

MISC-1

原创

Re1y0n



于 2021-07-31 12:04:09 发布



29



收藏

分类专栏: [CTF](#) 文章标签: [其他](#)

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/qdlws/article/details/119272457>

版权



[CTF 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

题目目录

reverseMe

this_is_flag.

pdf:

神奇的Modbus:

2017_Dating_in_Singapore:

simple_transfer:

就在其中:

MISCall:

如来十三掌:

give_you_flag:

reverseMe

文件的内容

{eð07eA07eS470sðcb17ed7c8078A777A} gslf

右键->编辑->旋转->水平翻转



[this_is_flag:](#)

A screenshot of a CTF challenge page for 'this_is_flag'. The page has a dark background. At the top, it shows the challenge name 'this_is_flag' with a thumbs-up icon and '129' likes, and a badge that says '最佳Writeup由王兆敏提供'. Below this, the '难度系数' (Difficulty Coefficient) is shown as '★★ 2.0'. The '题目来源' (Source) is '暂无' (None). The '题目描述' (Description) is 'Most flags are in the form flag{xxx}, for example:flag{th1s !_s_a_d4m0_4la9}'. The '题目场景' (Scenario) and '题目附件' (Attachments) are both '暂无' (None). The URL 'https://blog.csdn.net/qdlws' is in the bottom right corner.

试了两次:

flag{this_is_flag}和flag{th1s !_s_a_d4m0_4la9}

[pdf:](#)

pdf

👍 98

最佳Writeup由S_O_L_R提供

难度系数:  3.0

题目来源: [csaw](#)

题目描述: 菜猫给了菜狗一张图, 说图下面什么都没有

题目场景: 暂无

题目附件: [附件1](#)

