




# 世安杯CTF writeup

原创

IT老涵  于 2021-07-23 15:38:25 发布  113  收藏

分类专栏: [安全 网络](#) 文章标签: [网络安全](#) [信息安全](#) [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/HBohan/article/details/119037022>

版权



[安全](#) 同时被 2 个专栏收录

375 篇文章 21 订阅

订阅专栏



[网络](#)

355 篇文章 13 订阅

订阅专栏

## 1 这都是基础



VkZad1dGSXdUbUZOZWs1T1YyeEdXVki4Y0VWU01EVkxWbXhrV2xkVmVGVIVWa3BYVWpBd2VVMHdNVkJVYkVaWVUxWn  
dWVlpGTVVkvk1HUK9WMVY0VIZSV1NsVIRSRWs1VUZrd1BRPT0=

一道base64+base64+base64+base32 即可解出

## 2 就是一个网页

查看源代码发现有注释

```
<!--coding mac >
```

想到苹果系统的DS\_Store

然后源代码发现img标签src直接是网页根目录下，直接后面跟DS\_Store 下载打开发现flag

## 3 银行卡的秘密

下载回来发现是一个pcapng的文件，是一个wireshark回来的文件。

01.pcapng

发现有flag这个zip文件

01.pcapng [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000398	192.168.91.1	192.168.91.108	HTTP	476	GET /flag.zip HTTP/1.1
5	0.000951	192.168.91.108	192.168.91.1	HTTP	566	HTTP/1.1 200 OK (application/zip)

Frame 4: 476 bytes on wire (3808 bits), 476 bytes captured (3808 bits)

- Ethernet II, Src: Vmware\_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware\_f2:4e:17 (00:0c:29:f2:4e:17)
  - Destination: Vmware\_f2:4e:17 (00:0c:29:f2:4e:17)
  - Source: Vmware\_c0:00:08 (00:50:56:c0:00:08)
  - Type: IP (0x0800)
- Internet Protocol Version 4, Src: 192.168.91.1 (192.168.91.1), Dst: 192.168.91.108 (192.168.91.108)
  - Version: 4
  - Header length: 20 bytes
  - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  - Total Length: 462
  - Identification: 0x25c4 (9668)
  - Flags: 0x02 (Don't Fragment)
  - Fragment offset: 0
  - Time to live: 64
  - Protocol: TCP (6)
  - Header checksum: 0xdba7 [correct]
  - Source: 192.168.91.1 (192.168.91.1)
  - Destination: 192.168.91.108 (192.168.91.108)

0000 00 0c 29 f2 4e 17 00 50 56 c0 00 08 08 00 45 00 ...N.P V....E.  
0010 01 ce 25 c4 40 00 40 06 db a7 c0 a8 5b 01 c0 a8 ...%.@. ....[...  
0020 5b 6c 10 ee 00 50 2f 17 ed e1 d1 b1 7a 41 50 18 [...]P/. ...zAP.  
0030 08 05 b4 5d 00 00 47 45 54 20 2f 66 6c 61 67 2e ...].GE T /flag.  
0040 7e 60 70 30 48 54 54 50 2f 21 2e 21 04 0e 48 6f ...HTTP /1.1 U

分析一波

```

D:\CTF>binwalk 01.pcapng
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
1441         0x5A1          Zip archive data, encrypted at least v1.0 to extra
ct, compressed size: 47, uncompressed size: 35, name: flag.txt
1616         0x650          End of Zip archive, footer length: 22

D:\CTF>

```

7006S  
<https://blog.csdn.net/HBohan>

使用foremost自动分离

```

.bash_profile  .config/      .pip/         .tcshrc
[root@Ring0 ~]# foremost 01.pcapng
Processing: 01.pcapng
|foundat=flag.txt
*|
[root@Ring0 ~]# ll
total 16
-rw-r--r-- 1 root root 2084 Nov 27 15:06 01.pcapng
drwxr-xr-x 6 root root 4096 Nov 27 17:24 binwalk
drwxr-xr-x 2 root root 4096 Nov 27 17:04 foremost-1.5.7
drwxr-xr-- 3 root root 4096 Nov 27 22:38 output
[root@Ring0 ~]# cd output/
[root@Ring0 output]# ll
total 8
-rw-r--r-- 1 root root 659 Nov 27 22:38 audit.txt
drwxr-xr-- 2 root root 4096 Nov 27 22:38 zip
[root@Ring0 output]# cd zip/
[root@Ring0 zip]# ll
total 4
-rw-r--r-- 1 root root 198 Nov 27 22:38 00000002.zip
[root@Ring0 zip]#

