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

1 这都是基础

VkZad1dGSXdUbUZOZWs1T1YyeEdXVkl4Y0VWU01EVkxWbXhrV2xkVmVGVlVWa3BYVWpBd2VVMHdNVkJVYkVaWVUxWndWVlpGTVVkVk1HUk9WMVY0VlZSV1NsVlRSRWs1VUZRd1BRPT0=
一道base64+base64+base64+base32 即可解出

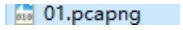
2 就是一个网页

查看源代码发现有注释

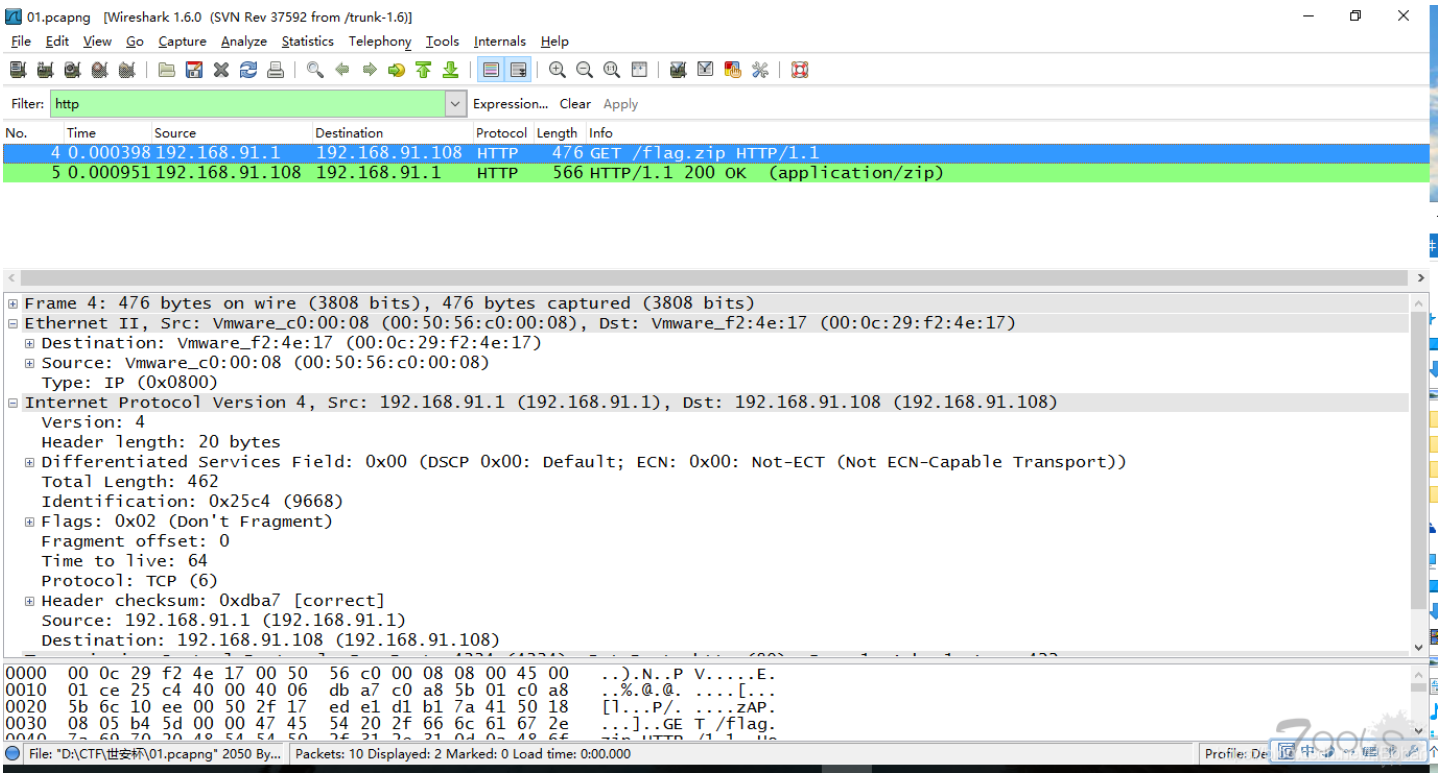
<!—coding mac >
想到苹果系统的DS_Store
然后源代码发现img标签src直接是网页根目录下，直接后面跟DS_Store 下载打开发现flag

