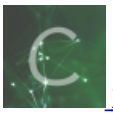
XCTF练习题---MISC---就在其中

原创

Hskb 于 2021-06-28 15:27:09 发布 109 收藏

分类专栏： XCTF 文章标签： 安全

本文链接：https://blog.csdn.net/liu914589417/article/details/118304155



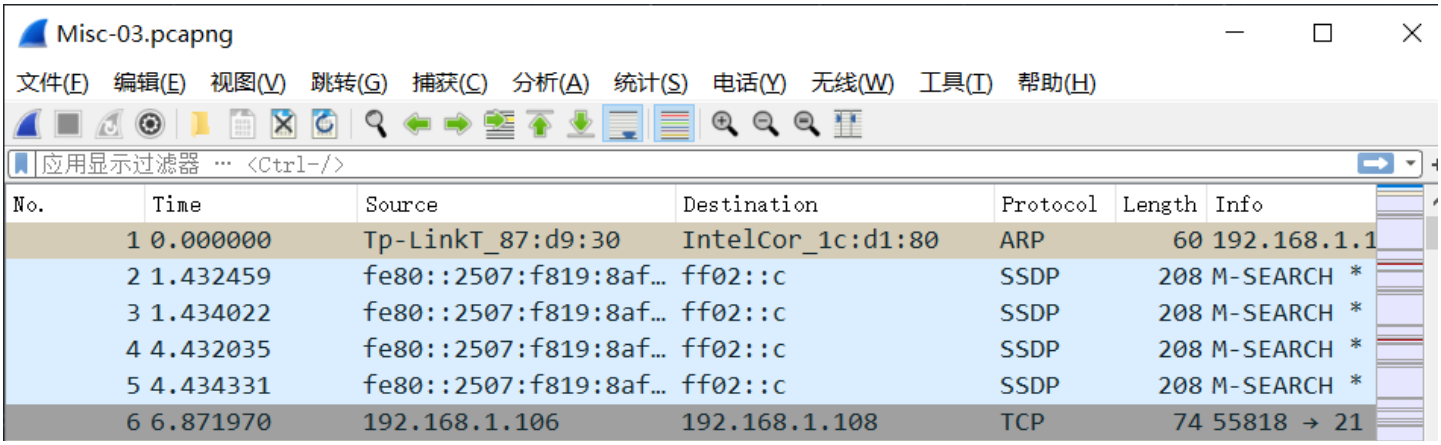
XCTF练习题—MISC—就在其中

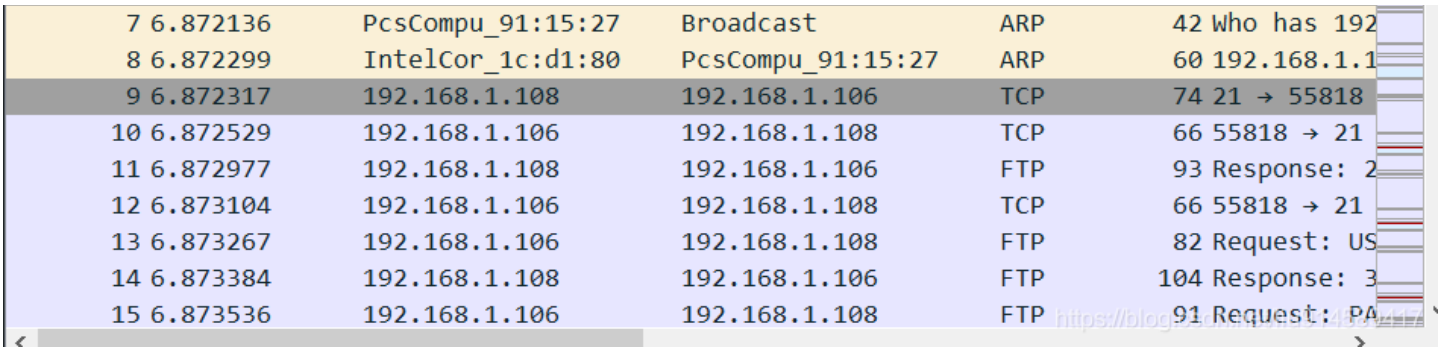
flag：flag{haPPy_Use_0penSsl}

解题步骤：

1、观察题目，下载附件

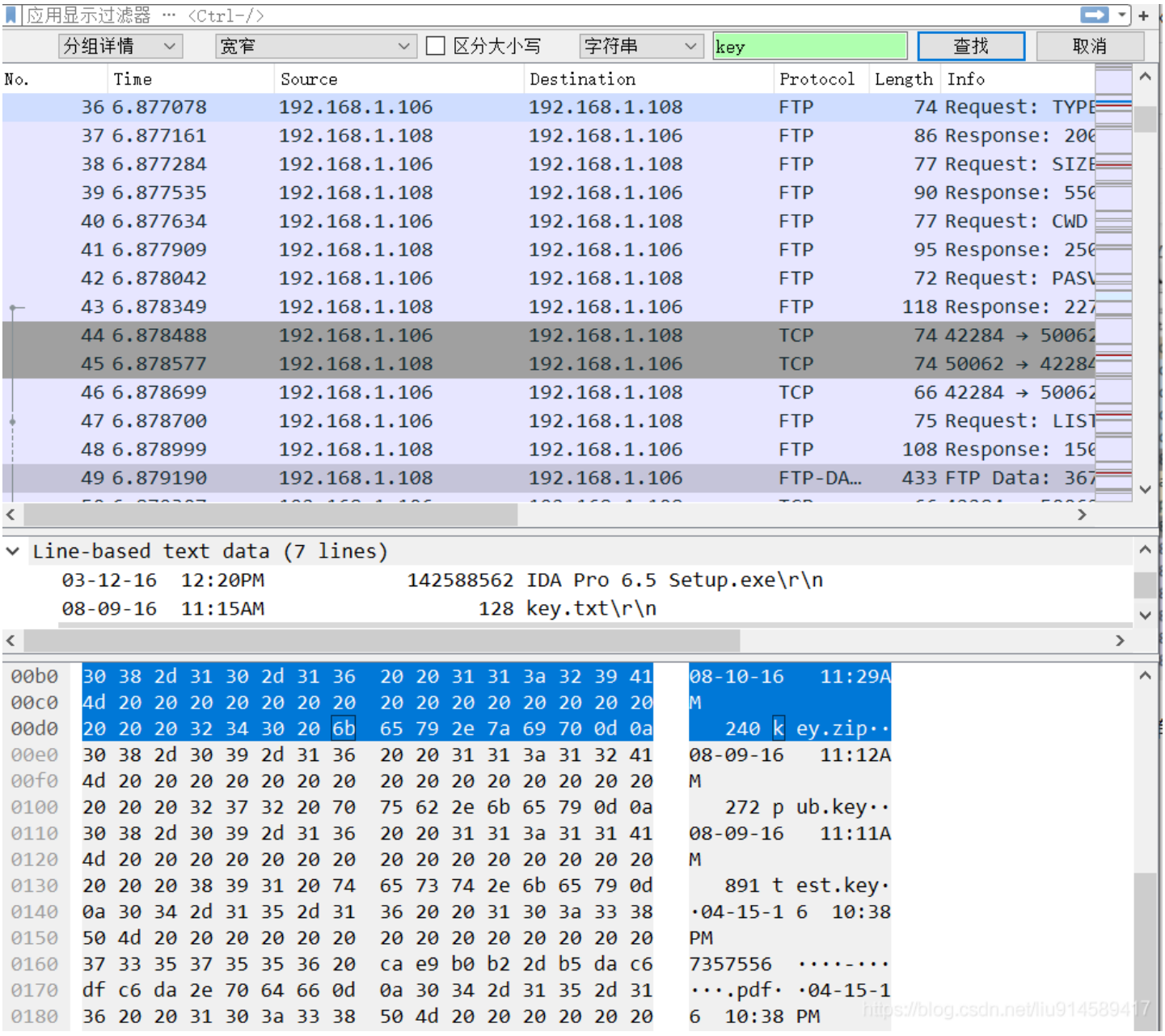
2、拿到手以后发现是一个数据包格式，直接上Wireshark查看相关数据





7	6.872136	PcsCompu_91:15:27	Broadcast	ARP	42 Who has 192
8	6.872299	IntelCor_1c:d1:80	PcsCompu_91:15:27	ARP	60 192.168.1.1
9	6.872317	192.168.1.108	192.168.1.106	TCP	74 21 → 55818
10	6.872529	192.168.1.106	192.168.1.108	TCP	66 55818 → 21
11	6.872977	192.168.1.108	192.168.1.106	FTP	93 Response: 2
12	6.873104	192.168.1.106	192.168.1.108	TCP	66 55818 → 21
13	6.873267	192.168.1.106	192.168.1.108	FTP	82 Request: US
14	6.873384	192.168.1.108	192.168.1.106	FTP	104 Response: 3
15	6.873536	192.168.1.106	192.168.1.108	FTP	91 Request: PA

