攻防世界 Misc高手进阶区 3分题 互相伤害!!!

原创

思源湖的鱼 于 2020-11-16 11:49:27 发布 534 收藏 2

分类专栏： ctf 文章标签： ctf 攻防世界 misc

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109717353

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

本篇是互相伤害!!!的writeup

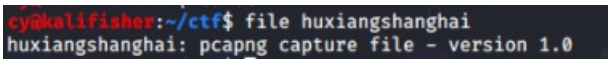
发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个无后缀文件

用file命令看看



是个流量包

扔进wireshark

追踪TCP

发现一堆图片

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · huxiangshanghai.pcapng

```
GET /seclover.php?file=0f17a594524a3488c7f8a691b7f9a800.jpg HTTP/1.1
Host: 192.168.30.139
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 30 Mar 2017 06:50:49 GMT
Server: Apache/2.4.23 (Debian)
Content-Disposition: attachment;filename="0f17a594524a3488c7f8a691b7f9a800.jpg"
Content-Length: 113611
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

......JFIF.....H.H.....C...
```


都导出来

Wireshark · 导出 · HTTP 对象列表

分组	主机名	内容类型	大小	文件名
104	192.168.30.139	application/octet-stream	113 kB	seclover.php?file=0f17a594524a3488c7f8a691b7f9a800.jpg
207	192.168.30.139	application/octet-stream	105 kB	seclover.php?file=1c901bb38602805a3f299fb1ec0ce1e7.jpg
305	192.168.30.139	application/octet-stream	98 kB	seclover.php?file=1f110a79a69aff5f42025a8453e79892.jpg
421	192.168.30.139	application/octet-stream	125 kB	seclover.php?file=3c04de52853c27a30692b64300260da1.jpg
536	192.168.30.139	application/octet-stream	127 kB	seclover.php?file=4e6ad17d81efa1cdf2baa8ae9666198a.jpg
640	192.168.30.139	application/octet-stream	104 kB	seclover.php?file=4fb1fea28ff7634193883bfccaefeb78.jpg
753	192.168.30.139	application/octet-stream	107 kB	seclover.php?file=5e67ac8c6184aab420abffb38bcfff5c.jpg
847	192.168.30.139	application/octet-stream	98 kB	seclover.php?file=6aa487619eeed968211c85576eac9a6b.jpg
946	192.168.30.139	application/octet-stream	102 kB	seclover.php?file=7cd42efa36aab97493c936e5a7feb215.jpg
1057	192.168.30.139	application/octet-stream	108 kB	seclover.php?file=57e5a2cfefb5381b78333c5d50fe9fb4.jpg
1187	192.168.30.139	application/octet-stream	121 kB	seclover.php?file=70bf85eda6b86ee92a5f437f7d83b7e5.jpg
1284	192.168.30.139	application/octet-stream	105 kB	seclover.php?file=82e503c2d71f66c72347a03de58b1bd3.jpg
1394	192.168.30.139	application/octet-stream	121 kB	seclover.php?file=96fd22f539a09f5e0b6876cae78f3e10.jpg
1525	192.168.30.139	application/octet-stream	147 kB	seclover.php?file=4356f2b426ad8355c99e9388a3189c89.jpg
1629	192.168.30.139	application/octet-stream	112 kB	seclover.php?file=0785906b91dba9167fe43da5e4dfadfa.jpg
1730	192.168.30.139	application/octet-stream	107 kB	seclover.php?file=a80c8e93404aed8d87f88fa71e203fa6.jpg
1859	192.168.30.139	application/octet-stream	126 kB	seclover.php?file=b9cd3560d86b8e8992c3d815b64b49dd.jpg
1953	192.168.30.139	application/octet-stream	98 kB	seclover.php?file=b19e02e5bd5bd0ac9342ad047957f0b5.jpg
2054	192.168.30.139	application/octet-stream	96 kB	seclover.php?file=b917666a139b2240115a695d52efe17d.jpg
2156	192.168.30.139	application/octet-stream	109 kB	seclover.php?file=efdd300d51da852d0fd7a33e59b4164b.jpg
2244	192.168.30.139	application/octet-stream	93 kB	seclover.php?file=f44cda8d98b465e9136ff0b6cfc18df6.jpg

翻找下

看到一张图

扫码

复制 U2FsdGVkX1+VpmdLwwhbyNU80MDlK+8t61sewce2qCVztitDMKpQ4fUl5nsAZOI7bE9uL8lW/KLfbs33aC1XXw==

AES解密

在线AES加密、AES解密工具

U2FsdGVkX1+VpmdLwwhbyNU80MDIK+8t61sewce2qCVztitDMKpQ4fUI5nsAZOI7bE9uL8lW/KLfbs33aC1XXw==

CTF

AES加密 AES解密 清空输入框 复制结果文本

668b13e0b0fc0944daf4c223b9831e49

得到`668b13e0b0fc0944daf4c223b9831e49`

断了
估计别的图片还有信息

根据题目提示
直接找到这张

binwalk看看

```
cy@kalifisher:~/ctf/新建文件夹$ binwalk seclover.php%3ffile\=70bf85eda6b86ee92a5f437f7d83b7e5.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
12357         0x3045          Zip archive data, encrypted at least v2.0 to extract, compressed size: 10
493, name: a1d63bb3ed1f9df89b72375f1ed79e5d.jpg
121462        0x1DA76         End of Zip archive, footer length: 22
```

发现是个zip
改后缀
解压

需要密码

将上面得到的`668b13e0b0fc0944daf4c223b9831e49`输入

解压
得到

扫码

整个二维码

复制 扔下内衣真有一线生机？？？
交出内裤才有活路！！！！

里面的小二维码

得到flag

结语

知识点

- wireshark
- AES
- 图片中的压缩包