

春秋杯2021-勇者山峰 helloshark

原创

A\R 于 2021-11-28 22:27:03 发布 268 收藏

分类专栏: [CTF-Misc](#) 文章标签: [web](#) [网络安全](#) [经验分享](#)

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_51804748/article/details/121599076

版权



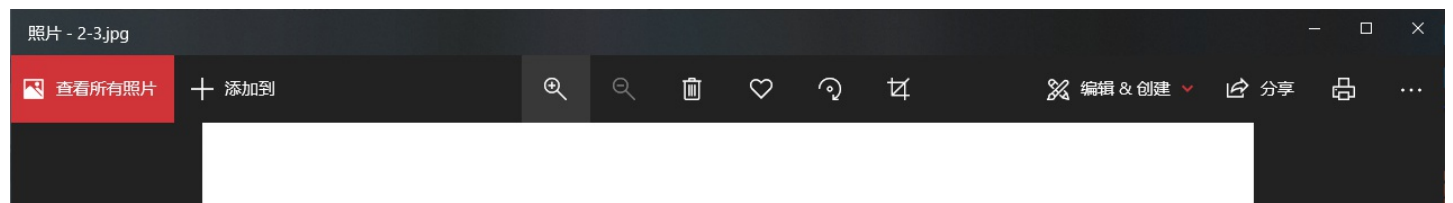
[CTF-Misc 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏



本题附件打开是一个bmp图片



将后缀名改为zip后打开压缩包，发现有两个文件，但是解压需要密码，其中有提示说密码在图片中。
尝试各种工具来解析这个图片，最后可以用 `zsteg` 来得到压缩包密码

```
zsteg -a 文件名
```

```
root@kali: ~
文件 动作 编辑 查看 帮助
000000d0: 68 ea c7 84 48 ee a8 29 3e ed cd d3 2c 22 01 27 |h...H..)>...,".'|
000000e0: fa bd e1 66 61 8b 26 e2 c8 69 be 13 80 51 60 42 |...fa.&..i...Q`B|
000000f0: 1a 92 c7 b1 06 fd e1 3e 6a e2 ad bb b0 49 48 a5 |.....>j....IH.|
imagedata .. text: ":ff:::~::~:f::"
b1,r,msb,xy .. file: Big-endian UTF-16 Unicode text, with very long lines, with no line terminators
b8,rgb,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b1,r,lsb,xy .. text: "password:@91902AF23C#276C2FC7EAC615739CC7C0"
b4,rgb,msb,xy .. text: ["w" repeated 12 times]
b8,rgb,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b2,rgb,lsb,xy,prime .. file: MPEG ADTS, layer III, v1, 160 kbps, 32 kHz, 2x Monaural
b3,r,lsb,xy,prime .. file: very old 16-bit-int big-endian archive
b5,r,lsb,xy,prime .. file: MPEG ADTS, layer II, v1, 384 kbps, JntStereo
b8,r,msb,xy,prime .. file: ddis/ddif
b1,r,msb,Yx .. text: "0C7CC937516CAE7CF2C672#C32FA20919@drowssap"
b2,r,msb,Yx .. text: "_w_W_}_uWuwu"
b1,r,lsb,Yx,prime .. file: AIX core file fulldump
b4,rgb,msb,Yx,prime .. text: ["w" repeated 10 times]

(root@kali)-[~]
#
```

CSDN @ \ A.R.

用密码解压文件，用wireshark打开流量包

The screenshot shows a Wireshark capture of a TCP stream. The packet list pane shows a sequence of packets, with packet 16 highlighted. The packet details pane shows the following information:

- Frame 16: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{C36F02AA-8D07-4F48-8197-F07DBF54A806}, id 0
- Ethernet II, Src: VMware_e2:8c:38 (00:50:56:e2:8c:38), Dst: VMware_68:db:25 (00:0c:29:68:db:25)
- Internet Protocol Version 4, Src: 106.75.209.165, Dst: 192.168.74.135
- Transmission Control Protocol, Src Port: 8007, Dst Port: 49491, Seq: 1, Ack: 59, Len: 58

The packet bytes pane shows the raw data of the packet, which includes the password:

```
0000 00 0c 29 68 db 25 00 50 56 e2 8c 38 08 00 45 00 ..)h.%P V..8..E-
0010 00 62 63 96 00 00 80 06 8f df 6a 4b d1 a5 c0 a8 ..bc.....:jk...
0020 4a 87 1f 47 c1 53 22 53 a5 91 3c 5b fa e5 50 18 J..G.S <<[.P-
0030 fa f0 79 7e 00 00 00 00 00 36 01 0a 33 01 07 72 ..y.....6.3..P
0040 65 73 09 5f 63 6d 64 0b 61 66 74 65 72 04 01 06 es.cmd.after...
0050 0d 31 35 36 35 2d 36 06 2f 6c 61 6f 5f 62 61 6e .1565-6./!ao_ban
0060 5f 49 5f 66 69 6e 64 5f 70 61 73 73 77 6f 72 64 _I_find_password
```

