

Bugku writeup (杂项) 1 【Telnet】

原创

[Sn1Per_395](#) 于 2018-09-29 09:25:38 发布 300 收藏

分类专栏: [ctf解题思路](#) 文章标签: [ctf bugku](#)

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/Dog_Captain/article/details/82892499

版权



[ctf解题思路](#) 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

【Telnet】

解压后得到.pcap文件, 这是一种数据流格式, wireshark软件可以直接把网络数据流变成这种格式



因此, 将文件拉到kali来研究。启动wireshark后, 打开此文件

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.221.1...	192.168.221.1...	TCP	66	1146 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000000	192.168.221.1...	192.168.221.1...	TCP	66	23 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=32
3	0.046800	192.168.221.1...	192.168.221.1...	TCP	54	1146 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.078000	192.168.221.1...	192.168.221.1...	TEL...	75	Telnet Data ...
5	0.093600	192.168.221.1...	192.168.221.1...	TCP	60	23 → 1146 [ACK] Seq=1 Ack=22 Win=14624 Len=0
6	4.508408	192.168.221.1...	192.168.221.1...	TEL...	66	Telnet Data ...
7	4.555208	192.168.221.1...	192.168.221.1...	TEL...	57	Telnet Data ...

```
0000  00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00  ..)&-... ).....E.
0010  00 34 07 98 40 00 80 06 00 00 c0 a8 dd 80 c0 a8  .4. .@.....
0020  dd a4 04 7a 00 17 46 01 d3 fb 00 00 00 00 80 02  ...Z..F.....
0030  20 00 3c 9d 00 00 02 04 05 b4 01 03 03 08 01 01  .<.....
0040  04 02  ..
```

https://blog.csdn.net/Dog_Captain

题目提示Telnet, 因此我们首先从telnet协议开始

41	18.423632	192.168.221.1...	192.168.221.1...	TELNET	92	Telnet Data	...
42	18.439232	192.168.221.1...	192.168.221.1...	TCP	60	23 → 1146 [ACK]	Seq=124 Ack=121 Win=14624 Len=0
<ul style="list-style-type: none"> ▶ Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) ▶ Ethernet II, Src: Vmware_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware_26:7e:0e (00:0c:29:26:7e:0e) ▶ Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164 ▶ Transmission Control Protocol, Src Port: 1146 (1146), Dst Port: 23 (23), Seq: 83, Ack: 124, Len: 38 							
<ul style="list-style-type: none"> ▼ Telnet <ul style="list-style-type: none"> Data: flag 							
0000	00 0c 29 26 7e 0e 00 0c	29 84 86 5f 08 00 45 00	..)&~...)...E.				
0010	00 4e 07 b0 40 00 80 06	00 00 c0 a8 dd 80 c0 a8	.N..@...				
0020	dd a4 04 7a 00 17 46 01	d4 4e 68 f0 2a 7a 50 18	...z...F. .Nh.*zP.				
0030	01 00 3c b7 00 00 66 6c	61 67 7b 64 33 31 36 37	...<...fl ag{				
0040	35 39 63 32 38 31 62 66	39 32 35 64 36 30 30 62					
0050	65 36 39 38 61 34 39 37	33 64 35 7d					

https://blog.csdn.net/Dog_Captain

在某一个Telnet协议的数据包下，即可看到flag