3、这么多数据，直接尝试搜索flag.txt，结果并没有发现什么有价值的信息，换个思路试着搜索一下key，果然得到了有价值的信息



应用显示过滤器 … <Ctrl-/>

分组详情 | 宽窄 | 区分大小写 | 字符串 | key | 查找 | 取消

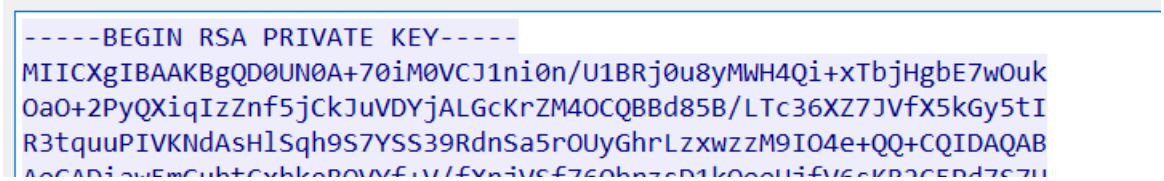
No.	Time	Source	Destination	Protocol	Length	Info
36	6.877078	192.168.1.106	192.168.1.108	FTP	74	Request: TYPE
37	6.877161	192.168.1.108	192.168.1.106	FTP	86	Response: 200
38	6.877284	192.168.1.106	192.168.1.108	FTP	77	Request: SIZE
39	6.877535	192.168.1.108	192.168.1.106	FTP	90	Response: 550
40	6.877634	192.168.1.106	192.168.1.108	FTP	77	Request: CWD
41	6.877909	192.168.1.108	192.168.1.106	FTP	95	Response: 250
42	6.878042	192.168.1.106	192.168.1.108	FTP	72	Request: PASV
43	6.878349	192.168.1.108	192.168.1.106	FTP	118	Response: 227
44	6.878488	192.168.1.106	192.168.1.108	TCP	74	42284 → 50062
45	6.878577	192.168.1.108	192.168.1.106	TCP	74	50062 → 42284
46	6.878699	192.168.1.106	192.168.1.108	TCP	66	42284 → 50062
47	6.878700	192.168.1.106	192.168.1.108	FTP	75	Request: LIST
48	6.878999	192.168.1.108	192.168.1.106	FTP	108	Response: 150
49	6.879190	192.168.1.108	192.168.1.106	FTP-DA…	433	FTP Data: 367

