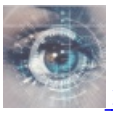
xctf攻防世界 MISC高手进阶区 互相伤害

原创

l8947943 已于 2022-02-03 23:18:25 修改 1648 收藏 5

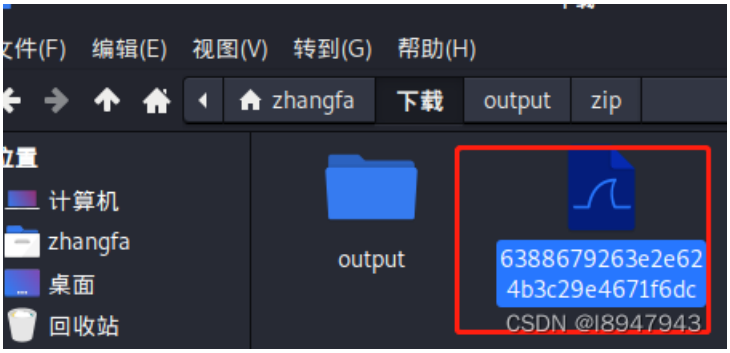
分类专栏： 攻防世界misc之路 文章标签： 安全 web安全

于 2022-02-03 23:14:54 首次发布



1. 进入环境，下载附件

题目给的是一个文件，我们直接扔进kali中，发现是流量包，如图：



