

BUUCTF [ACTF新生赛2020]swp

原创

F10NAF11pp3d 于 2020-09-24 19:18:27 发布 437 收藏

分类专栏: BUUCTF

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/m0_46481239/article/details/108765830

版权



[BUUCTF 专栏收录该内容](#)

24 篇文章 1 订阅

订阅专栏

下载后解压得到一个wget.zip,再解压得到wget.pcapng

名称	修改日期	大小	种类
wget.pcapng		8.1 MB	文稿
wget.zip		7 MB	ZIP 归档

把数据包放入Wireshark里分析一下

猜测http数据传输, 导入http对象

File(F) Edit(E) View(V) Go(G) Capture(C) Analyze(A) Statistics(S) Tools(T) Help(H)

No.	Time	Source	Destination	Protocol	Length	Info
46.130	192.168.146.2			DNS	76	Standard query 0x2a9c A wpad.localdomain
46.1	224.0.0.251			MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
6:1dd2:e58...	ff02::fb			MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
46.1	224.0.0.251			MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
6:1dd2:e58...	ff02::fb			MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
6:1dd2:e58...	ff02::1:3			LLMNR	84	Standard query 0xe50d A wpad
46.1	224.0.0.252			LLMNR	64	Standard query 0xe50d A wpad
6:1dd2:e58...	ff02::1:3			LLMNR	84	Standard query 0xe50d A wpad
46.1	224.0.0.252			LLMNR	64	Standard query 0xe50d A wpad
46.130	192.168.146.2			DNS	76	Standard query 0x2a9c A wpad.localdomain
224.0.0.251				MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
ff02::fb				MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
224.0.0.251				MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
ff02::fb				MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
15 1.002054	192.168.146.1			TFTP...		
16 1.002281	fe80::bc70:1002:e58...		ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
17 1.003273	fe80::bcf6:1dd2:e58...		ff02::1:3	LLMNR	84	Standard query 0x8b53 A wpad
18 1.003273	192.168.146.1		224.0.0.252	LLMNR	64	Standard query 0x8b53 A wpad

> Frame 6757: 982 bytes on wire (7856 bits), 982 bytes captured (7856 bits) on interface 0
> Ethernet II, Src: Vmware_fa:fe:9d (00:50:56:fa:fe:9d), Dst: Vmware_67:94:5a (00:0c:29:67:94:5a)
> Internet Protocol Version 4, Src: 47.107.33.15, Dst: 192.168.146.130
> Transmission Control Protocol, Src Port: 81, Dst Port: 50020, Seq: 4381, Ack: 434, Len: 928
> [4 Reassembled TCP Segments (5308 bytes): #6754(1460), #6755(1460), #6756(1460), #6757(928)]
> Hypertext Transfer Protocol
> Media Type

