

【XCTF 攻防世界】MISC 杂项 高手进阶区 就在其中

原创

Kali 于 2020-08-13 17:38:17 发布 675 收藏 1

分类专栏: [CTF刷题 杂项](#) 文章标签: [安全](#) [openssl](#) [加密解密](#)

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/weixin_45844670/article/details/107985213

版权



[CTF刷题 杂项 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

题目链接: <https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4925&page=2>

下载链接得到一个流量包

刚开始想用解压软件看看有没有什么隐藏文件, 结果发现只有一个key.txt

但是用了好多编码方法都不对

于是打算用流量包看看

□□沙?□顔f□q鯧?:\□榘□38 摸踣?月簪劔幽?軚觀□ 醇h~M牀d護□闕□U€\$ 莓猎□□燉醜-□挑忡?叔則趁C??场3?漚虛m

搜索flag.txt, 无果

分组详情 宽窄 区分大小写 字符串 flag.txt

No.	Time	Source	Destination	Protocol	Length	Info
358	25.070226	192.168.1.108	192.168.1.106	FTP-D...	957	FTP Data: 891 bytes (PASV) (RETR /abc/test.key)
353	25.069525	192.168.1.106	192.168.1.108	TCP	74	54430 → 50068 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=17579295 TS...
354	25.069622	192.168.1.108	192.168.1.106	TCP	74	50068 → 54430 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
355	25.069742	192.168.1.106	192.168.1.108	TCP	66	54430 → 50068 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=17579295 TSecr=6729513
359	25.070346	192.168.1.106	192.168.1.108	TCP	66	54430 → 50068 [ACK] Seq=1 Ack=892 Win=32768 Len=0 TSval=17579296 TSecr=6729513
360	25.070398	192.168.1.108	192.168.1.106	TCP	66	50068 → 54430 [FIN, ACK] Seq=892 Ack=1 Win=66560 Len=0 TSval=6729513 TSecr=17579...
362	25.070633	192.168.1.106	192.168.1.108	TCP	66	54430 → 50068 [FIN, ACK] Seq=1 Ack=893 Win=32768 Len=0 TSval=17579296 TSecr=6729...
364	25.070658	192.168.1.108	192.168.1.106	TCP	66	50068 → 54430 [ACK] Seq=893 Ack=2 Win=66560 Len=0 TSval=6729513 TSecr=17579296

> Frame 359: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{8A216302-F1F4-4A27-AE6B-0427A8D87FB6}, id 0
 > Ethernet II, Src: IntelCor_1c:d1:80 (60:6c:66:1c:d1:80), Dst: PcsCompu_91:15:27 (08:00:27:91:15:27)
 > Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.108
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x1bd8 (7128)
 > Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64

```

0000 08 00 27 91 15 27 60 6c 66 1c d1 80 08 00 45 00  ... ..l f....E-
0010 00 34 1b d8 40 00 40 06 9a c5 c0 a8 01 6a c0 a8  -4..@. ....j..
0020 01 6c d4 9e c3 94 dd c1 26 ca b6 04 b9 f6 80 10  -1.....&.....
0030 00 20 f7 ff 00 00 01 01 08 0a 01 0c 3d 20 00 66  .....=..f
0040 af 29
  
```

无分组的解析视图包含该字符串。 分组: 705 · 已显示: 8 (1.1%)

分析流量包发现大部分都是ftp协议，猜测传输的文件中有和flag有关的信息

搜索刚才得到的key，看到

应用显示过滤器 <Ctrl-/>

分组详情 宽窄 区分大小写 字符串 key

No.	Time	Source	Destination	Protocol	Length	Info
49	6.879190	192.168.1.108	192.168.1.106	FTP-D...	433	FTP Data: 367 bytes (PASV) (LIST -1)
50	6.879307	192.168.1.106	192.168.1.108	TCP	66	42284 → 50062 [ACK] Seq=1 Ack=368 Win=30720 Len=0 TSval=17574748 T...
51	6.879371	192.168.1.108	192.168.1.106	TCP	66	50062 → 42284 [FIN, ACK] Seq=368 Ack=1 Win=66560 Len=0 TSval=67276...
52	6.879503	192.168.1.108	192.168.1.106	FTP	90	Response: 226 Transfer complete.
53	6.882745	192.168.1.106	192.168.1.108	TCP	66	42284 → 50062 [FIN, ACK] Seq=1 Ack=369 Win=30720 Len=0 TSval=17574...
54	6.882748	192.168.1.106	192.168.1.108	TCP	66	55820 → 21 [RST, ACK] Seq=88 Ack=326 Win=29696 Len=0 TSval=1757474...
55	6.882801	192.168.1.108	192.168.1.106	TCP	66	50062 → 42284 [ACK] Seq=369 Ack=2 Win=66560 Len=0 TSval=6727694 T...
56	8.432454	fe80::2507:f...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
57	8.434314	fe80::2507:f...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
58	8.846398	192.168.1.106	192.168.1.108	TCP	74	55824 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
59	8.846470	192.168.1.108	192.168.1.106	TCP	74	21 → 55824 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 S...
60	8.846596	192.168.1.106	192.168.1.108	TCP	66	55824 → 21 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=17575240 TSecr=...
61	8.846842	192.168.1.108	192.168.1.106	FTP	93	Response: 220 Microsoft FTP Service
62	8.846909	192.168.1.106	192.168.1.108	TCP	66	55824 → 21 [ACK] Seq=1 Ack=28 Win=29696 Len=0 TSval=17575240 TSecr=...
63	8.846975	192.168.1.106	192.168.1.108	FTP	82	Request: USER anonymous
64	8.847034	192.168.1.108	192.168.1.106	FTP	104	Response: 331 Password required for anonymous.