```

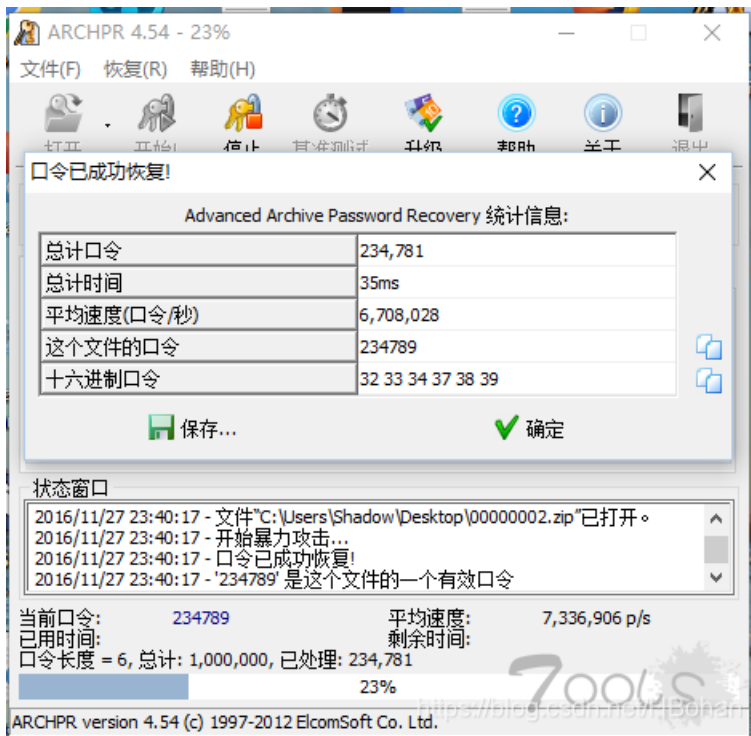
仅将文本发送到当前选项卡

SSH2 xterm 104x26 26,19 1 会话

7006S  
<https://blog.csdn.net/HBohan>

把分离出的zip文件下载到本地，发现里面有一个flag文件但是是加密过的

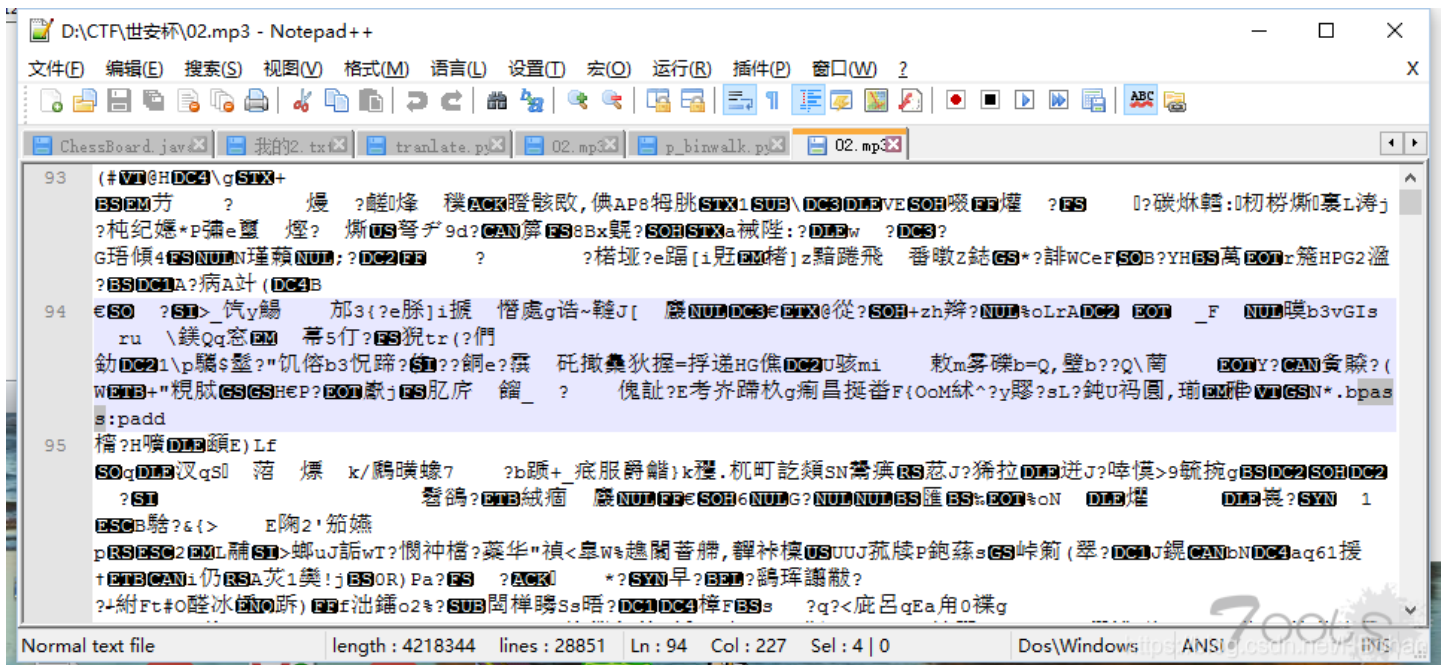
官方给出tips是弱口令，想到0-9 length为6位数。



### 3 我心永恒

然后是一个音频题

打开搜索pass关键字发现密码为padd



歌曲是我心永恒

使用MP3Stego解密

```
C:\WINDOWS\system32\cmd.exe
D:\CTF\世安杯\MP3Stego_1_1_18\MP3Stego>
D:\CTF\世安杯\MP3Stego_1_1_18\MP3Stego>
D:\CTF\世安杯\MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P padd 02.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = '02.mp3' output file = '02.mp3.pcm'
Will attempt to extract hidden information. Output: 02.mp3.txt
the bit stream file 02.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 10092]avg slots/frame = 417.919; b/smp = 2.90; br = 127.988 kbps
Decoding of "02.mp3" is finished
The decoded PCM output file name is "02.mp3.pcm"

D:\CTF\世安杯\MP3Stego_1_1_18\MP3Stego>
```

拿到flag

## 4 密码里的信息

题目给了一段密文

```
;<WEN='M23DI62%-5-#@Y='5Q<7%J55,X.31]
```

用UUencode解密之得到

```
synt{RNJVHSU489tuqqjUS894}
```

发现是凯撒加密过的，谷歌了一个凯撒解密的网站，解密后得到flag



Plaintext:

synt{RNJVHSU489tuqqqiUS894}

- Encrypt
- Decrypt

Ciphertext:

FLAG(eaWUfh489GHDDdwhf894)

- Case sensitive
- Keep non-alphabet characters
- Delete blanks (blocks of 5)

Plaintext-alphabet  52 Signs

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

NOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFGHIJKLM

Ciphertext-alphabet

Key:

+ 13  -  Rot-13 (uppercase only)



不错！我就是静静