




BUUCTF: [ACTF新生赛2020]swp

原创

末初  于 2020-07-23 11:13:17 发布  1776  收藏

分类专栏: [CTF_MISC_Writeup](#) 文章标签: [ACTF新生赛2020 swp](#)

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/mochu7777777/article/details/107531389>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 46 订阅

订阅专栏

题目地址: [https://buuoj.cn/challenges#\[ACTF%E6%96%B0%E7%94%9F%E8%B5%9B2020\]swp](https://buuoj.cn/challenges#[ACTF%E6%96%B0%E7%94%9F%E8%B5%9B2020]swp)

Challenge 88 Solves

[ACTF新生赛2020]swp

24

得到的 flag 请包上 flag{} 提交。

[attachment.tar](#)

Flag

Submit

<https://blog.csdn.net/mochu7777777>

This PC > Local Disk (C:) > Users > Administrator > Downloads > tmp

Name	Date modified	Type	Size
PaxHeader	7/23/2020 10:49 AM	File folder	
_wget.zip	3/5/2020 6:03 PM	ZIP 压缩文件	1 KB
wget.zip	3/5/2020 6:03 PM	ZIP 压缩文件	6,885 KB

wget.zip - Bandizip 6.27

文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 帮助(H)

打开 解压 新建 添加 删除 测试 查看 代码页

名称	压缩后大小	原始
wget.pcapng	7,049,246	8,066

<https://blog.csdn.net/mochu7777777>

解压后在 `wget.zip` 中发现个数据包, 解压后用 `wireshark` 打开, 看着像 `http` 数据传输

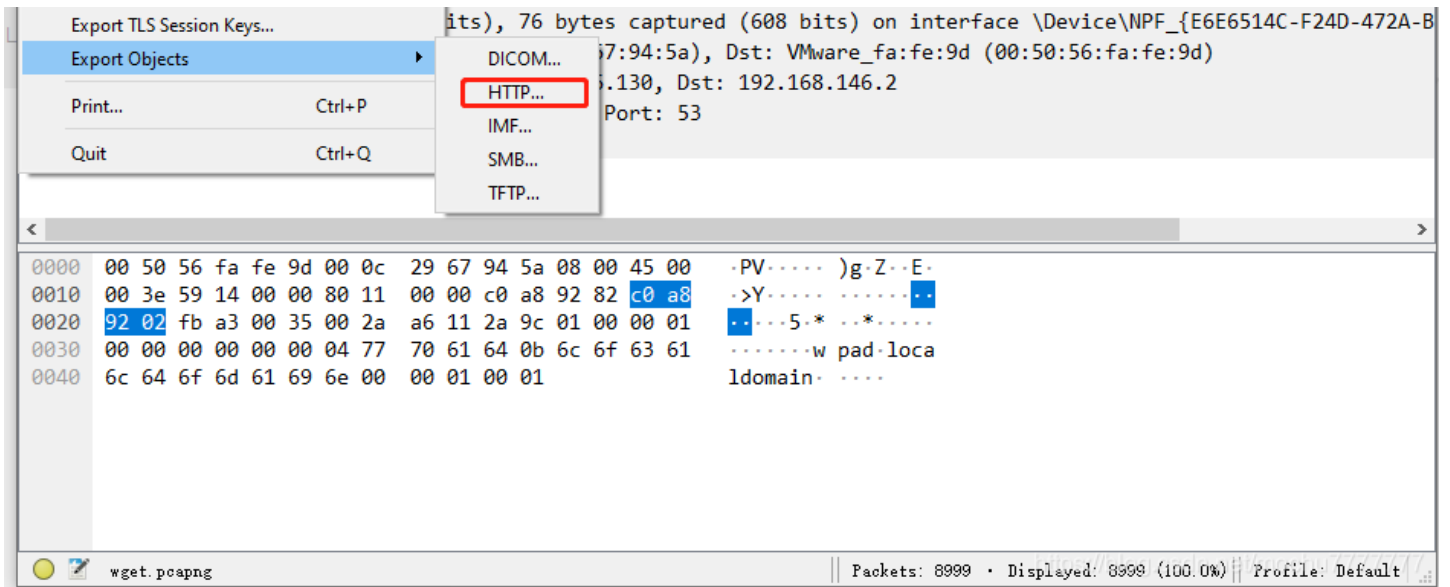
导出http

wget.pcapng

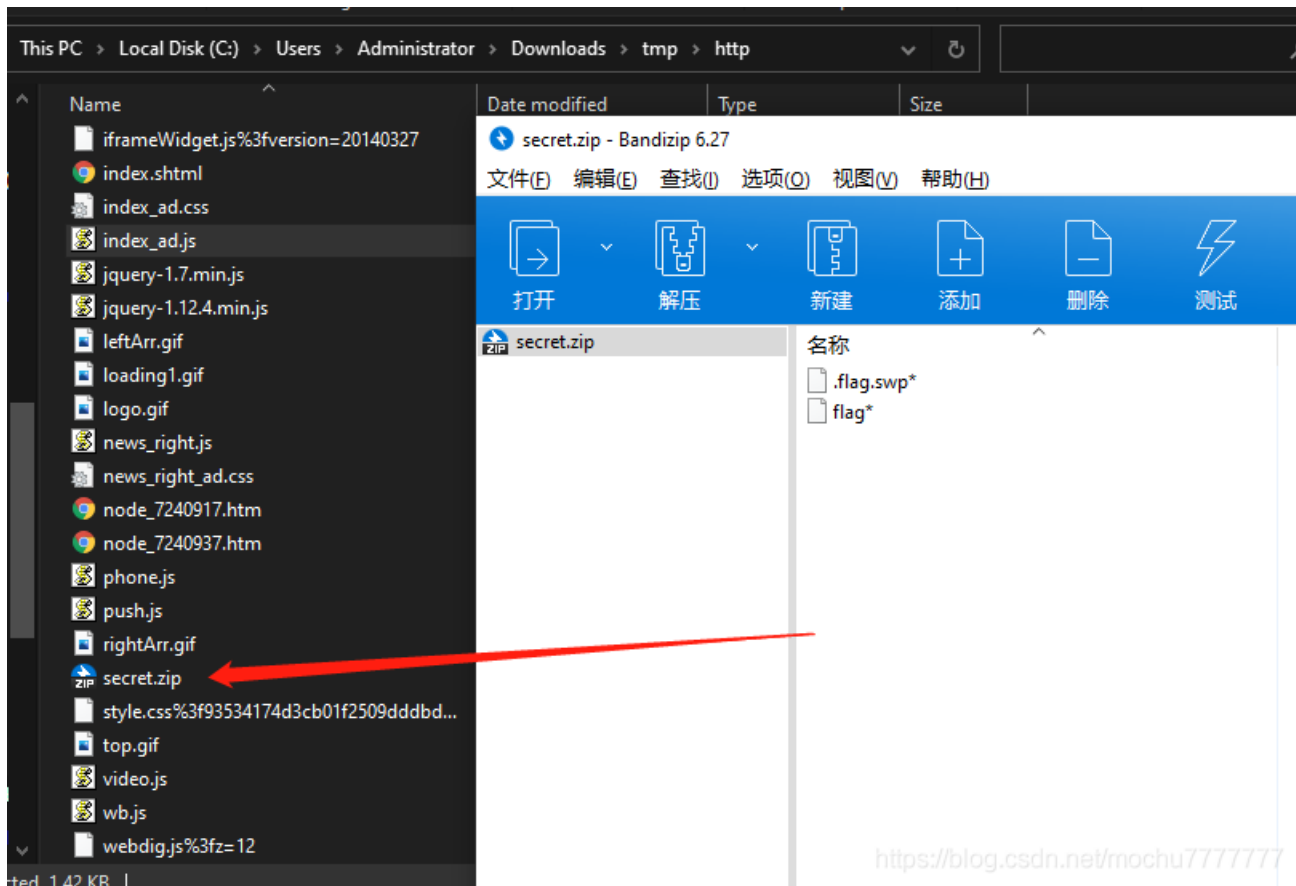
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

- Open Ctrl+O
- Open Recent
- Merge...
- Import from Hex Dump...
- Close Ctrl+W
- Save Ctrl+S
- Save As... Ctrl+Shift+S
- File Set
- Export Specified Packets...
- Export Packet Dissections
- Export Packet Bytes... Ctrl+Shift+X
- Export PDUs to File...