Command frame: 47
 [Current working directory: /abc/]
 > Line-based text data (7 lines)
 03-12-16 12:20PM 142588562 IDA Pro 6.5 Setup.exe\r\n
 08-09-16 11:15AM 128 key.txt\r\n
 08-10-16 11:29AM 240 key.zip\r\n
 08-09-16 11:12AM 272 pub.key\r\n
 08-09-16 11:11AM 891 test.key\r\n
 04-15-16 10:38PM 7357556 鯊-■■■■■■.pdf\r\n
 04-15-16 10:38PM 9871783 鯊-■■■■■■.pdf\r\n

https://blog.csdn.net/weixin_45844670

pub.key

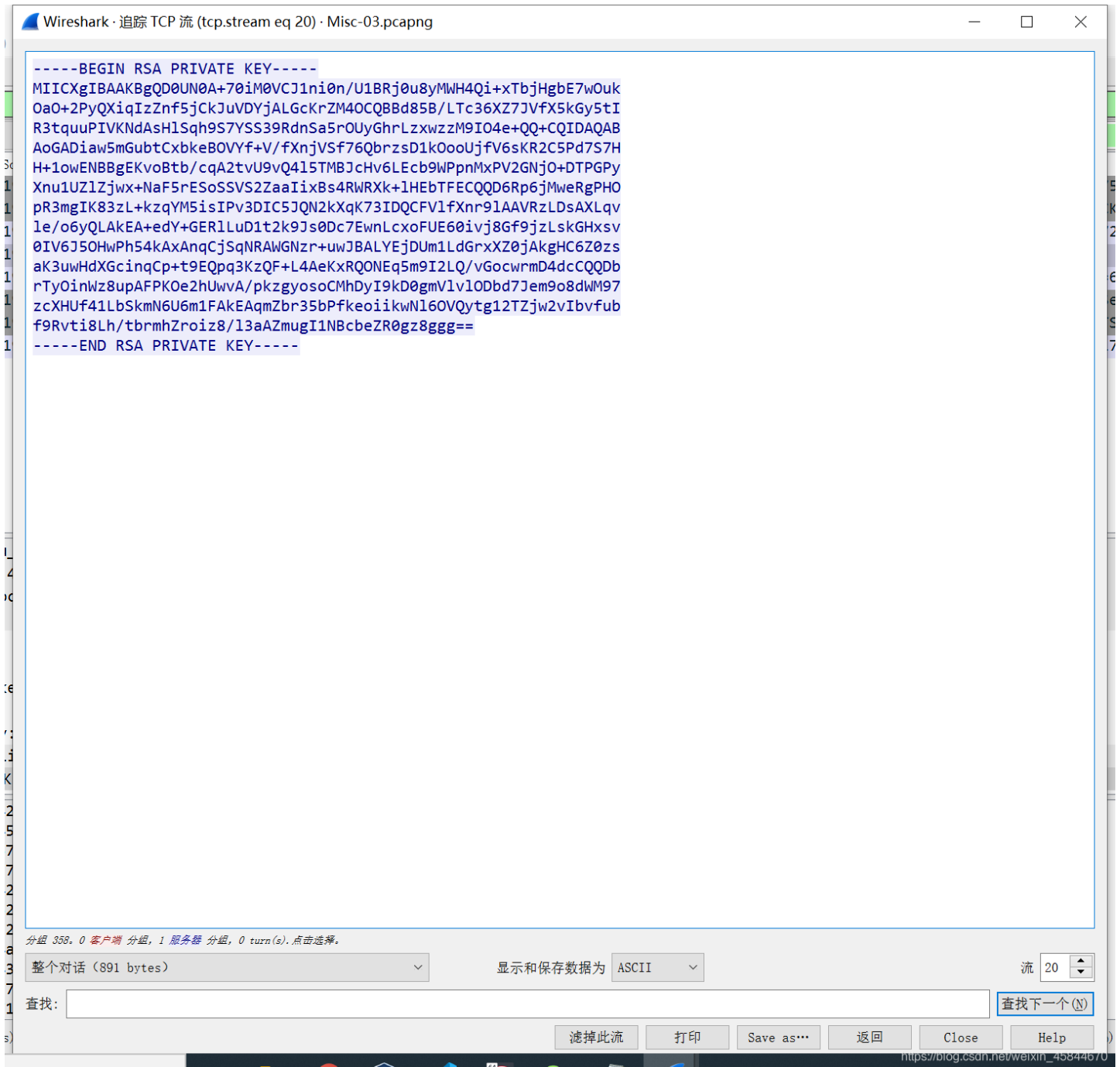
想到rsa加密

那么key.txt不能打开就有可能是因为加密过了

那我们来找一下私钥

搜索RSA或者PRVATE这些关键字

然后追踪tcp流可以得到:



把上面的内容复制出来

存为rsa.key文件

放到kali的openssl进行解密

```
openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
-in 为要解密的加密文档 -inkey 为密钥 -out 为输出文档
```

得到flag

File Edit Search View Document Help

Warning, you are using the root account, you may harm your system.

```
hi, boys and girls! flag is {haPPy_Use_0penSsI}
```