使用file命令查看该文件类型，发现也是提示是pcapng文件，如图：

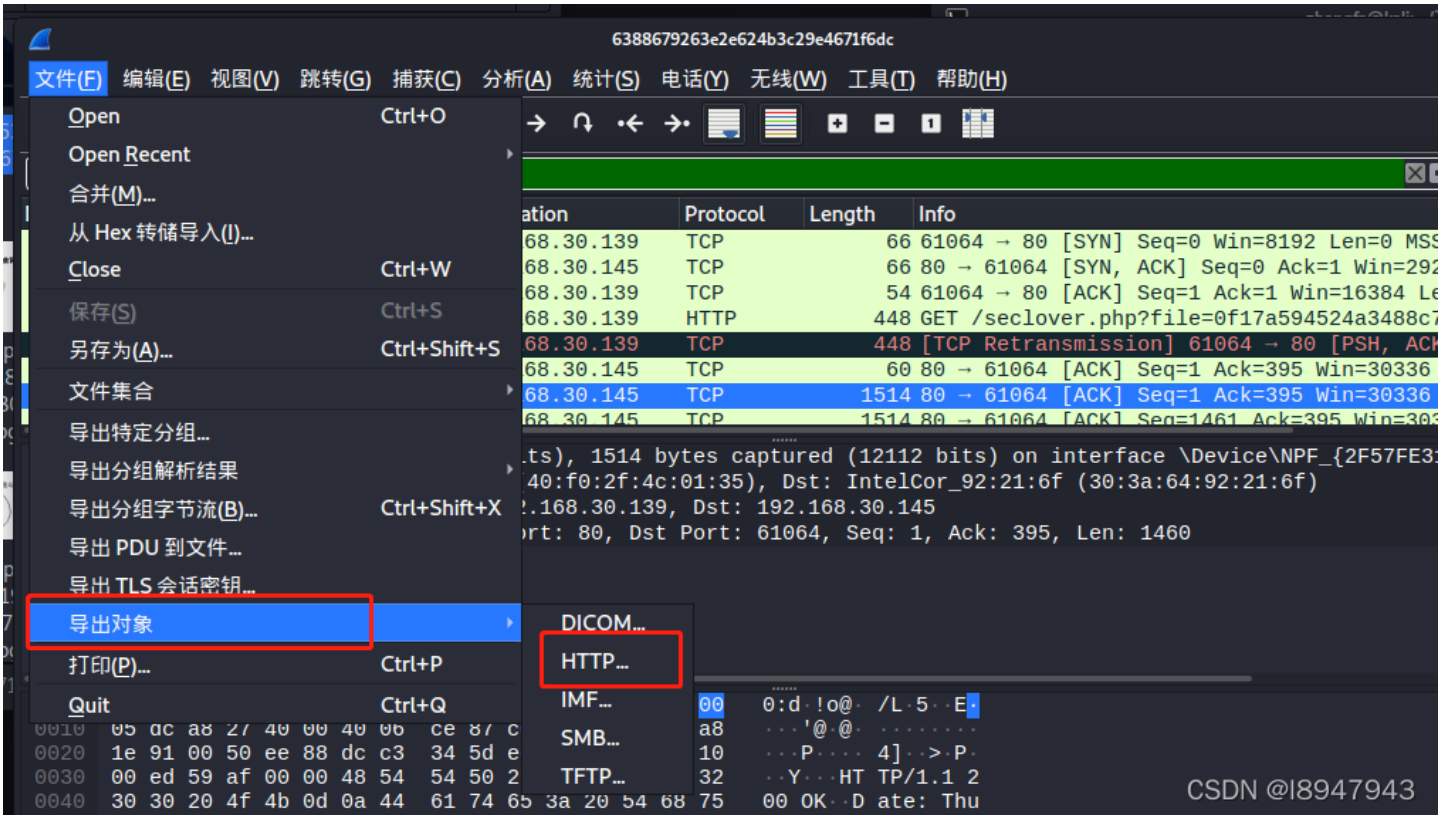
2. 问题分析

1. **提取数据**

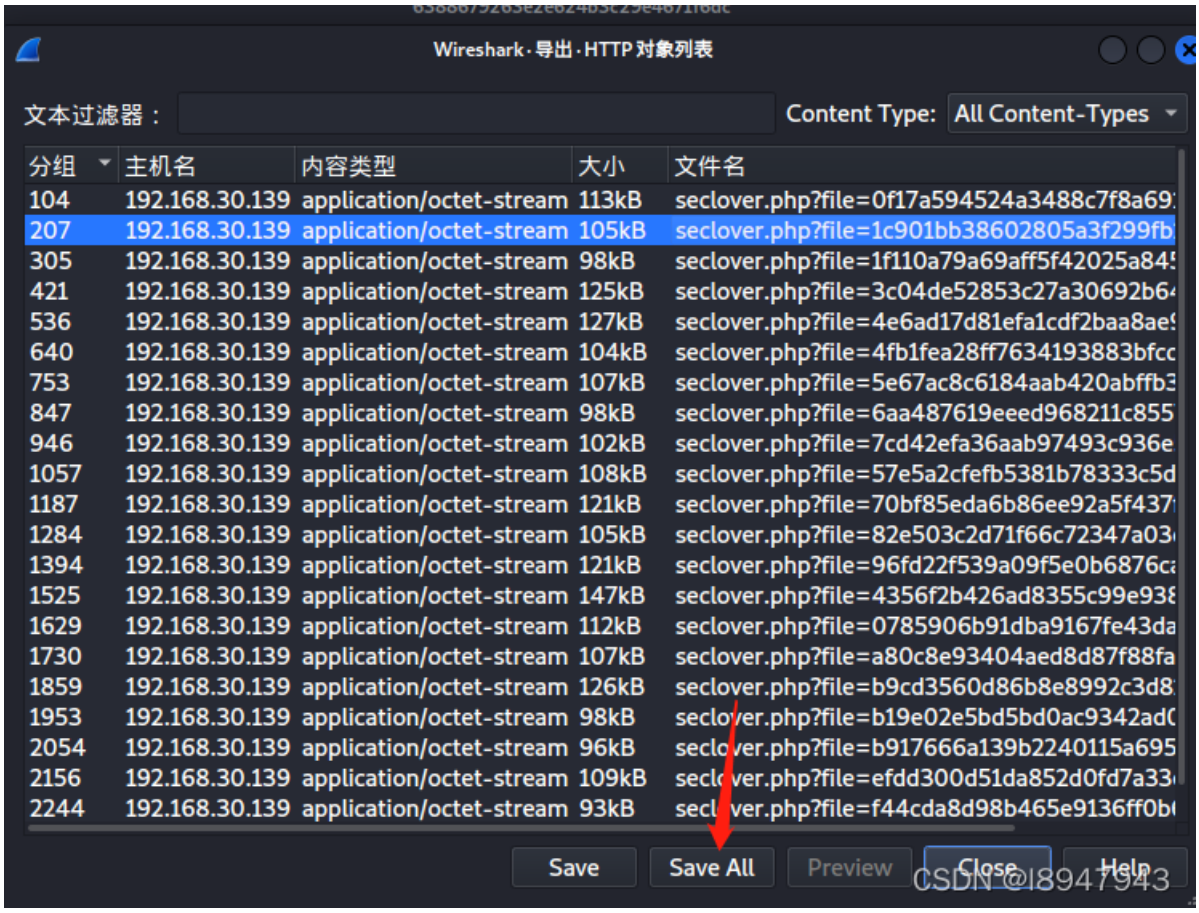
   我们打开文件，发现很多tcp流，我们追踪流可以看到，传输过程中有很多jpg文件，如图：

```
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...
```


