

# CTFHUB技能树-Misc-流量分析

原创

老大的豆豆酱 于 2020-08-17 18:37:57 发布 2135 收藏 6

分类专栏: [CTF](#) 文章标签: [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/weixin\\_43486981/article/details/108058698](https://blog.csdn.net/weixin_43486981/article/details/108058698)

版权



[CTF 专栏收录该内容](#)

27 篇文章 0 订阅

订阅专栏

## 文章目录

### 数据库类流量

[MySQL流量](#)

[Redis流量](#)

[MongoDB流量](#)

### 邮件流量

### 协议流量分析

[ICMP-Data](#)

[ICMP-Length](#)

### 原始流量

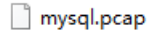


## 数据库类流量



## MySQL流量

下载题目附件，是一个 .pcap 文件



使用wireshark工具分析流量包

发现了ctfhub字段的信息，即得到了flag

The image shows a Wireshark capture of a MySQL response packet. The packet list pane shows a response from 30.0.30.10 to 30.0.250.11. The packet details pane shows the MySQL protocol structure, including the text field containing the flag: `ctfhub{mysql_is_S0_E4sy}`. The packet bytes pane shows the raw hex and ASCII data, with the flag text highlighted in a red box.

```
0000 00 9f 27 e0 01 f6 00 50 56 a8 bf b0 08 00 45 00  ..!...P V.....E.
0010 00 fc d8 dc 40 00 3f 06 0e 0a 1e 00 1e 0a 1e 00  ...@.?.....
0020 fa 0b 0c ea eb 29 8a b3 6d 35 1c b3 a5 99 80 18  ...)...m5.....
0030 00 eb 55 04 00 00 01 01 08 0a 95 0c 83 4c 38 92  ...U.....L8.
0040 58 60 01 00 00 01 03 28 00 00 02 03 64 65 66 04  X`....( ...def.
0050 66 6c 61 67 05 75 73 65 72 73 05 75 73 65 72 73  flag-use rs-users
0060 02 69 64 02 69 64 0c 3f 00 0b 00 00 00 03 03 50  .id?id? .....P
0070 00 00 00 2c 00 00 03 03 64 65 66 04 66 6c 61 67  ...,... def:flag
0080 05 75 73 65 72 73 05 75 73 65 72 73 04 6e 61 6d  -users-u sers·nam
0090 65 04 6e 61 6d 65 0c 21 00 fd 02 00 00 fd 00 00  e·name! .....
00a0 00 00 00 2c 00 00 04 03 64 65 66 04 66 6c 61 67  ...,... def:flag
00b0 05 75 73 65 72 73 05 75 73 65 72 73 04 64 65 73  -users·u sers·des
00c0 63 04 64 65 73 63 0c 21 00 fd 02 00 00 fd 00 00  c·desc! .....
00d0 00 00 00 05 00 00 05 fe 00 00 22 00 21 00 00 06  "....."
00e0 01 31 05 61 64 6d 69 6e 18 63 74 66 68 75 62 7b  .1·admin ·ctfhub{
00f0 6d 79 73 71 6c 5f 69 73 5f 53 30 5f 45 34 73 79  mysql_is _S0_E4sy
0100 7d 05 00 00 07 fe 00 00 22 00  }..... "
```

[https://blog.csdn.net/weixin\\_43486981](https://blog.csdn.net/weixin_43486981)

(小白一个，一个包一个包找的，并不知道怎么过滤关键包.....)

## Redis流量

## Redis:

- nosql数据库, 非关系型数据库
- 支持5大数据类型 (字符串String, 列表list、字典hash, 集合set, zset)
  - 与之相似的有memcache, 但memcache只支持string类型
- 单进程单线程, 好处在于不用考虑并发

下载题目附件, 打开是一个.pcap文件

### Redis流量

所需金币: 30      题目状态: **未解出**      解题奖励: 金币:50 经验:10

[📎 题目附件](#)

00:26:32

环境续期 ▾    **停止并销毁环境**

每分钟需要1个金币,请根据个人需求

Flag{.....}    [提交Flag](#)    [WriteUp](#)

[📎 redis.pcap](#)