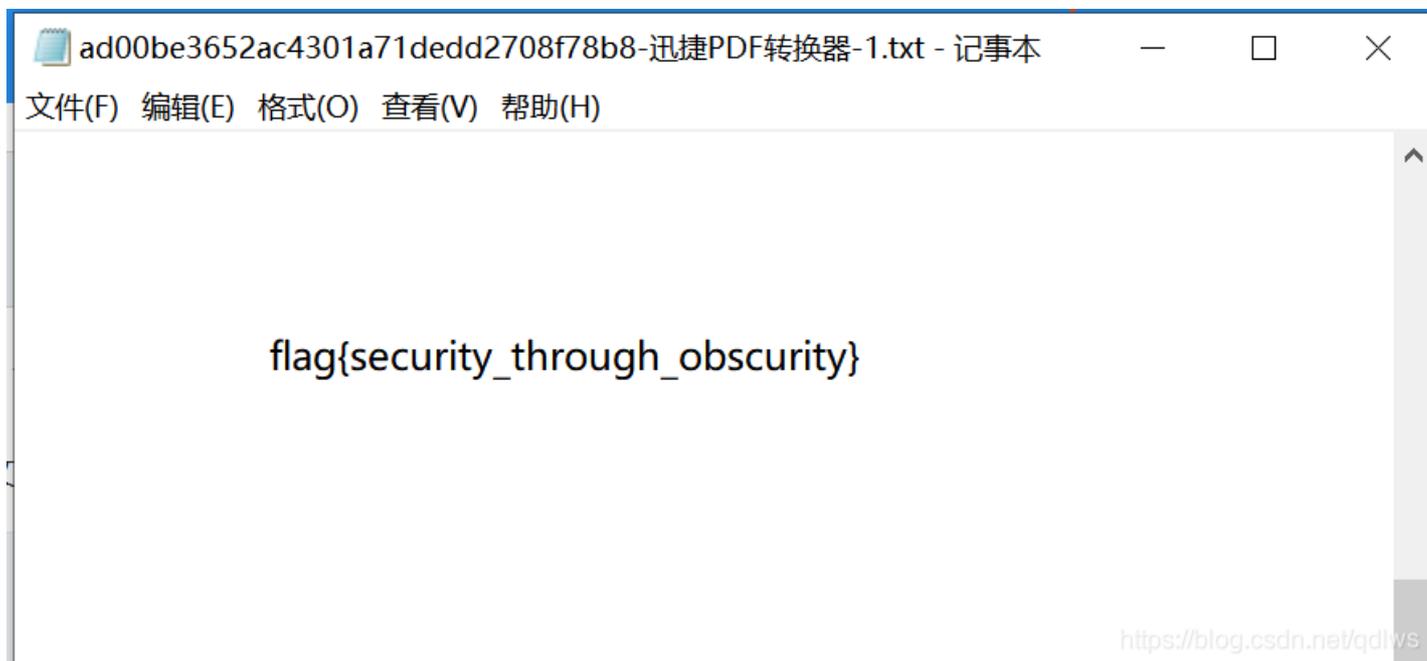
<https://blog.csdn.net/qdlws>



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

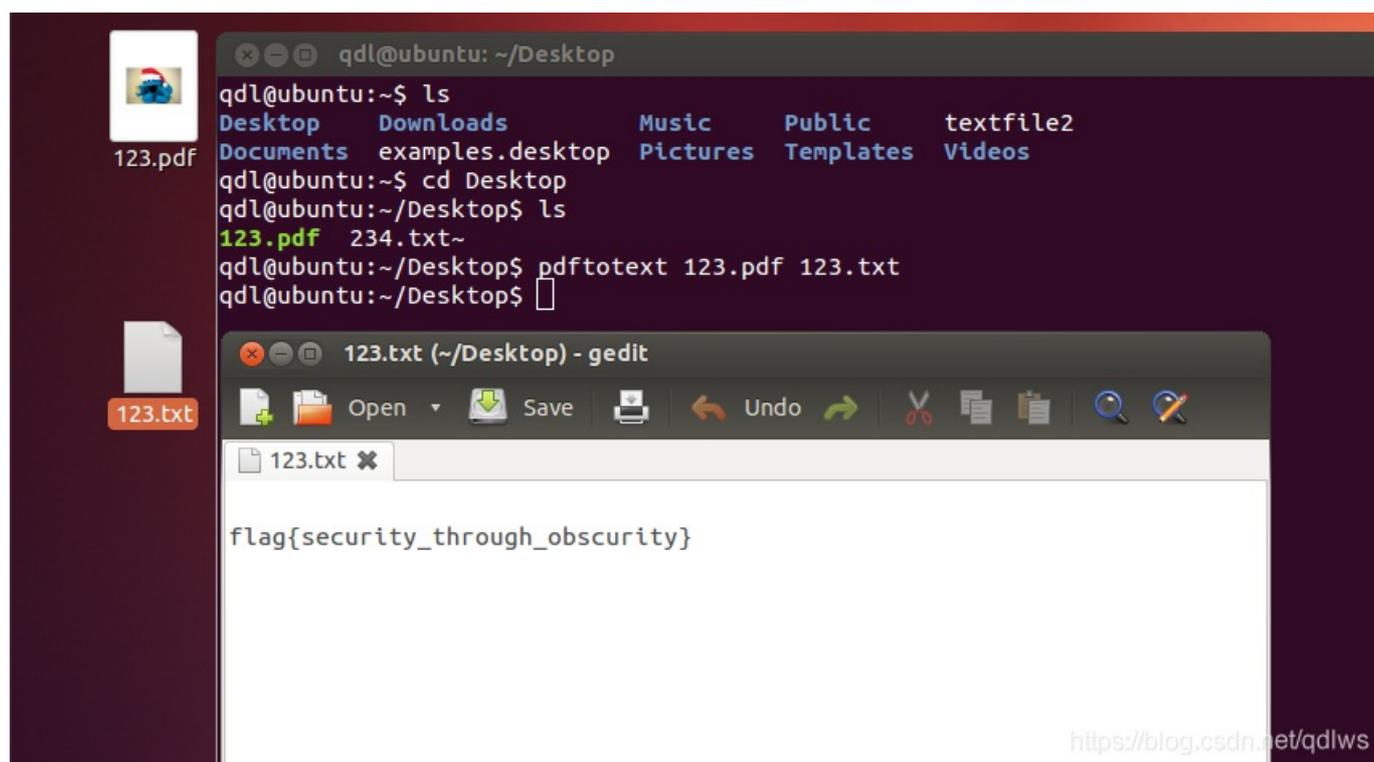
题目提示flag就在图片下面

利用[在线转换器](#)转换成txt得到flag, 本来想转换成word查看, 但是转换成word一直打不开



看了大佬写的博客，还可以利用Linux自带工具pdftotext解题，于是乎尝试一番

```
pdftotext 123.pdf 123.txt
```



神奇的Modbus:

神奇的Modbus

👍 25 最佳Writeup由Oxfafu-1 • giun提供

难度系数: ★ 1.0

题目来源: XCTF 4th-SCTF-2018

题目描述: 寻找flag,提交格式为sctf{xxx}

题目场景: 暂无

题目附件: 附件1

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

附件1是一个pcapng文件，使用wireshark打开

百度了一下，modbus是一个通讯协议，在wireshark中点击protocol进行分类，右键modbus通信协议的任意一条记录->追踪流->TCP流即得到字符串Easy_Mdbus



提交发现并不正确，少了一个字母o，flag应为为sctf{Easy_Modbus}

2017_Dating_in_Singapore:

2017_Dating_in_Singapore

👍 6 最佳Writeup由admin提供

WP 建议

难度系数: ★ 1.0

题目来源: XCTF 3rd-HITB CTF-2017

题目描述: 01081522291516170310172431-050607132027262728-0102030209162330-02091623020310090910172423-02010814222930-0605041118252627-0203040310172431-0102030108152229151617-04050604111825181920-0108152229303124171003-261912052028211407-04051213192625

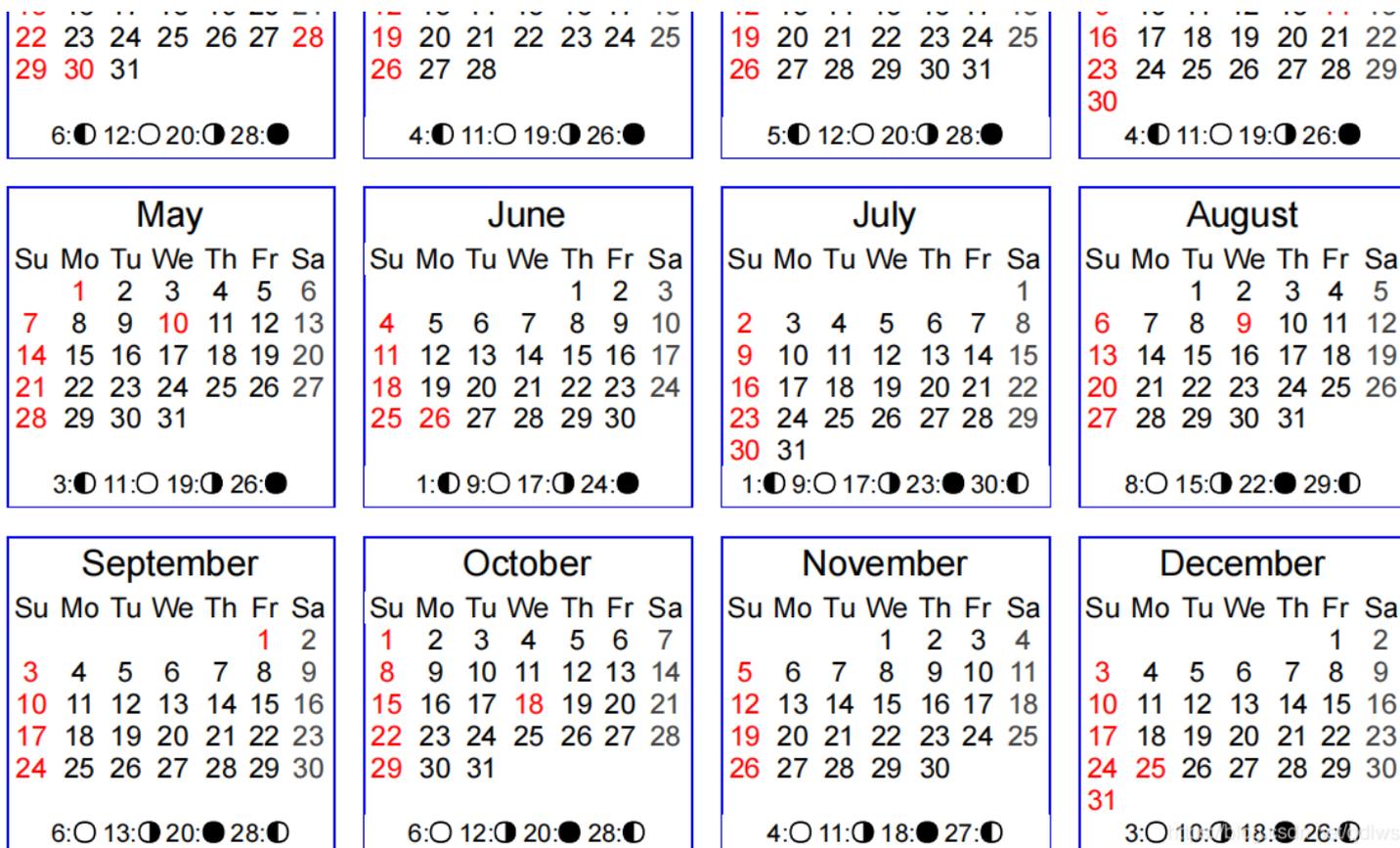
题目场景: 暂无

题目附件: 附件1

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

附件1:

