

xctf攻防世界 MISC高手进阶区 就在其中

原创

18947943 于 2022-01-17 11:45:45 发布 6132 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [安全](#) [web安全](#)

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/18947943/article/details/122535932>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境, 下载附件

题目给出的是一个pcapng流量包, 果断使用wireshark打开, 如图:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Tp-LinkT_87:d9:30	IntelCor_1c:d1:80	ARP	60	192.168.1.1 is at bc:d1:77:87:d9
2	1.432459	fe80::2507:f819:8af...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3	1.434022	fe80::2507:f819:8af...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
4	4.432035	fe80::2507:f819:8af...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
5	4.434331	fe80::2507:f819:8af...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
6	6.871970	192.168.1.106	192.168.1.108	TCP	74	55818 → 21 [SYN] Seq=0 Win=29200
7	6.872136	PcsCompu_91:15:27	Broadcast	ARP	42	Who has 192.168.1.106? Tell 192.

> Frame 2: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{8A216302-F1F4-4A2...}

> Ethernet II, Src: PcsCompu_91:15:27 (08:00:27:91:15:27), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

> Internet Protocol Version 6, Src: fe80::2507:f819:8af1:c603, Dst: ff02::c

> User Datagram Protocol, Src Port: 53449, Dst Port: 1900

> Simple Service Discovery Protocol

```
0000 33 33 00 00 00 0c 08 00 27 91 15 27 86 dd 60 00 33.....'...'..
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 25 07 .....%
0020 f8 19 8a f1 c6 03 ff 02 00 00 00 00 00 00 00 .....
0030 00 00 00 00 00 0c d0 c9 07 6c 00 9a 58 7f 4d 2d .....1..X.M-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [FF02::C
0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e 3a 4d ]:1900.. ST:urn:M
0070 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 icrosoft Windows
0080 20 50 65 65 72 20 4e 61 6d 65 20 52 65 73 6f 6c Peer Na me Resol
0090 75 74 69 6f 6e 20 50 72 6f 74 6f 63 6f 6c 3a 20 ution Pr otocol:
00a0 56 34 3a 49 50 56 36 3a 4c 69 6e 6b 4c 6f 63 61 V4:IPV6: LinkLoca
```

观察了一番, 搜索关键词flag, ctf没有任何提示。没有思路, 我们分组点点, 追踪流试试

2. 问题分析

尝试追踪流

一通尝试后，观察流量包，如图：

The image shows a Wireshark interface with a packet list and a details pane. A red box highlights the 'tcp.stream eq 2' filter. A secondary window titled 'Wireshark · 追踪 TCP 流 (tcp.stream eq 2) · Misc-03.pcapng' is open, displaying a list of files transferred over the stream. The files are:

Time	Size	Filename
03-12-16 12:20PM	142588562	IDA Pro 6.5 Setup.exe
08-09-16 11:15AM	128	key.txt
08-10-16 11:29AM	240	key.zip
08-09-16 11:12AM	272	pub.key
08-09-16 11:11AM	891	test.key
04-15-16 10:38PM	7357556pdf
04-15-16 10:38PM	9871783pdf

