

2021春秋杯网络安全联赛—秋季赛 勇者山峰wp（部分）

原创

聆风网络 于 2021-11-30 10:07:45 发布 3044 收藏 1

分类专栏: [网络安全 CTF](#) 文章标签: [安全](#) [网络安全](#)

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_55356211/article/details/121625820

版权



[网络安全](#) 同时被 2 个专栏收录

1 篇文章 1 订阅

订阅专栏



[CTF](#)

1 篇文章 0 订阅

订阅专栏

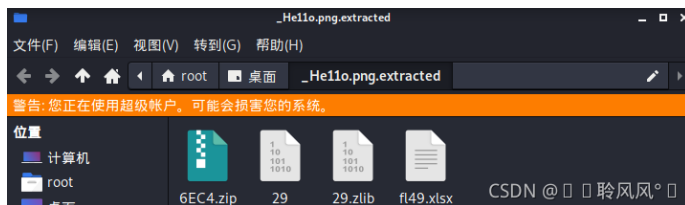
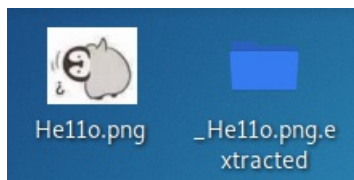
secret_chart

首先打开压缩包, 发现里面有一个he11o.png解压出来, 使用binwalk进行文件分离,

```
(root@kali) - [~/桌面]
# binwalk -e He11o.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 200 x 172, 8-bit/color RGB, non-interlaced
41	0x29	Zlib compressed data, best compression
28356	0x6EC4	Zip archive data, encrypted at least v2.0 to extract,
44333	0xAD2D	End of Zip archive, footer

分出来一个文件夹, 点击进去发现一个需要密码的压缩包



这里使用 zip2john 破解压缩包密码

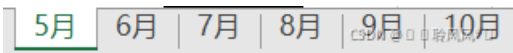
```

(root@kali)~/桌面/_He11o.png.extracted]
# zip2john 6EC4.zip >> passwd.txt
ver 2.0 6EC4.zip/fl49.xlsx PKZIP Encr: cmplen=15847, decmplen=15835, crc=DBACA87D

(root@kali)~/桌面/_He11o.png.extracted]
# john passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:45 3/3 0g/s 785752p/s 785752c/s plmminha..bigbydia
0g 0:00:00:51 3/3 0g/s 789686p/s 789686c/s aa5cbp..atxie5
0g 0:00:00:52 3/3 0g/s 790726p/s 790726c/s rllle2..r1mrya
0g 0:00:00:53 3/3 0g/s 791263p/s 791263c/s alinbabs..albo1969
9527 (6EC4.zip/fl49.xlsx)
1g 0:00:01:44 DONE 3/3 (2021-11-27 18:18) 0.009586g/s 808929p/s 808929c/s 808929c/s 5sf28..90cu
Use the "--show" option to display all of the cracked passwords reliably
Session completed
CSDN @ 聆风°

```

得出9527解压密码，解压后得到fl49.xlsx，打开后发现6个工作表，每个表里有的表格是1有的没有数据，可能是拆分的部分二维码



客服人员表现统计/月	迟到	早退	被好评	被投诉
宋爱梅	1		1	
王志芳	1		1	1
于光	1	1		
贾隽仙	1	1	1	1
贾燕青	1	1		1
刘振杰	1	1		
郭卫东	1			1
崔红宇	1	1		
马福平	1			1
冯红	1			
崔敬伟	1	1	1	
穆增志	1		1	
谢志威	1			1
吕金起	1			1
韩云庆	1	1	1	1
鲁全福	1		1	
郭建立	1	1	1	1
郝连水	1		1	1
闫智胜	1		1	

把6个工作表里的所有是1的表格填充为黑色

最后把6个表格填充完黑色，按顺序放到新建的工作表，并调整行高和列宽都为16像素



这里我使用手机上的QQ浏览器进行扫码

得到zfua{B3s1o9in1Nw0halUnofuNc0HM1}，使用凯撒位移20即可得出flag



flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}

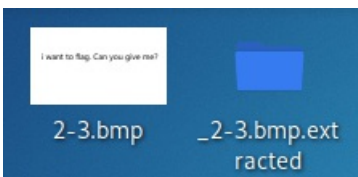
helloshark

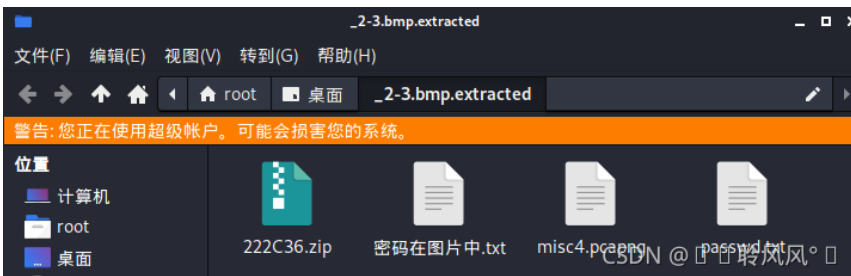
解压压缩包得到一个2-3.bmp文件，使用binwalk进行文件分离。

