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

本文链接：https://blog.csdn.net/qq_45837896/article/details/108042082

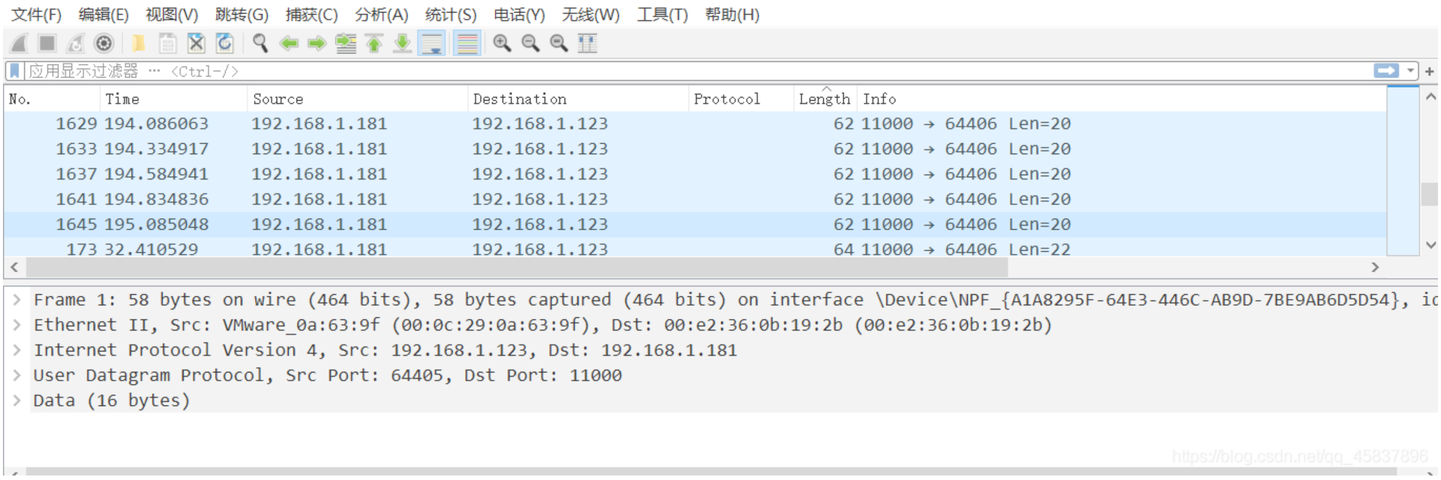
CRYPTO 专栏收录该内容

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

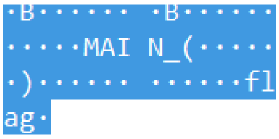

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
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
```

```
> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{A1A8295F-64E3-446C-AB9D-7BE9AB6D5D54}, id
> 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

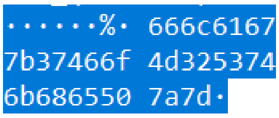
但是在长度上有些包的长度只出现过一次，非常可疑



```
·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



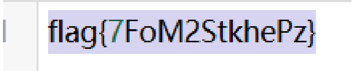
```
······%· 666c6167
7b37466f 4d325374
6b686550 7a7d·
```

长度为173.179的包里更是1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}
```