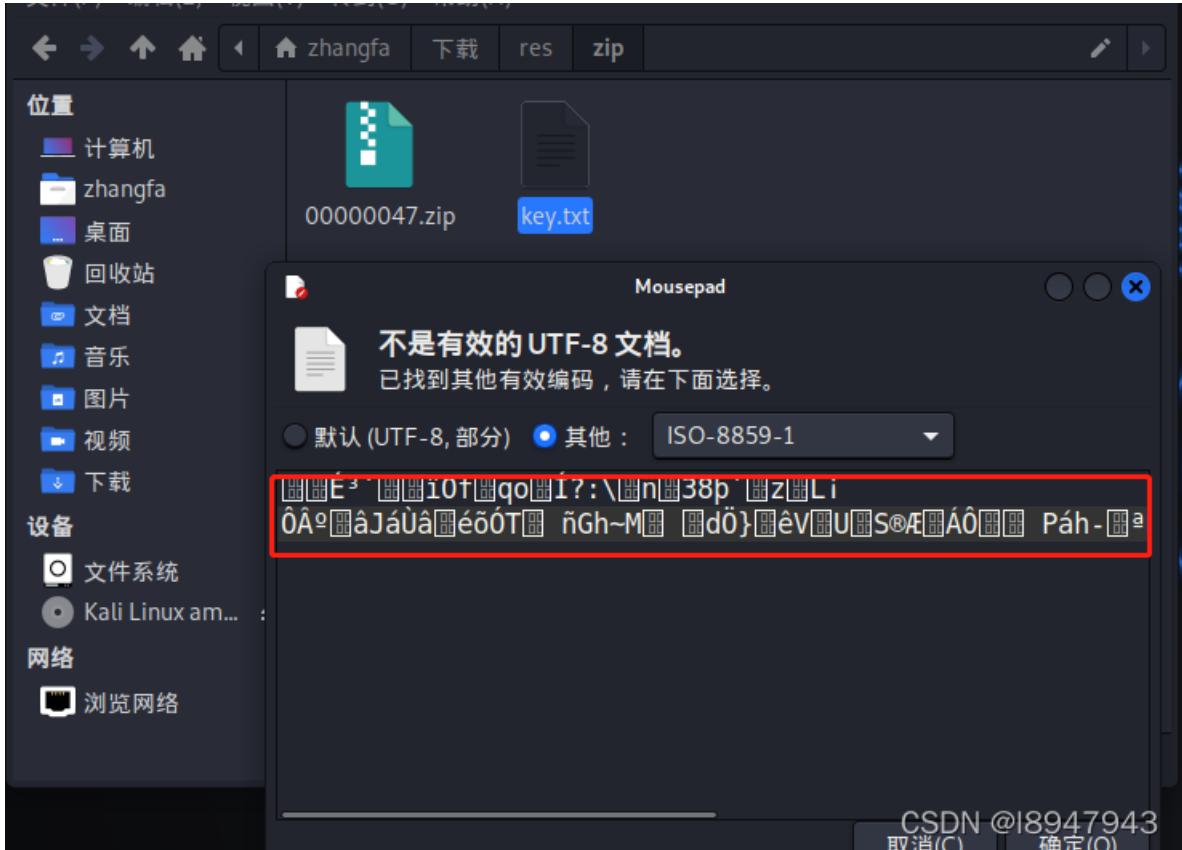
tcp流第二组时候，发现有pdf、key文件，怀疑是文件包含或者隐写。

丢入kali中foremost

```
foremost -i Misc-03.pcapng -o res
```

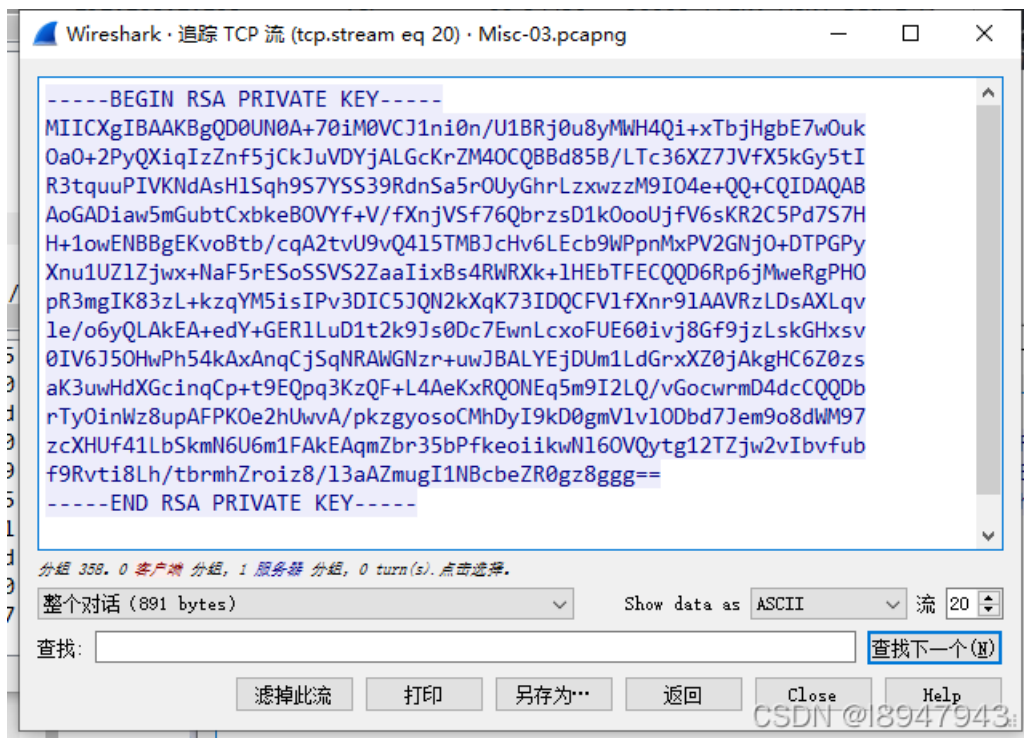
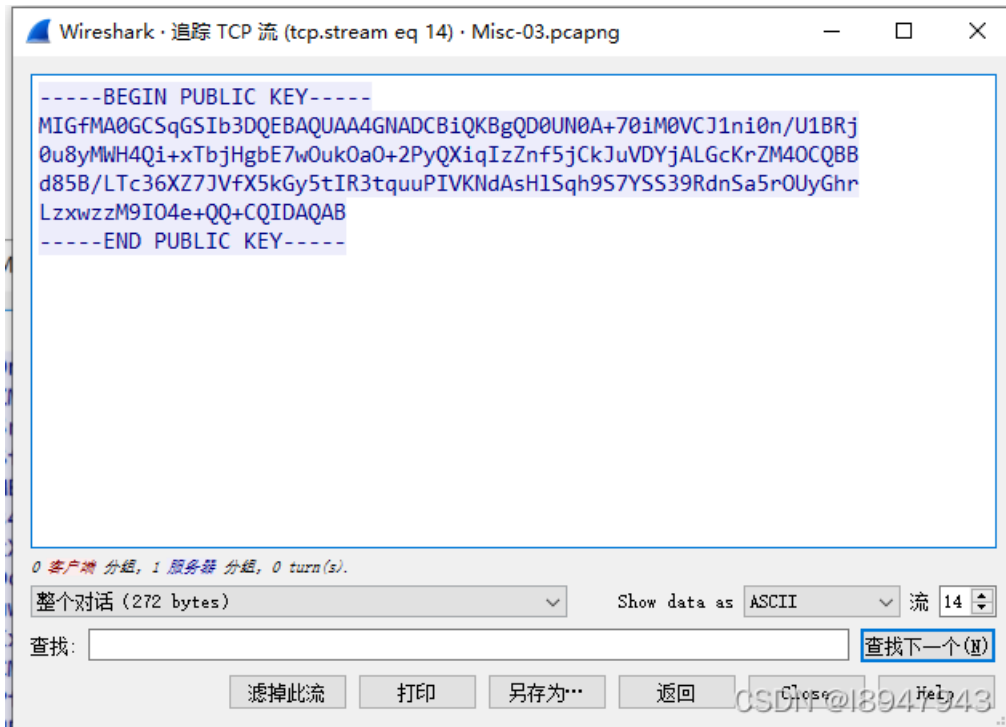
```
(zhangfa@kali)-[~/下载]
└─$ foremost -i Misc-03.pcapng -o res
Processing: Misc-03.pcapng
| foundat=key.txt
| 00000047.zip ~M d} VU S B P h - D
| PK
| *
└─$
```

