

攻防世界-Misc-新手练习记录

原创

大千SS 于 2019-04-13 19:01:57 发布 15293 收藏 15

分类专栏: [攻防世界](#) 文章标签: [攻防世界 Misc](#)

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/zz_Caleb/article/details/89287031

版权



[攻防世界](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

ext3

下载文件, 文件名是Linux, 拿到kali中看下文件类型:

```
root@kali:~# file linux
linux: Linux rev 1.0 ext3 filesystem data, UUID=cf6d7bff-c377-403f-84ae-956ce3c99aaa
```

ext3就是Linux的一个文件系统, strings查看一下有没有flag这样的字符串:

```
root@kali:~# strings linux | grep flag
.flag.txt.swp
flag.txttt.swx
~root/Desktop/file/07avZhikgKgbF/flag.txt
.flag.txt.swp
flag.txttt.swx
.flag.txt.swp
flag.txttt.swx
```

flag应该就在这个flag.txt中了, 把这个文件系统挂载到Linux上:

```
mount linux /mnt
```

挂上去之后看一下/mnt/下的文件, 用命令ls -al /mnt/, 可以看到上面strings查找到的O7avZhikgKgbF, flag.txt就在这个目录里, 得到文件内容为: ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=, base64解码即可。

give_you_flag

把动图保存下来，将每帧分开，看到地50帧有个二维码样子的东西：



这个二维码少了三个角的定位符，没有定位符肯定是扫不出来东西的，手动画上定位符：



扫描得flag。

pdf


```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e  
flag = ''  
for i in range(0,len(string), 2):  
    s = "0x" + string[i] + string[i+1]  
    flag += chr(int(s, 16) - 128)  
print(flag)
```

如来十三掌

真是要念经啊：

夜哆悉諳多苦奢陀奢諳冥神哆盧穆幡三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟
寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸
哆遠薩得槃漫夢盧幡亦醯呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽諳沙
楞鉢三死怯摩大蘇者數一遮

与佛论禅：<http://www.keyfc.net/bbs/tools/tudoucode.aspx>

得到base64码：MzkuM3gyMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

但是要先进行ROT13然后再base64解码：

```
flag{bdscjhbkmnfrdhbvckijndskvbkjdsab}
```

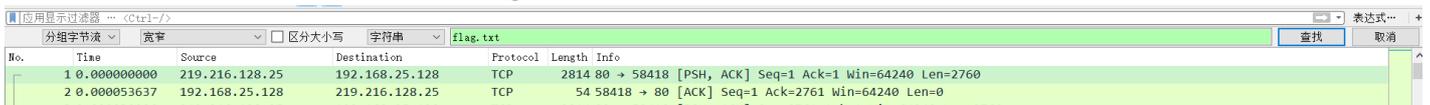
base64stego

参考：https://blog.csdn.net/zz_Caleb/article/details/89298335

功夫再高也怕菜刀

foremost分解出来一个加密的压缩包，里面是flag.txt文件，不是伪加密。

wireshark打开文件，分组字节流查找flag.txt：



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	219.216.128.25	192.168.25.128	TCP	2814	80 → 58418 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2760
2	0.000053637	192.168.25.128	219.216.128.25	TCP	54	58418 → 80 [ACK] Seq=1 Ack=2761 Win=64240 Len=0