January							February							March							April						
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7				1	2	3	4				1	2	3	4							1
8	9	10	11	12	13	14	5	6	7	8	9	10	11	5	6	7	8	9	10	11	2	3	4	5	6	7	8
15	16	17	18	19	20	21	12	13	14	15	16	17	18	12	13	14	15	16	17	18	9	10	11	12	13	14	15



有用的信息只有题目中的那一串数字和附件1中的日历，将数字进行处理

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

01081522291516170310172431-
050607132027262728-
0102030209162330-
02091623020310090910172423-
02010814222930-
0605041118252627-
0203040310172431-
0102030108152229151617-
04050604111825181920-
0108152229303124171003-
261912052028211407-
04051213192625

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

我一开始解读第一行的时候认为是从1月8号开始，但是后面就让我难以继续了，如果是一位数的月份前面也应该有个0，15月的话，想想就觉得自己有点憨，思考了一番无果，无聊数位数，第一行竟然是偶数，又数了两行，新即兹哇一兹摸你肚子，我悟了，数了一下行数，十二行，一行对应一个月啊，这下我彻底悟了，对数字进行两两分组

*新建文本文档.txt - 记事本

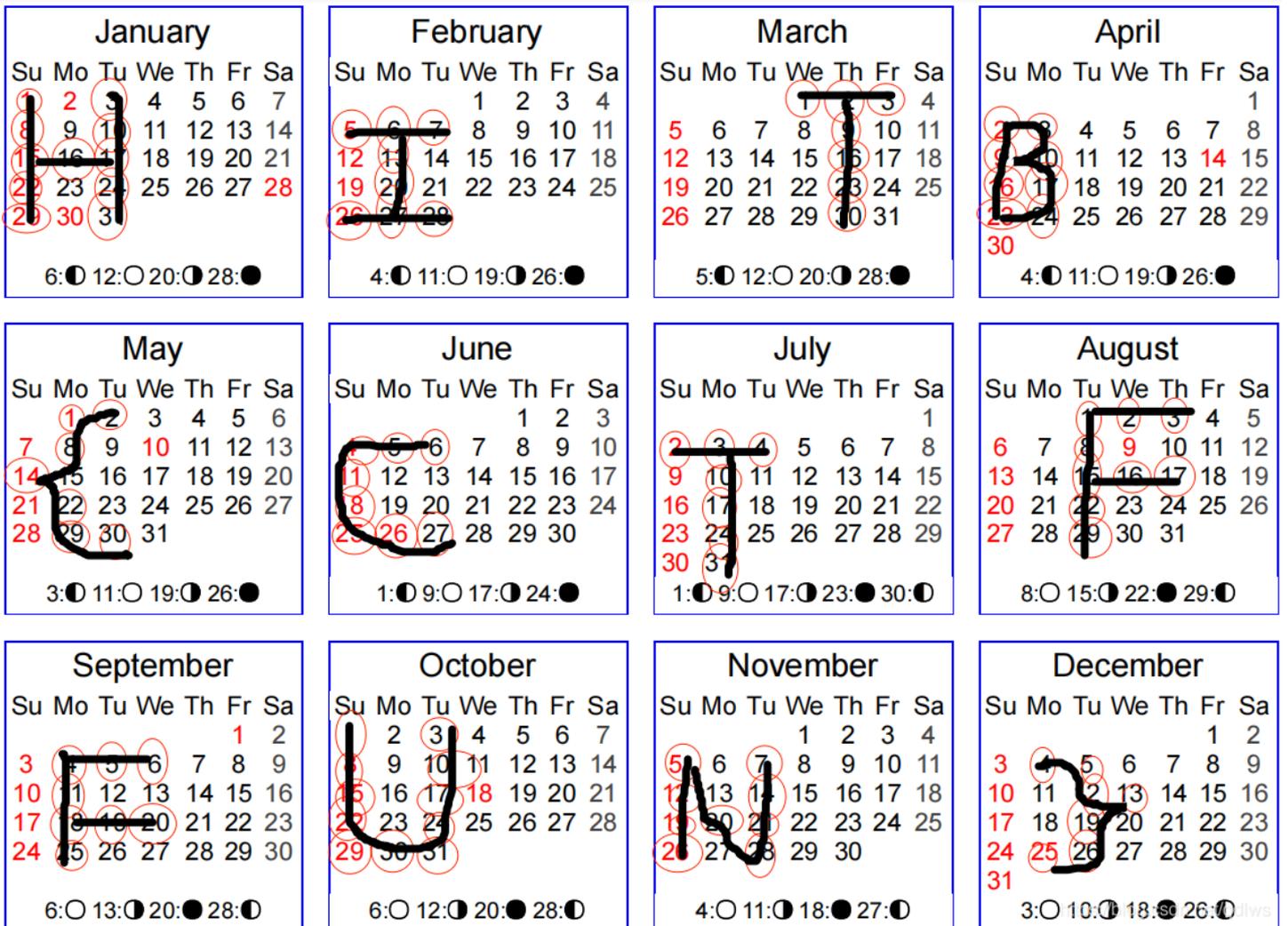
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