去瞅瞅这个这个文件，打开res->zip->key.txt



一个key一堆乱码？尝试其他编码格式后，发现没有任何变化。。。没有思路了，是不是丢掉了什么！怀疑是被加密的东西，因为前面分析流量包有pub.key，去shark中搜搜去。

找到密钥



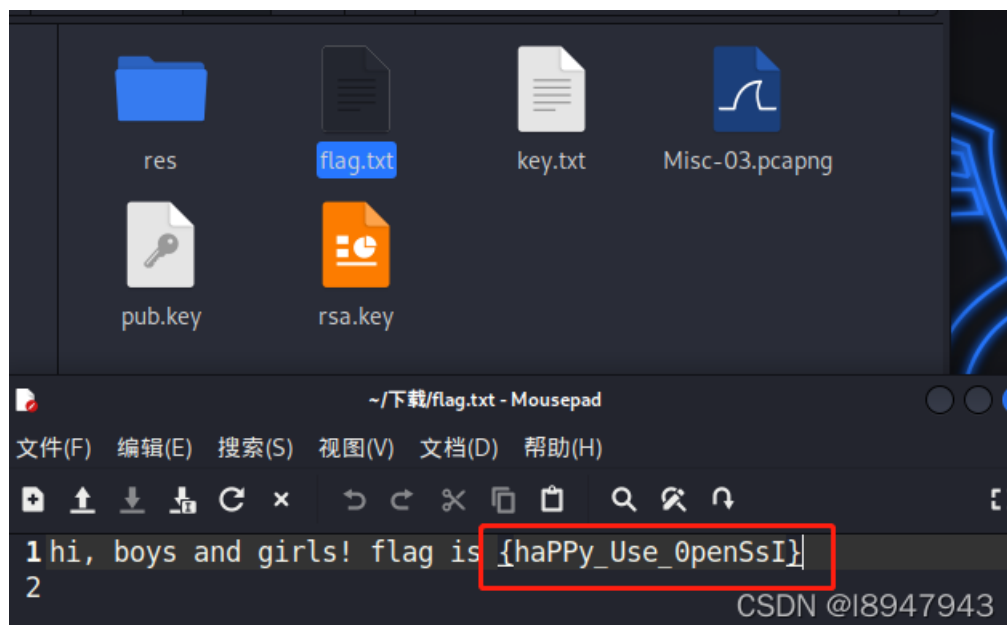
一共发现了两个key文件，突然想起曾经研究过的rsa非对称加密，而出现publickey和私钥，大体思路就明朗了。

OpenSSL解密

发现wp是让rsa去解密txt...查了查使用openssl的加密命令：

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

结果如图：



最终答案为： `flag{haPPy_Use_0penSsI}`

3. 总结

wireshark用的不熟，好麻烦。另外公钥私钥加密过程是需要进一步了解的。

相关OpenSSL文章：

- <https://www.cnblogs.com/274914765qq/p/4675535.html>
- <https://zhuannan.zhihu.com/p/91029303>
- <https://www.cnblogs.com/yangxiaolan/p/6256838.html>