bd..... .P..P.
0030  ff f5 bc c6 00 00 33 33 31 20 50 61 73 73 77 6f  .....33 1 Passwo
0040  72 64 20 72 65 71 75 69 72 65 64 20 66 6f 72 20  rd requi red for
0050  62 71 66 04 02 00 00 00 00 00 00 00 00 00 00 00  ctf

```

File: "C:\Users\136831\Desktop\305df1f7... Packets: 200 Displayed: 17 Marked: 0 Load time: 0:00:005 Profiler: Default CSDN@Dexret

选择一条数据包进行数据流追踪

Follow TCP Stream

Stream Content

```

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

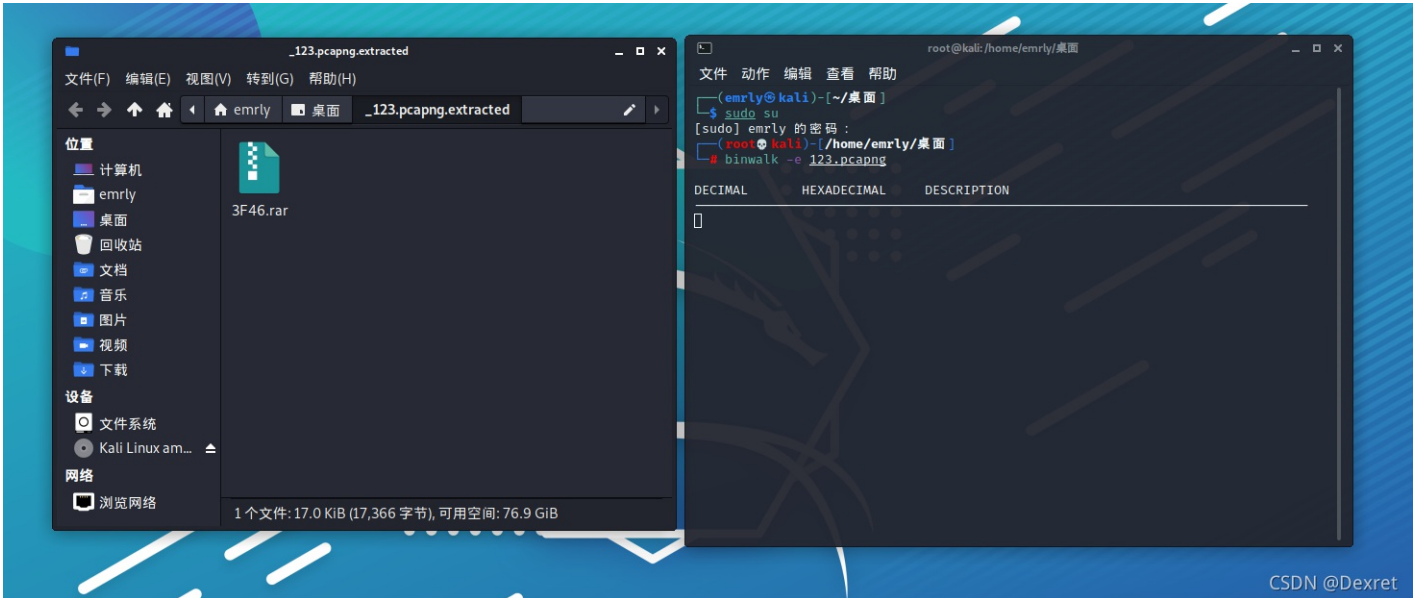
```

Find Save As Print Entire conversation (557 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close CSDN@Dexret

在这里查看到被盗取的文件为rar文件

利用kail中的binwalk对该数据包进行文件分离



分离后得到一个rar文件包，但是该rar文件包解压时需要密码

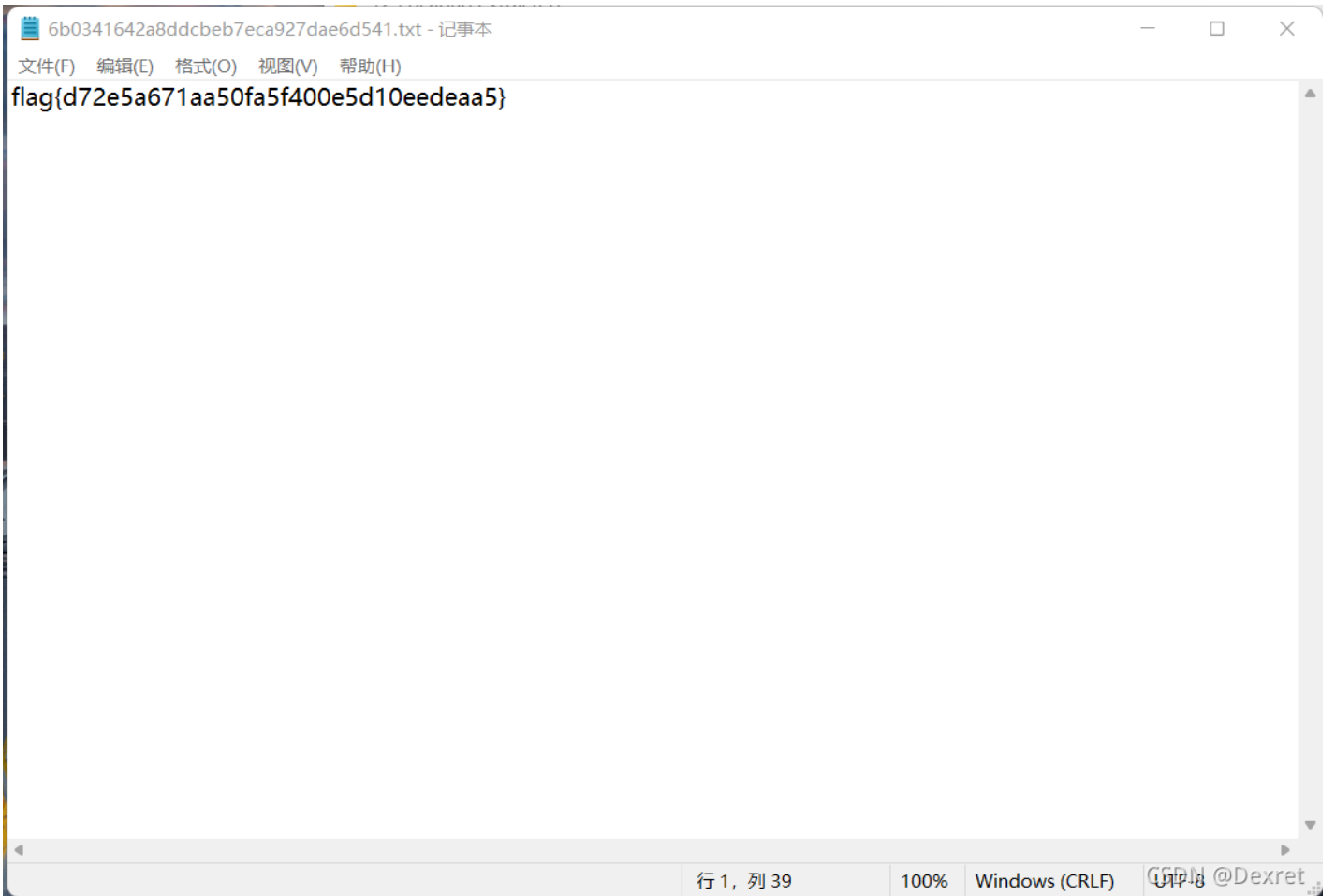
通过ARCHPR对该数据包进行密码爆破



得到该压缩包的密码为：1903

利用爆破后的密码解压该压缩包，发现里面有一个txt文件

打开该文件得到该题的flag



flag{d72e5a671aa50fa5f400e5d10eedeaa5}