01 08 15 22 29 15 16 17 03 10 17 24 31- 26位
05 06 07 13 20 27 26 27 28- 18位
01 02 03 02 09 16 23 30- 16位

02 09 16 23 02 03 10 09 09 10 17 24 23- 26位
 02 01 08 14 22 29 30- 14位
 06 05 04 11 18 25 26 27- 16位
 02 03 04 03 10 17 24 31- 16位
 01 02 03 01 08 15 22 29 15 16 17- 22位
 04 05 06 04 11 18 25 18 19 20- 20位
 01 08 15 22 29 30 31 24 17 10 03- 22位
 26 19 12 05 20 28 21 14 07- 18位
 04 05 12 13 19 26 25 14位

<https://blog.csdn.net/qdlw5>

然后就在附件上不停的画圈圈，最后连起来得到flag



simple_transfer:

simple_transfer



最佳Writeup由B301 • dals提供

难度系数: ★ 1.0

题目来源: XCTF 3rd-HITB CTF-2017

题目描述: 文件里有flag, 找到它。

题目场景: 暂无

题目附件: 附件1

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

附件1是一个pcap文件, wireshark打开, 点击protocol, 从后往前一条一条地找, 找了很久才找到这个file.pdf

No.	Time	Source	Destination	Protocol	Length	Info
4308	62.583851	10.0.2.5	10.0.2.4	NFS	174	V4 Call (Reply In 4314) SETCLIENTID_CONFIRM
4307	62.583814	10.0.2.4	10.0.2.5	NFS	130	V4 Reply (Call In 4306) SETCLIENTID
4306	62.583621	10.0.2.5	10.0.2.4	NFS	242	V4 Call (Reply In 4307) SETCLIENTID
4304	62.583488	10.0.2.4	10.0.2.5	NFS	122	V4 Reply (Call In 4303) LOOKUP Status: NFS4ERR_NOENT
4303	62.583091	10.0.2.5	10.0.2.4	NFS	230	V4 Call (Reply In 4304) LOOKUP DH: 0x0163bd75/file.pdf
4301	61.845888	10.0.2.4	10.0.2.5	NFS	266	V4 Reply (Call In 4300) GETATTR
4300	61.845705	10.0.2.5	10.0.2.4	NFS	210	V4 Call (Reply In 4301) GETATTR FH: 0x0163bd75
4298	61.844943	10.0.2.4	10.0.2.5	NFS	266	V4 Reply (Call In 4297) GETATTR

