

【BugKu-CTF论坛writeup(杂项)】telnet

原创

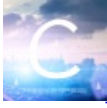
Kingyo12 于 2018-03-04 21:43:31 发布 251 收藏

分类专栏: [BugKu-CTF论坛writeup\(杂项\)](#)

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/preserphy/article/details/79440052>

版权



[BugKu-CTF论坛writeup\(杂项\)](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

telnet是基于TCP的明文传输协议, 所以直接用wireshark打开文件, 追踪TCP数据流

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.221.128	192.168.221.164	TCP	66	1146 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
2	0.000000	192.168.221.164	192.168.221.128	TCP	66	23 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
3	0.046800	192.168.221.128	192.168.221.164	TCP	54	1146 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.078000	192.168.221.128	192.168.221.164	TELNET	75	Telnet Data
5	0.093600	192.168.221.164	192.168.221.128	TCP	75	Telnet Data
6	4.508408	192.168.221.164	192.168.221.128	TELNET		
7	4.555208	192.168.221.128	192.168.221.164	TELNET		
8	4.570808	192.168.221.164	192.168.221.128	TELNET		
9	4.648808	192.168.221.128	192.168.221.164	TELNET		
10	4.648808	192.168.221.164	192.168.221.128	TELNET		
11	4.726808	192.168.221.128	192.168.221.164	TELNET		
12	4.758808	192.168.221.128	192.168.221.164	TELNET		

Context menu options:

- 标记/取消标记 分组(M) Ctrl+M
- 忽略/取消忽略 分组(I) Ctrl+D
- 设置/取消设置 时间参考 Ctrl+T
- 时间平移...
- 分组注释...
- Ctrl+Shift+T
- Ctrl+Alt+C
- 编辑解析的名称
- 作为过滤器应用
- 准备过滤器
- 对话过滤器
- 对话着色
- SCTP
- 追踪流
- 复制
- 协议首选项
- 解码为(A)...
- 在新窗口显示分组(W)

Packet 4 details:

- Frame 4: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
- Ethernet II, Src: Vmware_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware_26:7e:00 (00:0c:29:84:86:5f)
- Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164
- Transmission Control Protocol, Src Port: 1146, Dst Port: 23, Seq: 1, Ack: 1
- Telnet

Packet bytes:

```
0000 00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00 ... )&~... )...
0010 00 3d 07 9a 40 00 80 06 00 00 c0 a8 dd 80 c0 a8 ... .=.@...
0020 dd a4 04 7a 00 17 46 01 d3 fc 68 f0 29 ff 50 18 ... .z..F..h..P
0030 01 00 3c a6 00 00 ff fb 1f ff fb 20 ff fb 18 ff ... <.....
0040 fb 27 ff fd 01 ff fb 03 ff fd 03 ... !.....
```

```
.....!.....!#.....!#.....P.....!.....!.....!Ubuntu
12.04.2 LTS
hockeyinjune-virtual-machine login: ccssaaww
Password: flag{d316759c281bf925d600be698a4973d5}
Login incorrect
hockeyinjune-virtual-machine login: .
...^C
```

<http://blog.csdn.net/preserphy>