

BUUCTF Misc easycap

原创

Misc真快乐:) 于 2022-02-27 10:46:54 发布 597 收藏

分类专栏: [BUUCTF Misc](#) 文章标签: [网络安全](#) [信息安全](#)

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/Leslie_LIL/article/details/123160914

版权



[BUUCTF Misc](#) 专栏收录该内容

38 篇文章 0 订阅

订阅专栏

题目如下:

题目 解题快手榜 ×

easycap

1

注意: 得到的 flag 请包上 flag{} 提交

876932b1-5...

Flag

提交

CSDN @Misc真快乐:)

easycap.pcap

wireshark打开

easycap.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.98.199	192.155.81.86	TCP	74	46046 → 7890 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=66420265 TSecr=0
2	0.029197	192.155.81.86	172.31.98.199	TCP	74	7890 → 46046 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=33363363
3	0.029275	172.31.98.199	192.155.81.86	TCP	66	46046 → 7890 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=66420272 TSecr=333633659
4	22.722541	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=1 TSval=66425946 TSecr=333633659
5	22.749416	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=2 Win=29056 Len=0 TSval=333640474 TSecr=66425946
6	23.723048	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=2 Ack=1 Win=29312 Len=1 TSval=66426196 TSecr=333640474
7	23.753912	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=3 Win=29056 Len=0 TSval=333640775 TSecr=66426196
8	24.723642	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=3 Ack=1 Win=29312 Len=1 TSval=66426446 TSecr=333640775
9	24.753844	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=4 Win=29056 Len=0 TSval=333641076 TSecr=66426446
10	25.724349	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=4 Ack=1 Win=29312 Len=1 TSval=66426696 TSecr=333641076
11	25.753234	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=5 Win=29056 Len=0 TSval=333641376 TSecr=66426696

> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: ArubaHe_c9:7d:7a (9c:1c:12:c9:7d:7a), Dst: IntelCor_4b:f0:c3 (e4:b3:18:4b:f0:c3)

CSDN @Misc真快乐 :)

追踪TCP流，即可得到flag

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.98.199	192.155.81.86	TCP	74	46046 → 7890 [SYN] Seq=0 Win=
2	0.029197	192.155.81.86	172.31.98.199	TCP	74	7890 → 46046 [SYN, ACK] Seq=0
3	0.029275	172.31.98.199	192.155.81.86	TCP	66	46046 → 7890 [ACK] Seq=1 Ack=
4	22.722541	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=1
5	22.749416	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=
6	23.723048	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=2
7	23.753912	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=
8	24.723642	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=3
9	24.753844	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=
10	25.724349	172.31.98.199	192.155.81.86	TCP	67	46046 → 7890 [PSH, ACK] Seq=4
11	25.753234	192.155.81.86	172.31.98.199	TCP	66	7890 → 46046 [ACK] Seq=1 Ack=

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · easycap.pcap

> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: ArubaHe_c9:7d:7a (9c:1c:12:c9:7d:7a), Dst: IntelCor_4b:f0:c3 (e4:b3:18:4b:f0:c3)

> Internet Protocol Version 4, Src: 192.155.81.86, Dst: 172.31.98.199

> Transmission Control Protocol, Src Port: 7890, Dst Port: 46046

CSDN @Misc真快乐 :)