


XCTF_工业协议分析2

原创

[永远是深夜有多好。](#)  于 2022-01-06 17:29:51 发布  111  收藏

分类专栏: [XCTF](#) 文章标签: [安全 网络](#)

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_37370714/article/details/122348771

版权



[XCTF 专栏收录该内容](#)

17 篇文章 0 订阅

订阅专栏

用wireshark打开

The image shows a Wireshark interface with a packet list and a packet details pane. The packet list shows various UDP and SSDP packets. The selected packet (No. 9) is an SSDP M-SEARCH packet. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol layers. The data section shows the raw bytes of the packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|-----------------|----------|--------|-----------------------|
| 1 | 0.000000 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 2 | 0.000866 | 192.168.1.181 | 192.168.1.123 | UDP | 62 | 11000 → 64405 Len=20 |
| 3 | 0.001149 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 4 | 0.002151 | 192.168.1.181 | 192.168.1.123 | UDP | 566 | 11000 → 64405 Len=524 |
| 5 | 0.249455 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 6 | 0.250822 | 192.168.1.181 | 192.168.1.123 | UDP | 62 | 11000 → 64405 Len=20 |
| 7 | 0.251136 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 8 | 0.252397 | 192.168.1.181 | 192.168.1.123 | UDP | 566 | 11000 → 64405 Len=524 |
| 9 | 0.329000 | 192.168.1.243 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 10 | 0.515930 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 11 | 0.516733 | 192.168.1.181 | 192.168.1.123 | UDP | 62 | 11000 → 64405 Len=20 |
| 12 | 0.517000 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 13 | 0.518054 | 192.168.1.181 | 192.168.1.123 | UDP | 566 | 11000 → 64405 Len=524 |
| 14 | 0.765520 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 15 | 0.766798 | 192.168.1.181 | 192.168.1.123 | UDP | 62 | 11000 → 64405 Len=20 |
| 16 | 0.767134 | 192.168.1.123 | 192.168.1.181 | UDP | 58 | 64405 → 11000 Len=16 |
| 17 | 0.768226 | 192.168.1.181 | 192.168.1.123 | UDP | 566 | 11000 → 64405 Len=524 |

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

```

0000 00 e2 36 0b 19 2b 00 0c 29 0a 63 9f 08 00 45 00  ..6...+...).c...E
0010 00 2c cb 66 00 00 80 11 00 00 c0 a8 01 7b c0 a8  ,.f.....{..
0020 01 b5 fb 95 2a f8 00 18 84 aa 0c 00 20 dd 10 00  *.....
0030 41 00 00 00 66 00 00 00 00 00  A...f.....
  
```

看了半天发现没有思路 于是想看看长度

| Time | Source | Destination | Protocol | Length | Info |
|------|------------|-------------------|-------------------|--------|--|
| 133 | 16.936455 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 216 | 48.941246 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 536 | 71.444559 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 687 | 95.946840 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 829 | 146.943245 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 1204 | 169.444032 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 1594 | 191.943919 | VMware_0a:63:9f | 00:e2:36:0b:19:2b | ARP | 42 Who has 192.168.1.181? Tell 192.168.1.123 |
| 178 | 34.393278 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 179 | 35.133089 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 180 | 36.132350 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 184 | 37.132541 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 185 | 38.132725 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 186 | 41.419419 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 190 | 42.133548 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 191 | 43.132724 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 192 | 44.132864 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |
| 208 | 45.132527 | Universa_f7:ca:39 | Broadcast | ARP | 60 Who has 192.168.1.1? Tell 192.168.1.243 |

CSDN @猫于星空

就发现这几个出现次数很少 很有嫌疑最终在131和137找到了与众不同的一些十六进制数

| | | | | | |
|-----|-----|-------|---|-------|---------|
| UDP | 67 | 64406 | → | 11000 | Len=25 |
| UDP | 74 | 11000 | → | 64406 | Len=32 |
| UDP | 74 | 11000 | → | 64406 | Len=32 |
| UDP | 131 | 11000 | → | 64406 | Len=89 |
| UDP | 137 | 64406 | → | 11000 | Len=95 |
| UDP | 137 | 64406 | → | 11000 | Len=95 |
| UDP | 146 | 64406 | → | 11000 | Len=104 |
| UDP | 147 | 64406 | → | 11000 | Len=105 |
| UDP | 158 | 11000 | → | 64406 | Len=116 |
| UDP | 158 | 11000 | → | 64406 | Len=116 |
| UDP | 173 | 11000 | → | 64406 | Len=131 |
| UDP | 179 | 64406 | → | 11000 | Len=137 |

CSDN @猫于星空

据 `6c61677b37466f4d3253746b6865507a7d`

转化为字符串找到了lag（提交的时候记得把lag改为flag）

16进制转换文本 / 文本转16进制

6c61677b37466f4d3253746b6865507a7d

字符串转16进制 >>

lag{7FoM2StkhePz}

16进制转字符串 >>

CSDN @猫于星空



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)