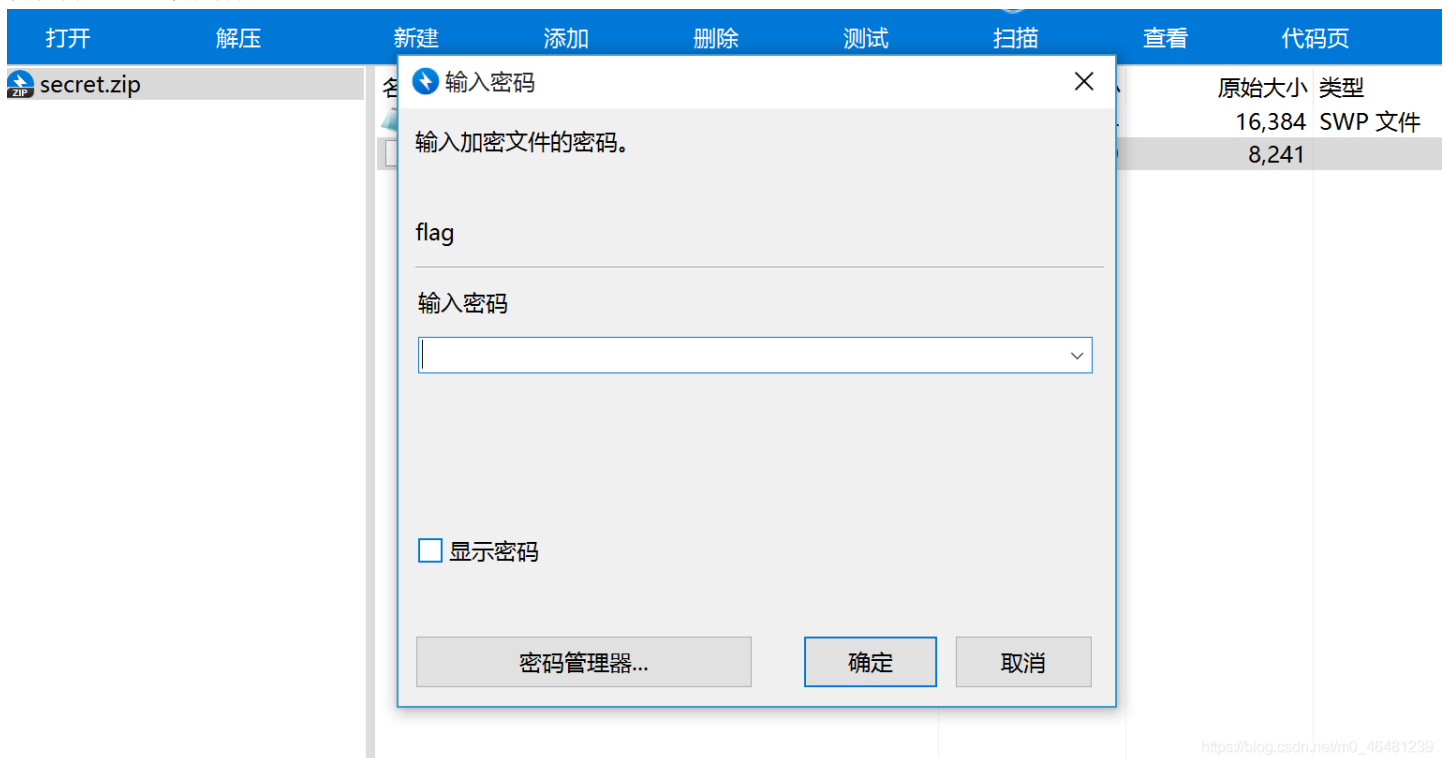
可以发现在导出的文件中发现secret.zip,保存下来

Wireshark · 导出 · HTTP 对象列表

分组	Hostname	Content Type	Size	Filename
4250	images.china.cn	image/jpeg	23 kB	672a3c01-f53d-4ef1-bf29-dc55eb3cea73.jpg
4286	images.china.cn	image/jpeg	14 kB	ac9e178530e1167afd0f56.jpg
4336	images.china.cn	image/gif	13 kB	leftArr.gif
5076	cl0.webterren.com	image/gif	34 bytes	link%3Furl%3D54EYU6YhA5wHwIFHSBTynQp_X5tyL
5120	cl.webterren.com	image/gif	34 bytes	link%3Furl%3D54EYU6YhA5wHwIFHSBTynQp_X5tyL

5126	images.china.cn	image/png	1152 kB	cbbef0d-4317-4f81-a157-4947d838ce59.png
5153	tv.cctv.com	text/html	2762 bytes	index.shtml
5182	push.zhanzhang.baidu.com	text/javascript	281 bytes	push.js
5226	js.t.sinajs.cn	application/x-javascript	4312 bytes	bundle.js?version=20150130.02
5236	js.t.sinajs.cn	application/x-javascript	15 kB	client.js?version=20150130.02
5276	js.t.sinajs.cn	application/x-javascript	88 kB	iframeWidget.js?version=20140327
5290	timimg.sjs.sinajs.cn	image/gif	796 bytes	loading1.gif
5340	www.cctv.com	application/javascript	7382 bytes	a2.js
5383	p5.img.cctvpic.com	image/jpeg	7292 bytes	35f51c0c428a4b19834084f8e29e0e22-79.jpg
5385	r.img.cctvpic.com	text/css	1316 bytes	style.css?93534174d3cb01f2509dddbd55f5d495
5464	p4.img.cctvpic.com	image/jpeg	7193 bytes	cf0219df98aa4ac699c2b520bb0992f1-40.jpg
5556	api.share.baidu.com	image/gif	0 bytes	content_683139.htm
5690	widget.weibo.com	text/html	0 bytes	aj_relationship.php?fuid=1791805181&callback=ST
5803	js.data.cctv.com	application/javascript	126 kB	_aplus_plugin_cctv.js...plus_plugin_aplus_u.js
5919	p.data.cctv.com	image/gif	43 bytes	v.gif?logtype=0...title=%E6%8E%A8%E5%B9%BF1_9
6757	47.107.33.15:81	application/zip	5015 bytes	secret.zip
7792	47.107.33.15:81	text/html	320 bytes	hint.html
7796	47.107.33.15:81	text/html	287 bytes	favicon.ico