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
```

```
00b0  30 38 2d 31 30 2d 31 36  20 20 31 31 3a 32 39 41   08-10-16   11:29A
00c0  4d 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20   M
00d0  20 20 20 32 34 30 20 6b  65 79 2e 7a 69 70 0d 0a      240 k ey.zip··
00e0  30 38 2d 30 39 2d 31 36  20 20 31 31 3a 31 32 41   08-09-16   11:12A
00f0  4d 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20   M
0100  20 20 20 32 37 32 20 70  75 62 2e 6b 65 79 0d 0a      272 p ub.key··
0110  30 38 2d 30 39 2d 31 36  20 20 31 31 3a 31 31 41   08-09-16   11:11A
0120  4d 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20   M
0130  20 20 20 38 39 31 20 74  65 73 74 2e 6b 65 79 0d      891 t est.key·
0140  0a 30 34 2d 31 35 2d 31  36 20 20 31 30 3a 33 38   ·04-15-1 6  10:38
0150  50 4d 20 20 20 20 20 20  20 20 20 20 20 20 20 20   PM
0160  37 33 35 37 35 35 36 20  ca e9 b0 b2 2d b5 da c6   7357556  ····-···
0170  df c6 da 2e 70 64 66 0d  0a 30 34 2d 31 35 2d 31   ····.pdf·  ·04-15-1
0180  36 20 20 31 30 3a 33 38  50 4d 20 20 20 20 20 20   6  10:38 PM
```

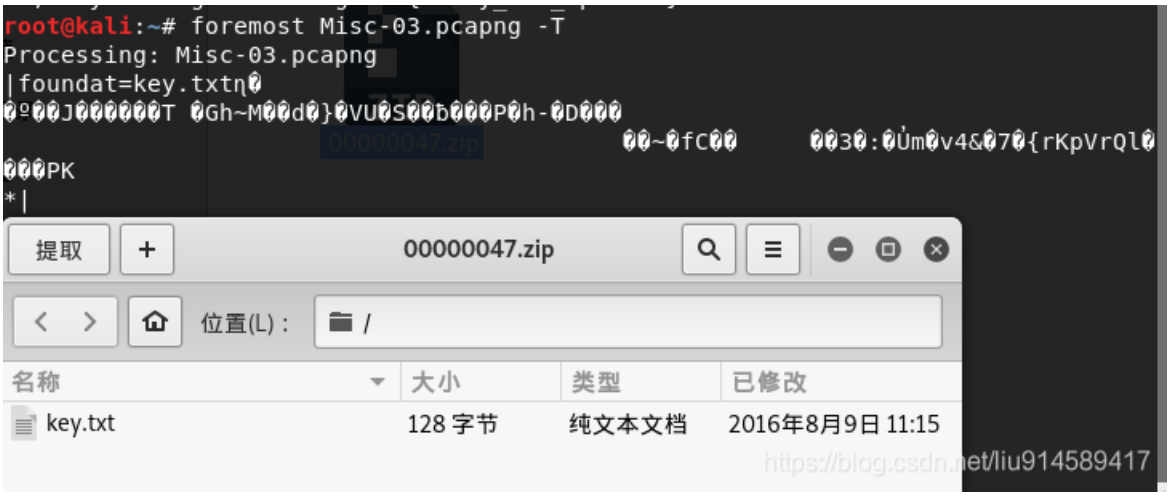
4、发现了一个pub.key，感觉有点像RSA加密？，先找到再说，直接搜索RSA追踪TCP流看看



```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj0u8yMWH4Qi+xTbjHgbE7wOuk
OaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBBd85B/LTc36XZ7JVfX5kGy5tI
R3tquuPIVKNdAsHlSqh9S7YSS39RdnSa5rOUyGhrLzxwzzM9IO4e+QQ+CQIDAQAB
```

```
H+1owENBBgEKvoBtb/cqA2tvU9vQ4l5TMBJcHv6LEcb9WPpnMxPV2GNjO+DTPGPy
Xnu1UZlZjwx+NaF5rESoSSVS2ZaaIixBs4RWRXk+lHEbTFECQQD6Rp6jMweRgPHO
pR3mgIK83zL+kzqYM5isIPv3DIC5JQN2kXqK73IDQCFVlfXnr9lAAVRzLDsAXLqv
le/o6yQLAkEA+edY+GERlLuD1t2k9Js0Dc7EwnLcxoFUE60ivj8Gf9jzLskGHxsv
0IV6J5OHwPh54kAxAnqCjSqNRAWGNzr+uwJBALYEjDUm1LdGrxXZ0jAkgHC6Z0zs
aK3uwHdXGcinqCp+t9EQpq3KzQF+L4AeKxRQONEq5m9I2LQ/vGocwrmD4dcCQQDb
rTyOinWz8upAFPKOe2hUwvA/pkzgyosoCMhDyI9kD0gmVlvlODbd7Jem9o8dWM97
zcXHUf41LbSkmN6U6m1FAkEAqmZbr35bPfkeoiikwNl6OVQytg12TZjw2vIbvfub
f9Rvti8Lh/tbrmhZroiz8/l3aAZmugI1NBcbeZR0gz8ggg==
-----END RSA PRIVATE KEY-----
```


5、把这个RSA密钥保存为rsa.key文件，准备上Kali进行破解，在刚刚找到的信息中发现有key.txt文件，直接上Kali的foremost分离原数据包



6、接下来手里有rsa.key的文件了（密钥），也有key.txt的密文了，上命令进行破解，得到flag，查看flag文件即可啦

命令：openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt

```
root@kali:~# openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
root@kali:~# cat flag.txt
hi,boys and girls! flag is {haPPy_Use_0penSsI}
root@kali:~#
```

7、提交答案，完成

知乎地址：https://www.zhihu.com/people/yi-kuai-xiao-bing-gan-43-64/posts
博客园地址：https://www.cnblogs.com/redHskb/
欢迎关注评论，耶斯莫拉