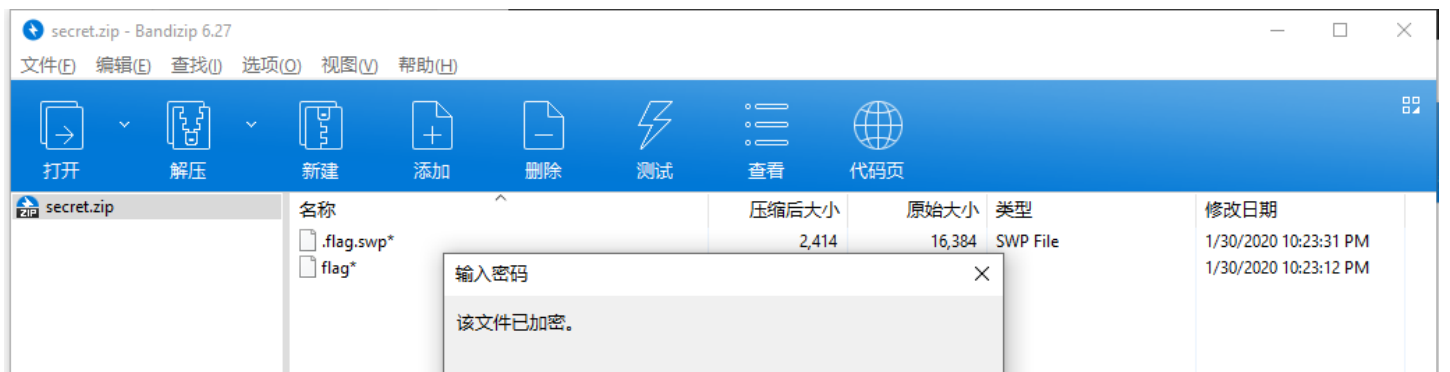
	Destination	Protocol	Length	Info
130	192.168.146.2	DNS	76	Standard query 0x2a9c A wpad...
1	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad...
1dd2:e58...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad...
1	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad...
1dd2:e58...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad...
1dd2:e58...	ff02::1:3	LLMNR	84	Standard query 0xe50d A wpad
1	224.0.0.252	LLMNR	64	Standard query 0xe50d A wpad
1dd2:e58...	ff02::1:3	LLMNR	84	Standard query 0xe50d A wpad
1	224.0.0.252	LLMNR	64	Standard query 0xe50d A wpad
130	192.168.146.2	DNS	76	Standard query 0x2a9c A wpad...
1	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad...

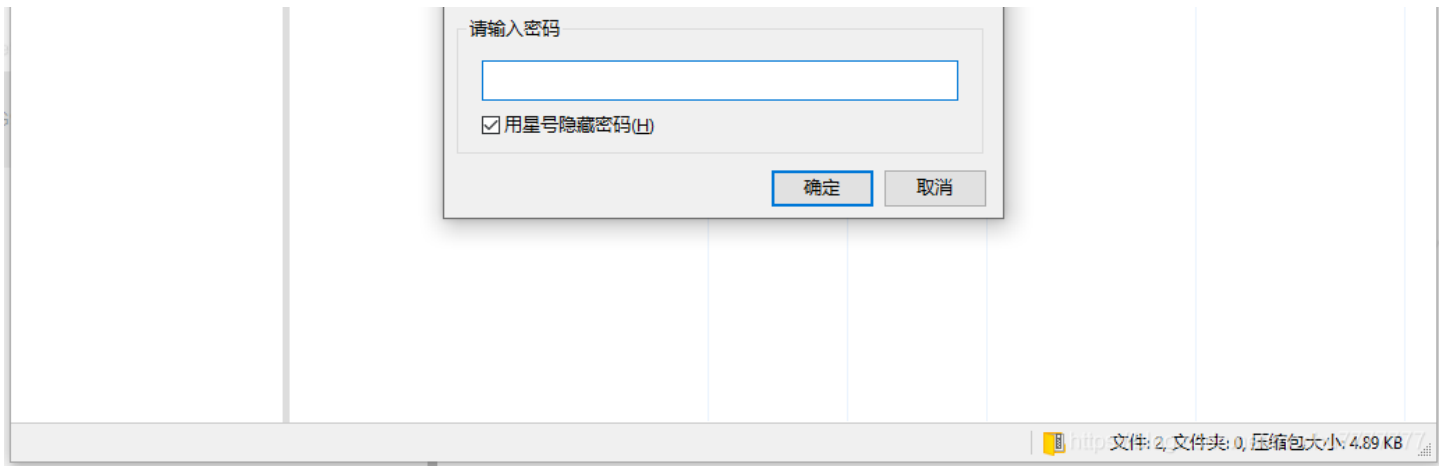


在导出的文件中发现一个 `secret.zip`，看一眼是啥



解压提示需要输入密码，经验稍微有点的都猜得到可能是 `zip伪加密`





使用 `ZipCenOp.jar` 修复, `ZipCenOp.jar`下载地址: <https://github.com/fox-huyu/ZipCenOp.jar>

```
java -jar .\ZipCenOp.jar r .\secret.zip
```

或者使用 `winhex` 等工具修改16进制标志位也可

Name	Date modified	Type	Size
.flag.swp	1/30/2020 10:23 PM	SWP File	16 KB
flag	1/30/2020 10:23 PM	File	9 KB



```
actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
```