查找到第1150个包时，追踪流看到：

Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · 6666.pcapng

```
POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 204999

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRlc3B5YXlFZlZjY3ZjZiIiwMcIwP0BzZXRfdGltZV9saw1pdCgWkTtAc2V0X2h2Z1jX3
F1b3Rlc19ydw50aw1KDAp02Vjag8oIi0%2BfCIp0zskzj1iYXNlNjRfZGVjb2RlKCRfUE9TVF5ieJeiXSk7JGM9JF9QT1NUWjY6MiJdOyRjPjXN0cl9yZXBsYW
NlK3C3cciIsiiSjGMpOyRjPjXN0cl9yZXBsYWNlK3C3c3IiIjIjGMpOyRidwY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTSkaSs9MikkYnVmLj11cmxkZWNV
ZGUoIiUiLnNlYnN0cigkYyWkaSwyKSk7ZWNoYhAZndyaXRlKGZvcGVuKCRmL3J3IksJGj1Zik%2FIjEioIiwIk702Vjag8oInw8LSIp02RpzSgpOw%3D%3D
&z1=RDpccdfTcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE000104A46494600010101007800780000FFDB004300010101010101010101
0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
FFC0001108013901E203012200021101031101FFC4001F00000105010101010100000000000000000102030405060708090A0BFFC400B51000020103
0302040305040400000017D010203000041105122131410613516107227114328191A1082342B1C11552D1F02433627282090A161718191A2526272829
2A3435363738393AA34445464748494AA535455565758595AA636465666768696A737475767778797A838485868788898AA92939495969798999AA2A3A4A5
A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F0100030101
01010101010100000000000102030405060708090A0BFFC400B5110002010204040304070504040001027700010203110405213106124151076171
1322328108144291A1B1C109233352F0156272D10A162434E125F11718191A262728292A35363738393AA34445464748494AA535455565758595AA636465
666768696A737475767778797A82838485868788898AA92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4
D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012BCF5E3
0056C4310192E7D0CC40EFC30478E3B0DF00FD8F352DA3DBB0AF0769F2C1FF00964839699FC3866C9C11CF719E33AD6F1B7C840EB930AB71C672D732
7B0C1D99EC0632179FF49A8C75F376FF002FB9DFAD9BE65D66EDFE56D79EFADBB3D9AB5BE4AC95FB69D5455EDC28724C9C703CD238D89FC30A1F523AE3
D4F6539D88632E4EE013080CA57FE58C5FC31A7FD34933F377E7DCD54B78F714DA0B00711038F9DC7DF9DFFD95E703FA6EAD98101D8A83702FF20FF9ED
3779187FCF34391CF5F539AF568C36EFD7BAD36F5BBDBBE9F146DE3D79F4DDAFBAFA2F93D1EFA2B35B4657B90A6428036314F7C5BC1F967CC7DDCF739
1D0B1C6CDBA6D0BB70AA4292B9FF963177918FF00CF47E3033B88C6324A8AAB020551D24F9B1EF7336781D4131A13C738C7BB606BDB0464B82FF0030DF
8EB34BD5635C7F021C671DBA0C9435EA528EDE56FF0087D3F357B745A42FE4566B5F3EFADB656B3F5B5B4ECDABD465BB78FCF85540620B421B811A1FBD
7327FB47036E4F5E47DD4AD7B78F732141F2AFFA856EE73FBCB993B0C6D2573C63D81354E14C96DDF32EE5F39971FBC906365845D72A300311C71E8A2B
6A353921B19E3CE65FE151F72DA3C74E061B6F4C73F74E7D6A11DB4ED7B697DBEE4ADD3E1B69750478D5A5ABD6FA7E76F4BEEB6FAD9CED1B70A9F9047
F30DC7C956E3CD9070F3B8FEEA9FB8BD30790D5A70C61400079997C2E7ADCCFD089C9E638B2703EEFA9059B15E24DBB830D8B479C47FCB284E36C080
E7E77380D9FA1CE18D694319272C46760DD48B780F0101EF2CB9C63A9CF62C71D96D52D36DBB256F5B7CF6B59E91A89F0DDEBAE8DAEAEF6D6775BEFB
ADFE74BDFA76B3146A796CBA87191D4DCDC765F689339FA3D7A30AD2452C4863B81606661EF2DA5FE18131D634E99E871CFE05578D1890061095C8FE9E
```

