

攻防世界CRYPTO 工业协议分析2 writeup

原创

[Sprint#51264](#) 于 2020-08-16 20:12:01 发布 275 收藏 1

分类专栏: [CRYPTO](#)

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/qq_45837896/article/details/108042082

版权



[CRYPTO 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

这道题涉及到用wireshark进行流量分析

题目提醒到流量包中有异常点, 那么我们打开附件进行查看

The screenshot shows the Wireshark interface with a list of network packets. The packet list pane shows several packets with the same source and destination IP addresses (192.168.1.181 and 192.168.1.123) and a length of 64 bytes. The details pane for the selected packet shows it is an Ethernet II frame, an Internet Protocol Version 4 packet, and a User Datagram Protocol (UDP) packet with source port 64405 and destination port 11000. The data field is highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
1629	194.086063	192.168.1.181	192.168.1.123		62	11000 → 64406 Len=20
1633	194.334917	192.168.1.181	192.168.1.123		62	11000 → 64406 Len=20
1637	194.584941	192.168.1.181	192.168.1.123		62	11000 → 64406 Len=20
1641	194.834836	192.168.1.181	192.168.1.123		62	11000 → 64406 Len=20
1645	195.085048	192.168.1.181	192.168.1.123		62	11000 → 64406 Len=20
173	32.410529	192.168.1.181	192.168.1.123		64	11000 → 64406 Len=22

Details for Frame 173:
> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{A1A8295F-64E3-446C-AB9D-7BE9AB6D5D54}, interface 0
> Ethernet II, Src: VMware_0a:63:9f (00:0c:29:0a:63:9f), Dst: 00:e2:36:0b:19:2b (00:e2:36:0b:19:2b)
> Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.181
> User Datagram Protocol, Src Port: 64405, Dst Port: 11000
> Data (16 bytes)

经过比对发现它们的源还有目标地址大抵相同

但是在长度上有些包的长度只出现过一次, 非常可疑

```
·B······B·····  
·...·MAI N_(·...·  
·)····· ······fl  
ag·
```

比如说这个长度为147的UDP包里就包含了一个flag的异样字符串

再往后看

```
·...·%· 666c6167  
7b37466f 4d325374  
6b686550 7a7d·
```

长度为173.179的包里更是出现了两串相同的奇怪字符串

猜测是经过加密的flag

观察这串字符串发现它们都不超过F, 所以认为是经过16进制加密的

进行解码

```
| flag{7FoM2StkhePz}
```