ctf内存取证----easy_dump

原创

MOLLMY 于 2019-09-15 22:04:07 发布 2333 收藏 11
分类专栏： 网络攻防 CTF

本文链接：https://blog.csdn.net/MOLLMY/article/details/100865618


网络攻防 同时被 2 个专栏收录
4 篇文章 0 订阅
订阅专栏


CTF
5 篇文章 0 订阅
订阅专栏

前一段时间又做了去年护网杯的内存取证题

第一次不参考任何wp提示，自己做，没想到做得挺顺利

Easy_dump writeup

解题步骤

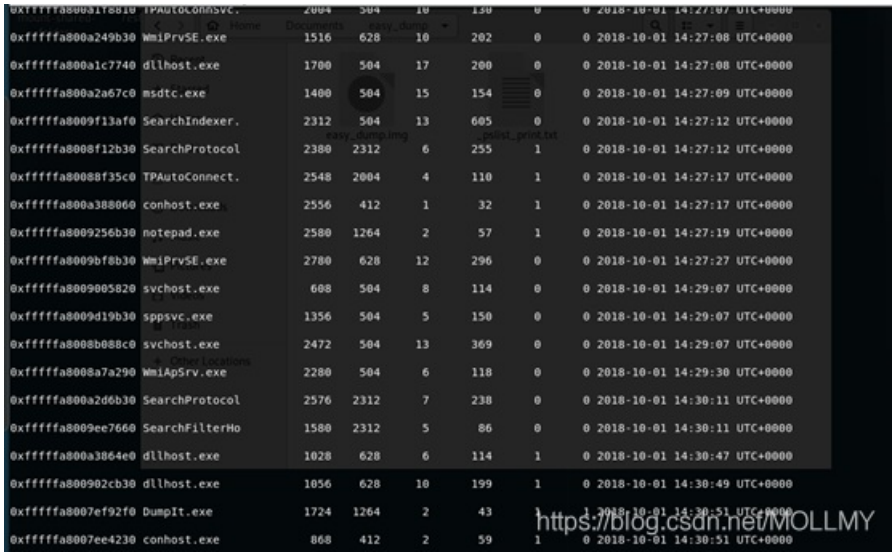
Step 1

Volatility imageinfo

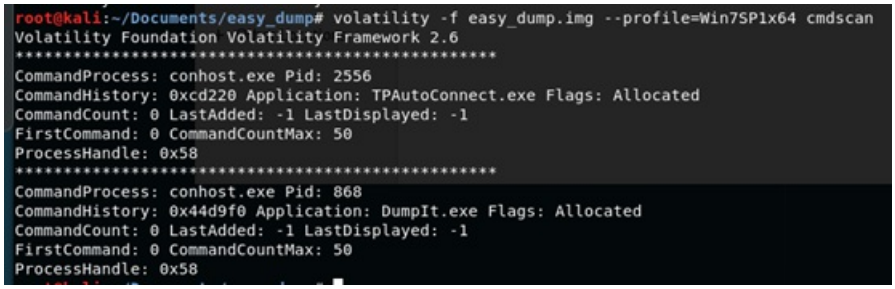
得知系统为Win7SP1x64

Setp 2

查看进程列表