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。



发现有flag这个zip文件



分析一波

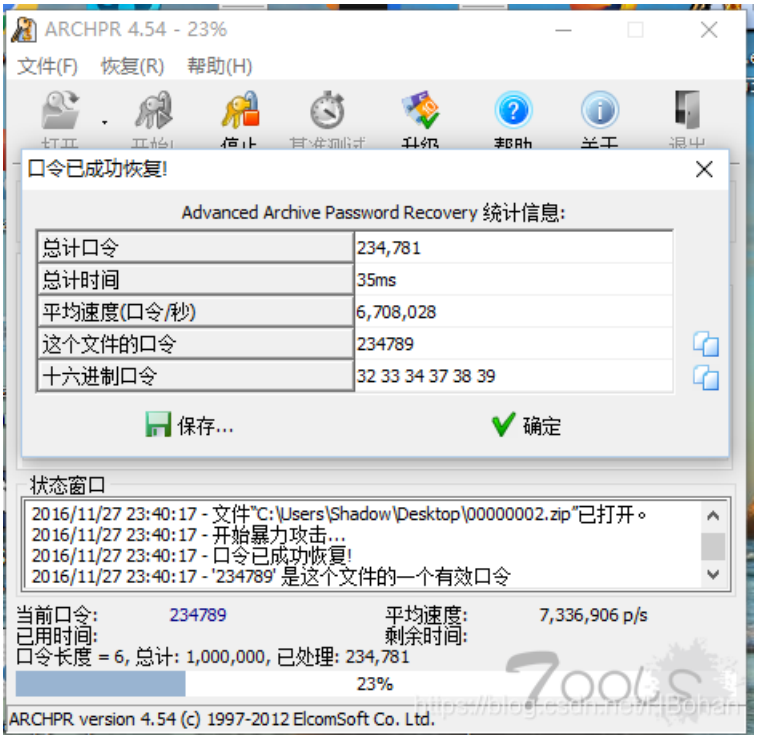
```
D:\CTF>binwalk 01.pcapng
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

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>
```