我们使用wireshark自带的提取数据功能，导出数据：

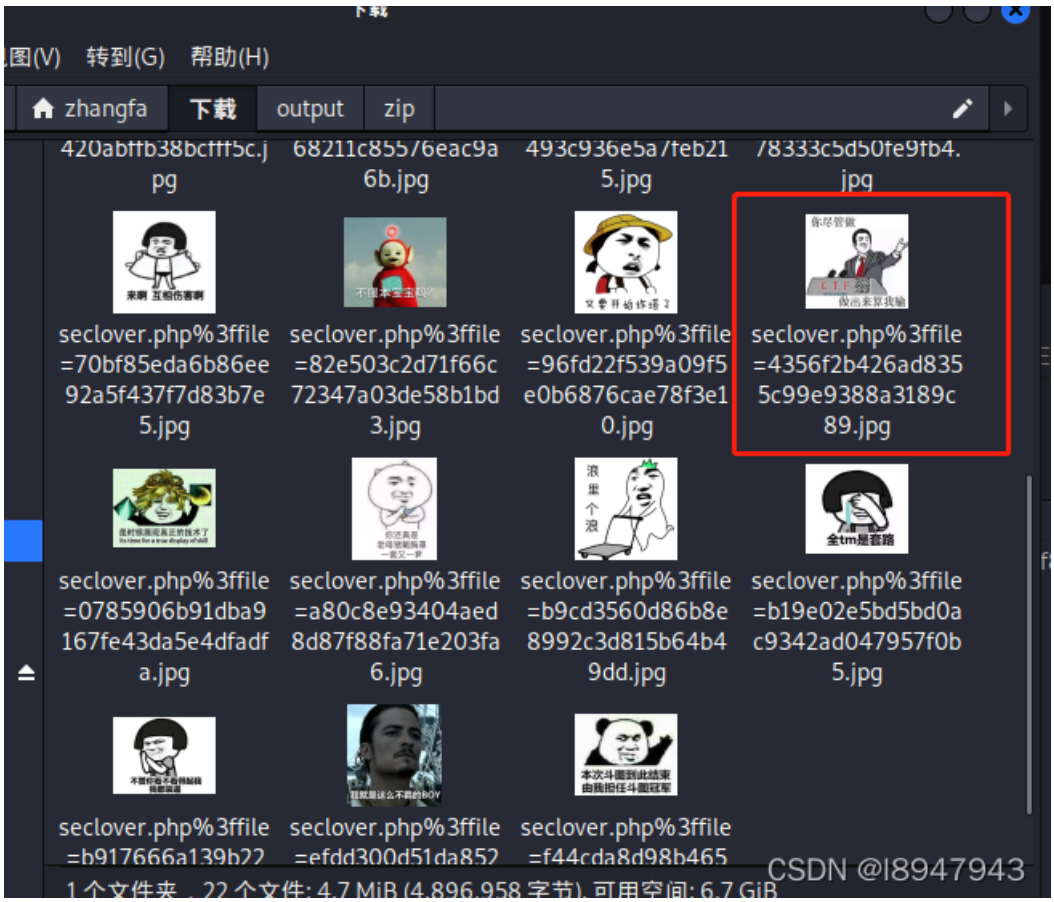


选择save all即可，如图：



2. **发现二维码**

发现一张奇怪的图片，包含二维码：



使用在线二维码解析：https://cli.im/deqr/，提取的数据为`U2FsdGVkX1+VpmdLwwhbyNU80MDlK+8t61sewce2qCVztitDMKpQ4fUl5nsAZOI7 bE9uL8lW/KLfbs33aC1XXw==`

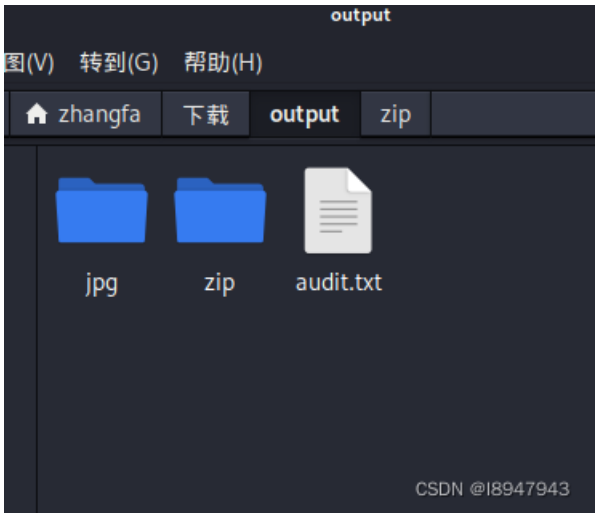
感觉是像base64编码，解码后乱七八糟的。不知道出发点在哪里，查看了wp后才发现，该编码是AES解密，密码为图中的CTF，在线工具地址为：http://www.jsons.cn/aesencrypt/，解密后如图：

密码为：`668b13e0b0fc0944daf4c223b9831e49`

3. **找到隐藏文件**

   使用binwalk后发现每张图都有zip隐藏文件，人麻了，但是唯独这个图是wp中的合理图片，如图：

使用foremost进行分离，得到zip压缩包：



有解压密码，使用刚刚的AES解密密码输入，得到解压后的二维码，如图：

搁着还是个俄罗斯套娃，拖到最大，扫描最里面的二维码：

扫描后得到最终的答案：`flag{97d1-0867-2dc1-8926-144c-bc8a-4d4a-3758}`