使用wireshark工具分析流量包。

使用在线工具, 将ctfhub转换为十六进制数值

### ASCII在线转换器-十六进制, 十进制、二进制

ASCII转换到 ASCII (例: a b c)

ctfhub

[添加空格](#)    [删除空格](#)     将空白字符转换

[十六进制转换到](#) 16进制(例:0x61或61或61/62)     删除 0x

637466687562

在wireshark中搜索该十六进制关键字

十六进制值 ▾ 637466687562

Protocol Length Info

发现了包含ctfhub字段信息的数据包，第66个包发现只有部分的flag信息，并不完整。

```
65 101.418008 fe80::29f:27ff:fee0::ff02::1 ICMPv6 110 Router Advertisement from 00:9f:27:e0:01:f6
66 105.037564 30.0.250.11 30.0.30.10 TCP 119 63757 - 6379 [PSH, ACK] Seq=76 Ack=14762 Win=131072 Len=53 TSval=949699226 TSecr=101651567
67 105.037716 30.0.30.10 30.0.250.11 TCP 71 6379 - 63757 [PSH, ACK] Seq=14762 Ack=129 Win=29056 Len=5 TSval=101730651 TSecr=949699226
68 105.044115 30.0.250.11 30.0.30.10 TCP 66 63757 - 6379 [ACK] Seq=129 Ack=14767 Win=131040 Len=0 TSval=949699235 TSecr=101730651
69 117.418202 fe80::29f:27ff:fee0::ff02::1 ICMPv6 110 Router Advertisement from 00:9f:27:e0:01:f6
> Frame 66: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
> Ethernet II, Src: 00:9f:27:e0:01:f6 (00:9f:27:e0:01:f6), Dst: VMware_a8:bf:b0 (00:50:56:a8:bf:b0)
> Internet Protocol Version 4, Src: 30.0.250.11, Dst: 30.0.30.10
> Transmission Control Protocol, Src Port: 63757, Dst Port: 6379, Seq: 76, Ack: 14762, Len: 53
> Data (53 bytes)
0000 00 50 56 a8 bf b0 00 9f 27 e0 01 f6 08 00 45 00 PV.....E
0010 00 69 96 d4 40 00 3f 06 50 a5 1e 00 fa 0b 1e 00 e..@.?P
0020 1e 0a f9 0d 18 eb 0d a4 8c 8c 6c 85 20 74 80 18 .....l.t
0030 10 00 2d 12 00 00 01 01 08 0a 38 9b 42 9a 06 0f .....8.Y
0040 14 6f 2a 33 0d 0a 24 33 0d 0a 53 45 54 0d 0a 24 o*3.$3..SET.$
0050 35 0d 0a 46 6c 34 67 31 0d 0a 24 32 32 0d 0a 63 5..Flag..$2..a
0060 74 66 68 75 62 7b 36 30 35 31 64 36 31 32 33 64 tfhub{60 51d6123d
0070 65 34 33 64 66 0d 0a e43df..
```

[https://blog.csdn.net/weixin\\_43486981](https://blog.csdn.net/weixin_43486981)

在66号包后面继续寻找，发现70号数据包出现了另一半flag信息

```
69 117.418202 fe80::29f:27ff:fee0::ff02::1 ICMPv6 110 Router Advertisement from 00:9f:27:e0:01:f6
70 119.251861 30.0.250.11 30.0.30.10 TCP 115 63757 - 6379 [PSH, ACK] Seq=129 Ack=14767 Win=131072 Len=49 TSval=949713350 TSecr=101730651
71 119.251958 30.0.30.10 30.0.250.11 TCP 71 6379 - 63757 [PSH, ACK] Seq=14767 Ack=178 Win=29056 Len=5 TSval=101744866 TSecr=949713350
72 119.252202 30.0.250.11 30.0.30.10 TCP 66 63757 - 6379 [ACK] Seq=178 Ack=14770 Win=131040 Len=0 TSval=101744866 TSecr=101744866
> Frame 70: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0
> Ethernet II, Src: 00:9f:27:e0:01:f6 (00:9f:27:e0:01:f6), Dst: VMware_a8:bf:b0 (00:50:56:a8:bf:b0)
> Internet Protocol Version 4, Src: 30.0.250.11, Dst: 30.0.30.10
> Transmission Control Protocol, Src Port: 63757, Dst Port: 6379, Seq: 129, Ack: 14767, Len: 49
> Data (49 bytes)
0000 00 50 56 a8 bf b0 00 9f 27 e0 01 f6 08 00 45 00 PV.....E
0010 00 65 80 ec 40 00 3f 06 66 91 1e 00 fa 0b 1e 00 e..@.?P
0020 1e 0a f9 0d 18 eb 0d a4 8c c1 6c 85 20 79 80 18 .....l.y
0030 10 00 9a a9 00 00 01 01 08 0a 38 9b 79 c6 06 10 .....8.Y
0040 49 5b 2a 33 0d 0a 24 33 0d 0a 73 65 74 0d 0a 24 I[*3.$3..set.$
0050 35 0d 0a 66 6c 61 67 32 0d 0a 24 31 38 0d 0a 64 5..Flag..$2..a
0060 64 37 36 30 39 38 30 34 39 32 35 63 30 31 32 31 d7609804 925c0121
0070 7d 0d 0a }..
```