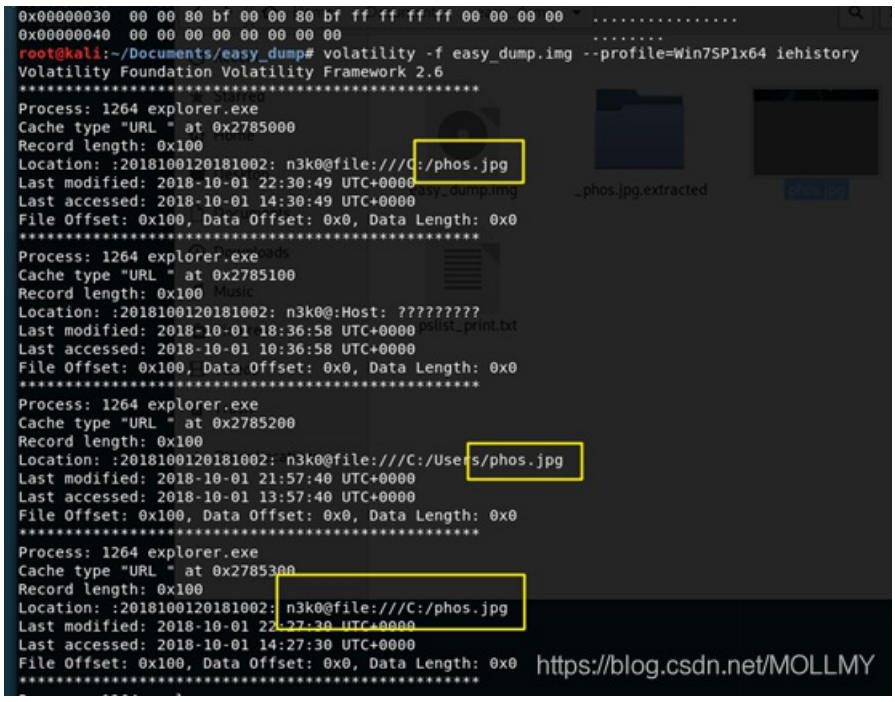
查看命令行历史



没有什么发现

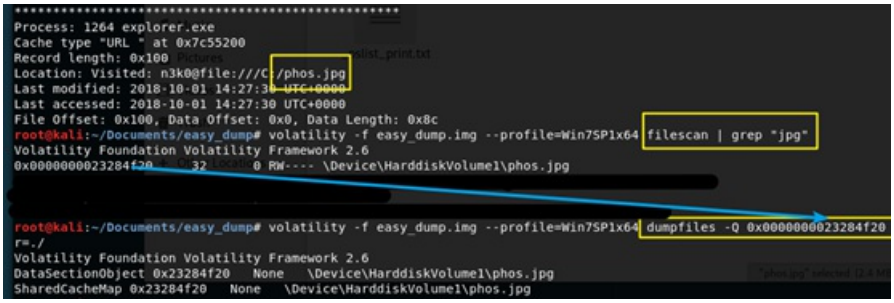
Step 3

执行netscan、iehistory等命令，发现在iehistory中有一个jpg文件

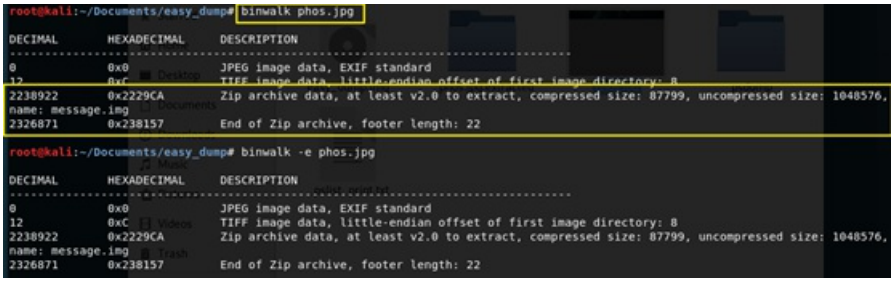


Filescan | grep “jpg” 找到这个jpg文件，

dumpfiles -Q physic_address -D directory_in_which_to_dump导出



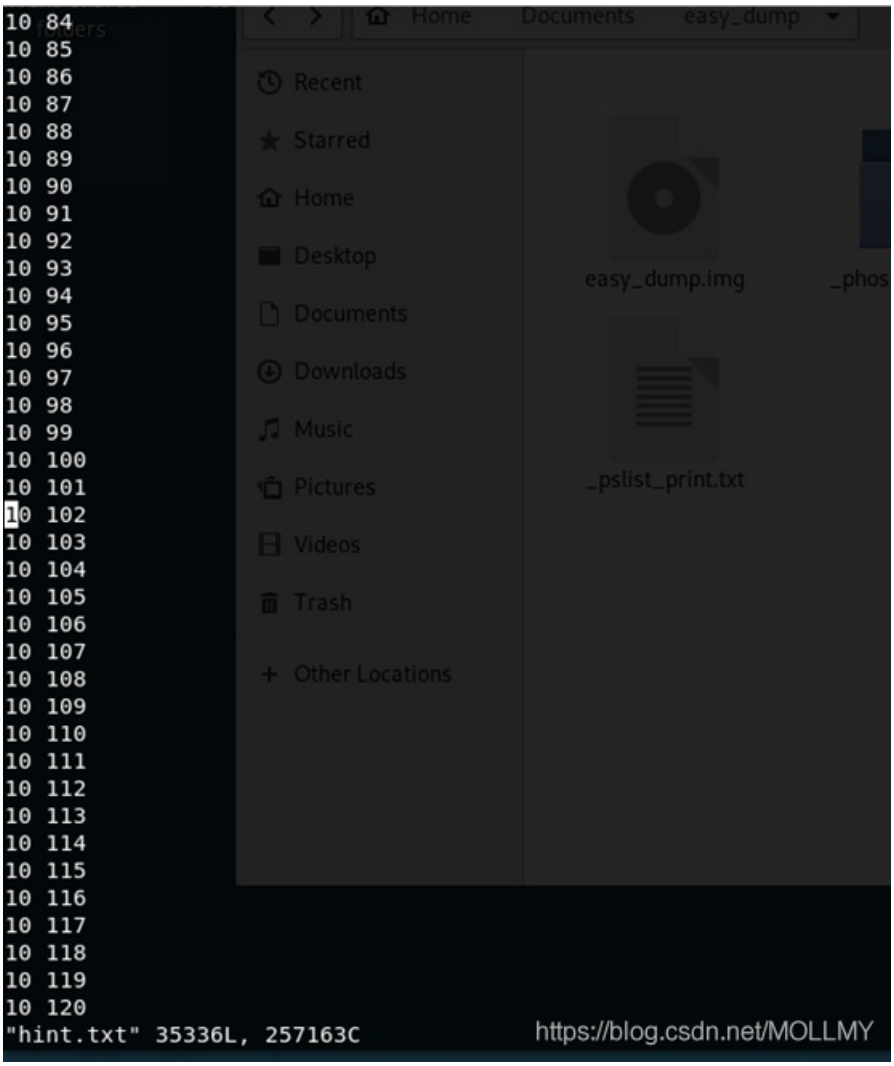
Binwalk phos.jpg发现图片后面附了一个zip文件，



binwalk -e phos.jpg提取文件，解压后得到一个message.img文件，binwalk -e message.img提取到一个hint.txt

Step 4

查看hint.txt



疑似坐标点

将这些数字作为坐标画出来

```
import matplotlib.pyplot as plt
import numpy as np
'''
@author:sunmx
根据二位坐标点绘图
'''
x = []
y = []
with open('hint.txt','r') as f:
    datas = f.readlines()
    for data in datas:
        arr = data.split(' ')
        x.append(int(arr[0]))
        y.append(int(arr[1]))

plt.plot(x,y,'ks',ms=1)
plt.show()
```

二维码内容为“Here is the vigenere key: aeolus, but I deleted the encrypted message.”