```
(root@kali) - [~/桌面]
# binwalk -e 2-3.bmp
```

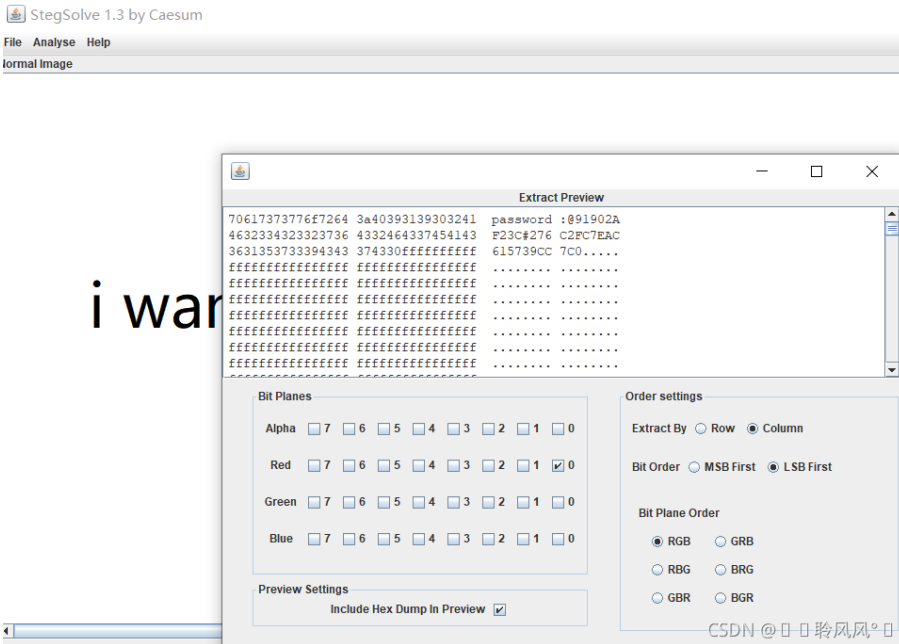
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PC bitmap, Windows 3.x format,, 1152 x 648 x 24
2239542	0x222C36	Zip archive data, encrypted at least v2.0 to extract, compressed size: 599403,
2839359	0x2B533F	End of Zip archive, footer length: 22

可以分离出来文件，进去发现有一个需要密码的压缩包



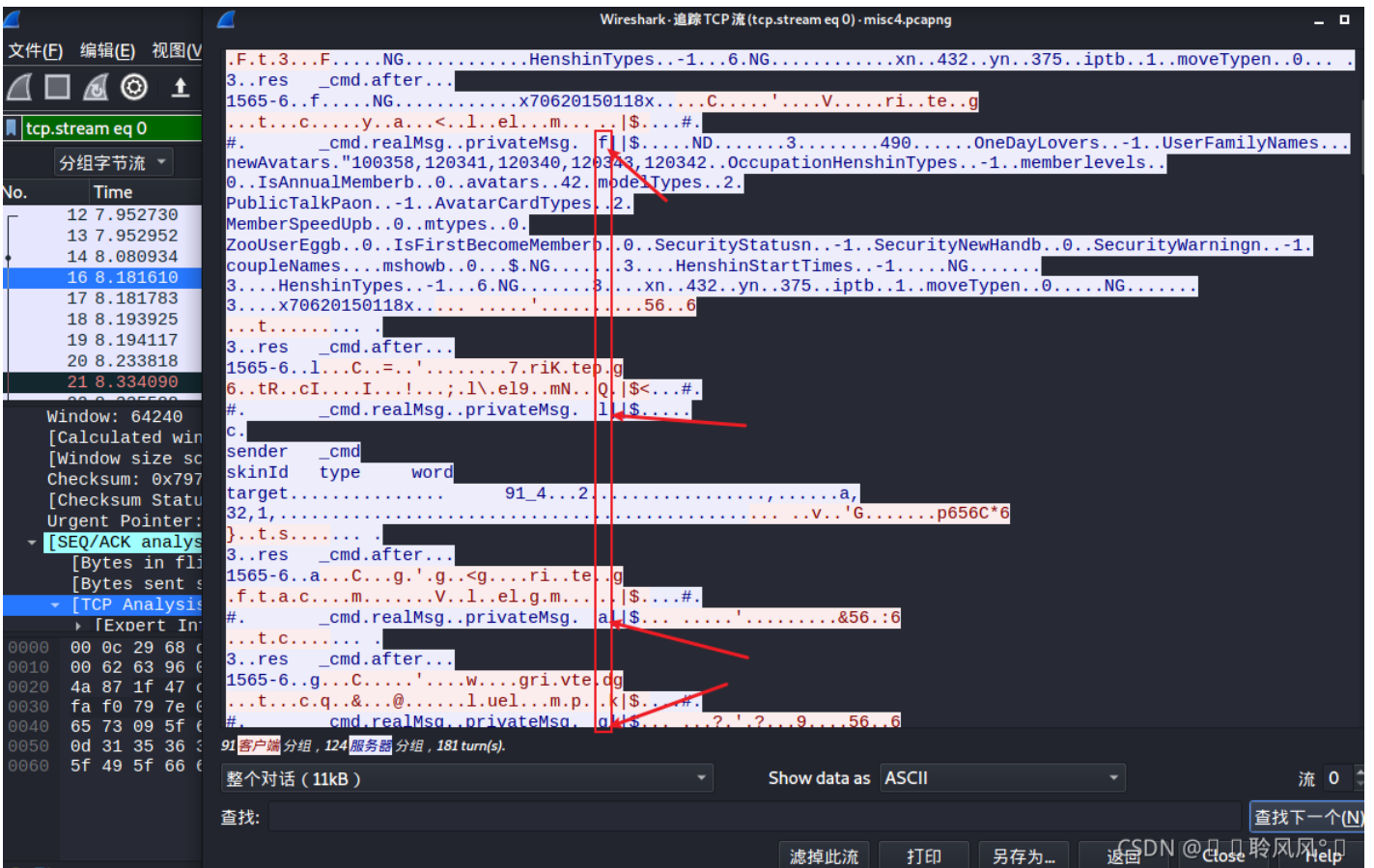


发现是LSB隐写，得出密码 @91902AF23C#276C2FC7EAC615739CC7C0



使用这个密码去解压压缩包，可以得出一个misc4.pcapng文件

追踪TCP流发现flag就在这里面，是竖着分开有顺序的



最后手动把每个字符一个一个记下来得到flag

flag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}

问卷调查

填写调查问卷，即可获得flag

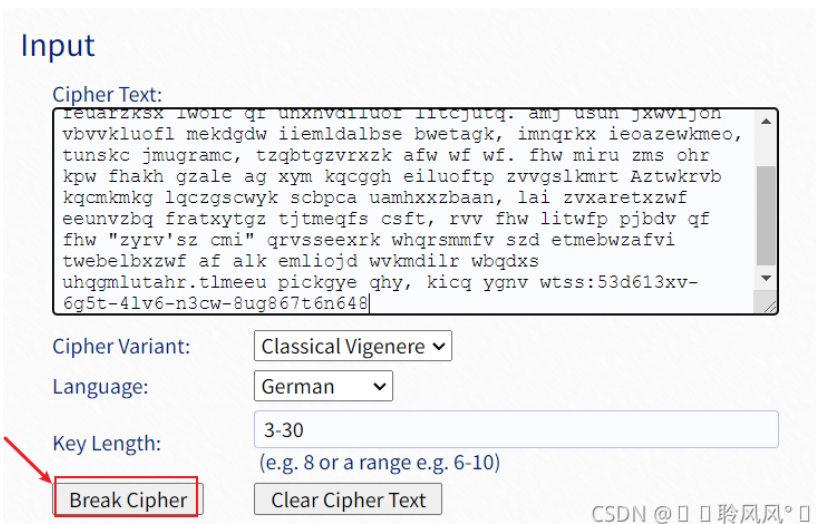
flag{让我们一起带给世界安全感}

Vigener

首先解压缩包，得到一个txt文件，打开后发现是密文，根据题目名字得知是维吉尼亚密码。

这里使用了一个国外的在线解密网站：[Vigener Solver - www.guballa.de](http://www.guballa.de)

把txt里所有内容ctrl+a 复制到网站input里，点击 Break Cipher



即可获得flag

Result

Clear text [\[hide\]](#)

Clear text using key "asterism":

```
has many years of research experience and high technical level in
information security. his main research directions include
penetration testing, reverse engineering, binary security,
cryptography and so on. the team has won the third prize in the
second national industrial Internet security technology skills
competition, the information security triathlon training camp, and
the second prize in the "guan'an cup" management operation and
maintenance competition of isg network security skills
competition.cdusec welcome you, take your flag:53d613fc-6c5c-4dd6-
b3ce-8bc867c6f648
```

CSDN @ 聆风

flag{53d613fc-6c5c-4dd6-b3ce-8bc867c6f648}