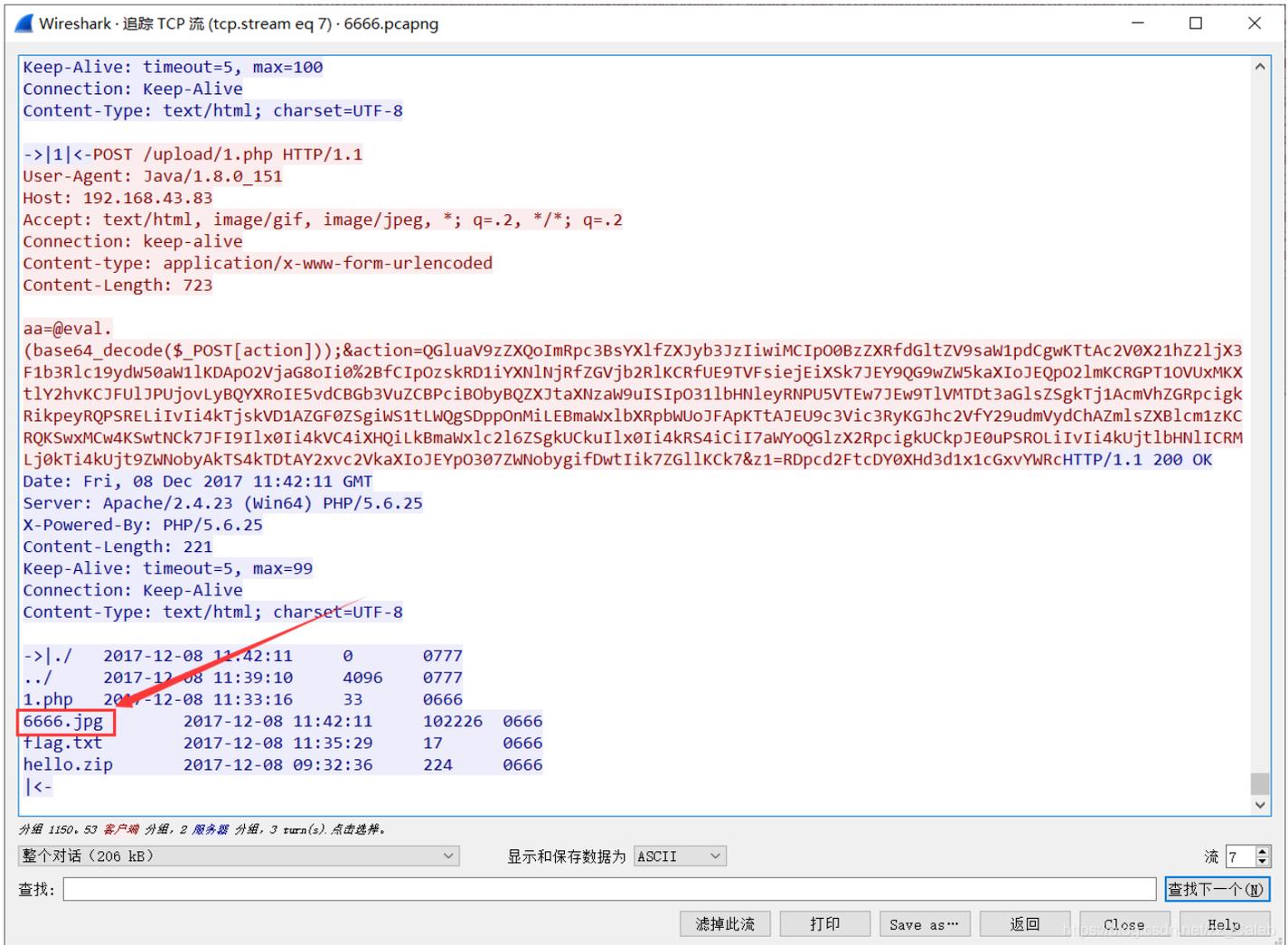
19 客户端 分组, 0 服务器 分组, 0 元组(s).

整个对话 (206 kB) 显示和保存数据为 ASCII 流 7

查找: 查找下一个 (N)

滤掉此流 打印 Save as... 返回 Close Help

看着很像一个文件的16进制码，翻到最下面看到：



再回过头来看看16进制码的头和尾，发现就是一个图片，把这个图片搞出来：



解压拿到flag:

flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)