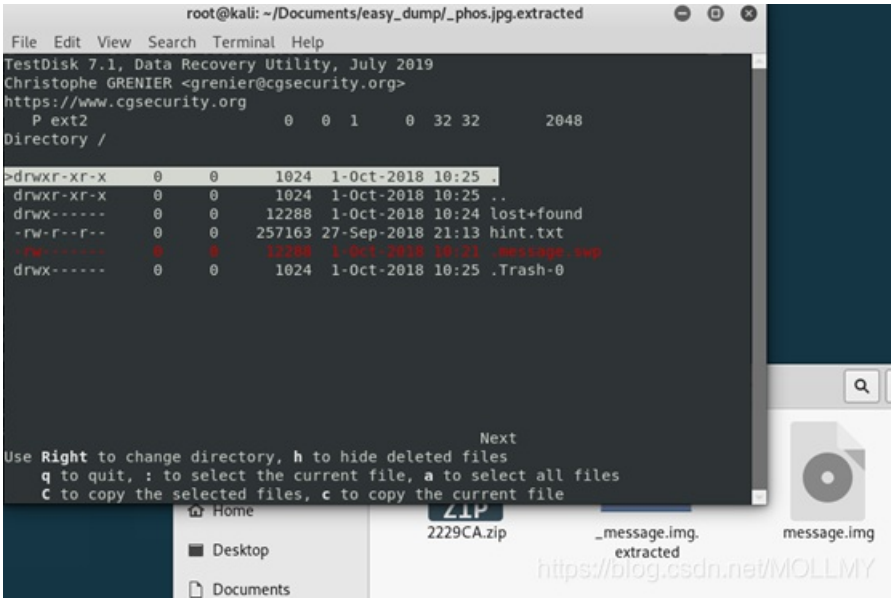
Here is the vigenere key: aeolus, but i deleted the encrypted message。

Step 5

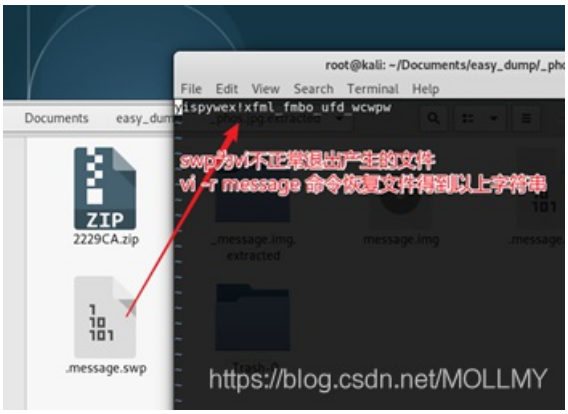
恢复删掉的信息

Testdisk message.img[孙1]

分析，然后list



恢复到当前文件夹，ls -a查看所有的文件包括隐藏文件



恢复这个message文件得到字符串yispywex!xfml_fmbo_ufd_wcwpw

这应该是vigenere加密的密文

Step 6

Vigenere 解密

Key：aeolus

密文：yispywex!xfml_fmbo_ufd_wcwpw

```
'''
@author:sunmx
维吉尼亚密码解密
'''


key = 'aeolus'
cip = 'yispywex!xfml_fmbo_ufd_wcwpw'
asci = 'abcdefghijklmnopqrstuvwxyz'
# 忽略符号，符号仍位于原来的位置
syb = dict()
cip_l = list(cip)
for i in range(len(cip)):
    if cip[i] not in asci:
        syb[i] = cip[i]
        cip_l.pop(cip_l.index(syb[i]))
print(syb)

cipher = ''.join(cip_l)
k_len = len(key)
c_len = len(cipher)
plaintxt = ''
i = 0
while i < c_len:
    j = i % k_len
    k = asci.index(key[j])
    m = asci.index(cipher[i])
    if m < k:
        m += 26
    plaintxt += asci[m-k]
    i += 1

syb_i = syb.keys()
for i in syb_i:
    plaintxt = plaintxt[:i]+syb[i]+plaintxt[i:]

print(plaintxt)
```

或者在线解密[孙2]

yeeeeeet!just_find_and_solve

应该是flag

[孙1]参考https://www.cgsecurity.org/wiki/TestDisk:_undelete_file_for_ext2

https://www.cgsecurity.org/wiki/Testdisk_%E6%93%8D%E4%BD%9C%E6%8C%87%E5%8D%97#.E8.BF.90.

[孙2]https://www.qqxiuzi.cn/bianma/weijiniyamima.php