[https://blog.csdn.net/weixin\\_43486981](https://blog.csdn.net/weixin_43486981)

## MongoDB流量

所需金币: 30

题目状态: 未解出

解题奖励: 金币:50 经验:10

开启题目 ¥ 30

Flag{.....}

提交Flag

WriteUp

下载题目附件，打开是一个.pcap文件

mongodb.pcap

使用在线转换工具将ctfhub{转换为十六进制表示

## ASCII在线转换器-十六进制，十进制、二进制

ASCII转换到 ASCII (例: a b c)

ctfhub{

添加空格

删除空格

 将空白字符转换十六进制转换到 16进制(例:0x61或61或61/62)  删除 0x

6374666875627b

在wireshark中搜索该十六进制

十六进制值

6374666875627b

即可查找到包含关键字ctfhub{的数据包

Time	Source	Destination	Protocol	Length	Info
482.65.908925	30.0.250.11	30.0.30.10	TCP	106	63822 → 27017 [PSH, ACK] Seq=2045 Ack=4361 Win=131072 Len=40 TSval=954513459 TSecr=2506053404 [TCP segment of a reassembled PDU]
483.65.908966	30.0.250.11	30.0.30.10	TCP	226	63822 → 27017 [PSH, ACK] Seq=2085 Ack=4361 Win=131072 Len=160 TSval=954513459 TSecr=2506053404 [TCP segment of a reassembled PDU]
Flags: 0x018 (PSH, ACK) Window size value: 4096 [Calculated window size: 131072] [Window size scaling factor: 32] Checksum: 0x2958 [unverified] [Checksum Status: Unverified]					
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps [SEQ/ACK analysis] [Timestamps] TCP payload (160 bytes) TCP segment data (160 bytes)					
0000	00 50 56 a8 bf b0 00 9f 27 e0 01 f6 08 00 45 00				..PV.....E-
0010	00 d4 8a 9f 40 00 3f 06 5c 6f 1e 00 fa 0b 1e 00				...@?..No.....
0020	1e 0a f9 4e 69 89 03 b5 1c 9d fa a0 67 91 80 18				...NI.....g...
0030	10 00 29 58 00 00 01 01 08 0a 38 e4 b8 33 95 5f				...X.....B..3..
0040	57 1c a0 00 00 02 69 6e 73 65 72 74 00 05 09				W.....i insert...
0050	00 00 66 6c 61 67 00 04 64 6f 63 75 6d 65 6e 74				...flag..document
0060	73 00 51 00 00 03 00 00 49 00 00 00 07 5f 69				..s Q...@ I...-1
0070	64 00 5e b3 c2 c4 9d af 59 23 62 e9 06 30 02 66				d A.....Yh..0..f
0080	6c 61 67 00 29 00 00 00 63 74 66 68 75 62 7b 35				..lag)....ctfhub{5
0090	66 32 38 34 65 63 63 32 37 39 64 32 63 62 64 31				..f284ecc2 79d2cbd1
00a0	61 00 32 35 38 62 62 35 33 63 37 61 35 66 36 7d				..af258bb5 3c7a5f6)
00b0	00 00 00 00 6f 72 64 65 72 65 64 00 01 63 6c 73				...orde red...15
00c0	69 64 00 1e 00 00 00 05 69 64 00 10 00 00 00 04				id.....id.....
00d0	08 0f a0 8f 6f fd 44 70 b6 40 39 1d 69 10 96 37				...o Dp ..@9 i..7
00e0	00 00				...

https://blog.csdn.net/weixin\_43486981

## 邮件流量