发现需要密码才能打开



猜测是zip伪加密，利用工具ZipCenOp.jar进行修复

ZipCenOp.jar下载地址：

<https://github.com/fox-huyu/ZipCenOp.jar>

打开输入：

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

```

PS C:\Tools\Misc\ZipCenOp.jar> java -jar .\ZipCenOp.jar r .\secret.zip
>>>
java.lang.NullPointerException
  at zip.CenOp$1.run(CenOp.java:97)
  at java.security.AccessController.doPrivileged(Native Method)
  at zip.CenOp.clean(CenOp.java:89)
  at zip.CenOp.operate(CenOp.java:80)
  at zip.CenOp.main(CenOp.java:32)
  at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
  at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
  at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
  at java.lang.reflect.Method.invoke(Unknown Source)
  at org.eclipse.jdt.internal.jarinjarloader.JarRsrcLoader.main(JarRsrcLoader.java:58)
success 0 flag(s) foundPS C:\Tools\Misc\ZipCenOp.jar> java -jar .\ZipCenOp.jar r .\secret.zip
>>>
success 2 flag(s) foundPS C:\Tools\Misc\ZipCenOp.jar>

```

https://blog.csdn.net/m0_46481239

secret.zip修复成功
打开看见flag

名称	压缩后大小	原始大小	类型
.flag.swp	2,414	16,384	SWP 文件
flag	2,329	8,241	

flag - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

      =
      h
      "
      Y
      libc.so.6 puts __cxa_finalize __libc_start_main GLIBC_2.2.5
      _ITM_deregisterTMCloneTable __gmon_start__ _ITM_registerTMCloneTable
      u i 1 ? ? 0 ? ?
      ? ? ? ? ? ? ? ? ? ? ? ?
      ? ? ? ? ? ? ? ? ? ? ? ?
      H?H?? H?t 蠪? 5? %? @? %? h 猷
      %? f? 1 鞠壯^H峯H秣銷TL?? H? H? ? ? ?D H?? UH?? H9
      鳧文t?H?Z H?t] 鄱. ? ? ]?@ f. ? ? H?i H?b UH) 藹文H隆 ?H姓H H?t^]
      鄱? ? ]?@ f. ? ? €=? u/H?? UH文t^H?? ? 鑠 ?? ? ]?€
      竺f?D UH文]聞 UH文H?? 杵? ? ]昵. ? ? □D AWAVI壺AUATL?F□ UH?
      F□ SA扶I髫L) 鋼拔□H筊□鑄? H味t 1?? L李L髫D彗A □蹶兜□H9 賤闔颯□□A
      \A^A 腓f. ? ? 竺 H?H?H? ? ? actf{c5558bcf-26da-4f8b-b181-
      b61f3850b9e5} □□□;8 □ □ 恣 ? ^? ? ? T & ? L ?
      ? , □ □ □zR □x□□□^□□?□□□ 例 + □
      □zR □x□□□^□□? $ ? ? □□F□□J□□w□€ ?□;*3$" □ □ D
      X? □ \ Z? □ A□□?C□R^□□ □ D | `? e B□□?
      B□□?E□ ?B□ (?H□0?H□8?M□@r□8A□0A□(B□ B□□B□□B□□ □ ? 堉

```

https://blog.csdn.net/m0_46481239