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]#
```


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

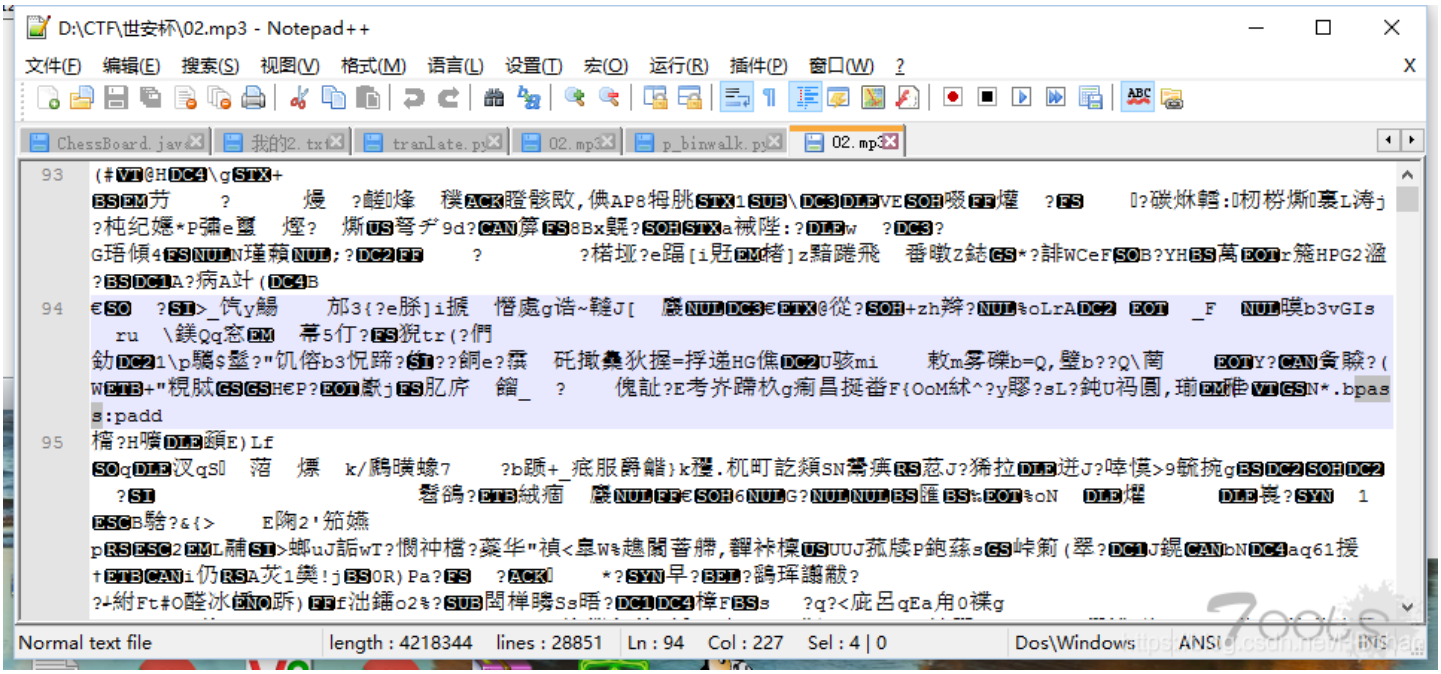
官方给出tips是弱口令，想到0-9 length为6位数。



3 我心永恒

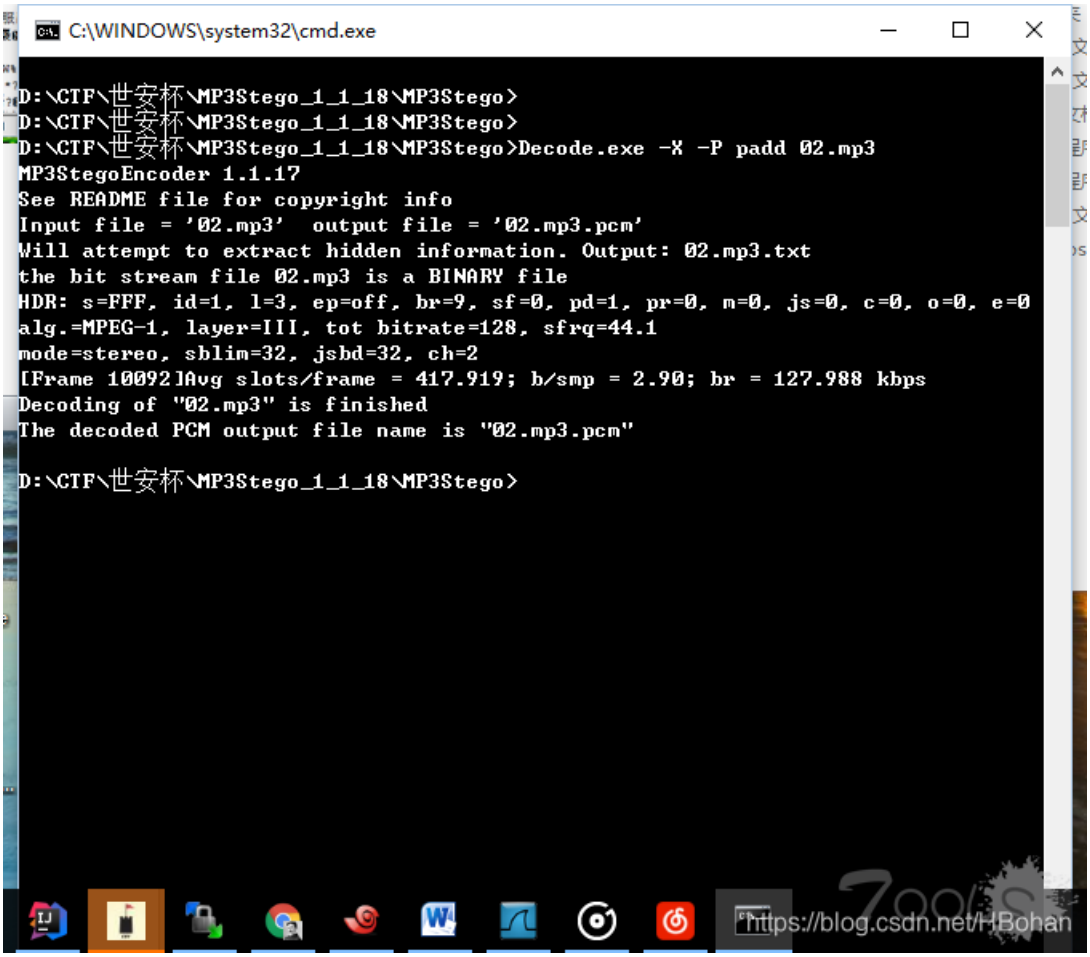
然后是一个音频题

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



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{RNJVHSU489tuqqqjUS894}

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{RNJVHSU489tuqqqjUS894}

Encrypt
Decrypt

Ciphertext:

FLAG{eaWiUfh489GHDDDwhf894}

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

Plaintext-alphabet Parse alphabet >> 52 Signs

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

NOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFGHIJKLM

Ciphertext-alphabet

Key:

+ 13 - Rot-13 (uppercase only)