

ctfhub MongoDB流量

原创

「铁躯电芯」 于 2021-06-06 14:23:13 发布 205 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/plant1234/article/details/117626578>

版权

MongoDB流量：

知识点:wireshark过滤搜索功能

这题我们打开题目得到流量包，查找ctfhub得到很多有关的流量包

且不是要的答案：

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)

Apply a display filter ... <Ctrl-/> 表达式...

分组字节流 宽窄 区分大小写 字符串 ctfhub 查找 取消

No.	Time	Source	Destination	Protocol	Length	Info
495	65.923952	30.0.250.11	30.0.30.10	TCP		66 63823 → 27017 [ACK] Seq=1915 Ack=16222 V
496	65.924058	30.0.250.11	30.0.30.10	TCP		66 63877 → 27017 [ACK] Seq=1166 Ack=27859 V
497	65.942330	30.0.250.11	30.0.30.10	TCP		105 63821 → 27017 [PSH, ACK] Seq=2397 Ack=40
498	65.942339	30.0.250.11	30.0.30.10	TCP		122 63821 → 27017 [PSH, ACK] Seq=2436 Ack=40
499	65.942354	30.0.250.11	30.0.30.10	TCP		106 63824 → 27017 [PSH, ACK] Seq=1567 Ack=15
500	65.942361	30.0.250.11	30.0.30.10	TCP		140 63824 → 27017 [PSH, ACK] Seq=1607 Ack=15
501	65.942406	30.0.30.10	30.0.250.11	TCP		66 27017 → 63821 [ACK] Seq=4055 Ack=2492 W
502	65.942419	30.0.30.10	30.0.250.11	TCP		66 27017 → 63824 [ACK] Seq=15807 Ack=1681 V
503	65.942465	30.0.30.10	30.0.250.11	TCP		119 27017 → 63821 [PSH, ACK] Seq=4055 Ack=24
504	65.942505	30.0.250.11	30.0.30.10	TCP		106 63823 → 27017 [PSH, ACK] Seq=1915 Ack=16
505	65.942513	30.0.250.11	30.0.30.10	TCP		142 63823 → 27017 [PSH, ACK] Seq=1955 Ack=16

> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (40 bytes)
TCP segment data (40 bytes)

Offset	Hex	ASCII
0000	00 50 56 a8 bf b0 00 9f 27 e0 01 f6 08 00 45 00	.PV.....E.
0010	00 5c 0a a4 40 00 3f 06 dc e2 1e 00 fa 0b 1e 00	.\.@.?.....
0020	1e 0a f9 4f 69 89 ad 62 4c 42 a9 06 0c e7 80 18	..Oi.b LB.....
0030	10 00 21 eb 00 00 01 01 08 0a 38 e4 b8 51 95 5f	..!.....8.Q.
0040	81 b1 74 00 00 00 59 00 00 00 00 00 00 00 d4 07	..t..v.....
0050	00 00 00 00 00 00 63 74 66 68 75 62 2e 24 63 6dct fhub.scm
0060	64 00 00 00 00 00 ff ff ff ff	d.....

<https://blog.csdn.net/plant1234>

于是我们增加精确用ctfhub{得到flag:

[Calculated window size: 131072]
[Window size scaling factor: 32]
Checksum: 0x2958 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (160 bytes)
TCP segment data (160 bytes)

0030	10 00 29 58 00 00 01 01 08 0a 38 e4 b8 33 95 5f	..)X.... ..8..3.._
0040	57 1c a0 00 00 00 02 69 6e 73 65 72 74 00 05 00	W.....i nsert...
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 00 03 30 00 49 00 00 00 07 5f 69	s.Q....0 ..I...._i
0070	64 00 5e b3 c2 c4 9d af 59 23 62 e9 06 30 02 66	d.^... Y#b...f
0080	6c 61 67 00 29 00 00 00 63 74 66 68 75 62 7b 35	lag.)... [t#hub{5
0090	66 32 38 34 65 63 63 32 37 39 64 32 63 62 64 31	f284ecc2 79d2cbd1
00a0	61 66 32 35 38 62 62 35 33 63 37 61 35 66 36 7d	af258bb5 3c7a5f6}
00b0	00 00 00 08 6f 72 64 65 72 65 64 00 01 03 6c 73	...orde red...ls
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	..