▼ Opcode: PUTFH (22)
 ▼ FileHandle
 length: 28
 [hash (CRC-32): 0x0163bd75]
 FileHandle: 01000700bb23060000000005c7536b9c59642ef9c9651d4...

```
0000 08 00 27 1f c2 a8 08 00 27 f3 75 4b 08 00 45 00  ..'.....'uK..E..
0010 00 d8 09 72 40 00 40 06 18 a6 0a 00 02 05 0a 00  ...r@.@.....
0020 02 04 03 56 08 01 bb 86 59 19 29 a2 bc 04 80 18  ...V....Y.)....
0030 01 49 18 d3 00 00 01 01 08 0a 00 02 4d 2f 00 02  ..I.....M/..
0040 49 cb 80 00 00 a0 7f c0 e6 45 00 00 00 00 00 00  I.....E.....
0050 00 02 00 01 86 a3 00 00 00 04 00 00 00 01 00 00  .....$. '8....ct
0060 00 01 00 00 00 24 01 06 27 38 00 00 00 0a 63 74  ...f-client.....
0070 66 2d 63 6c 69 65 6e 74 00 00 00 00 00 00 00 00  .....
0080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00  .....
00a0 00 16 00 00 00 1c 01 00 07 00 bb 23 06 00 00 00  ...#....
00b0 00 00 5c 75 36 b9 c5 96 42 ef 9c 96 51 d4 3c 03  ..\u6...B...Q.<
00c0 75 59 00 00 00 0f 00 00 00 08 66 69 6c 65 2e 70  uY.....file.p
00d0 64 66 00 00 00 0a 00 00 00 09 00 00 00 02 00 10  df.....
00e0 01 1a 00 b0 a2 3a .....
```

将文件更名拖进kali linux, foremost指令分离文件

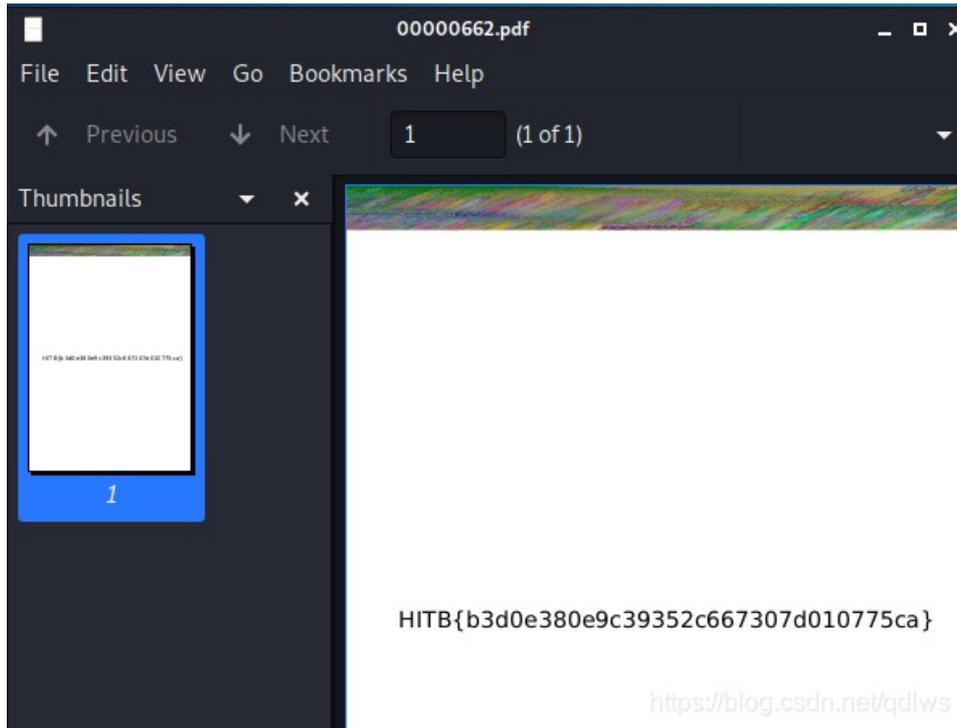
```
foremost -T 文件名
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
└─$ ls
Desktop  Downloads  output_Mon_Aug_16_01_12_27_2021  Pictures  Templates
Documents  Music      output_Mon_Aug_16_01_19_28_2021  Public    Videos

(kali@kali)-[~]
└─$ cd Desktop

(kali@kali)-[~/Desktop]
└─$ foremost -T a.pcap
Processing: a.pcap
[*]
```

然后桌面上就会多出一个文件，进入文件打开pdf得到flag



看了一下大佬的博客，大佬使用wireshark的统计->协议分级查看，通过协议的字节百分比占用基本全在nfs协议上来过滤nfs，然后观察报文发现file.pdf，我发现还可以点protocol将协议分类然后每一种协议都右键->追踪流查看

就在其中：

就在其中

👍 5 最佳Writeup由admin提供

难度系数: ★★ 2.0

题目来源: ISCC-2017

题目描述: 格式为flag{xxxx}

题目场景: 暂无

题目附件: 附件1

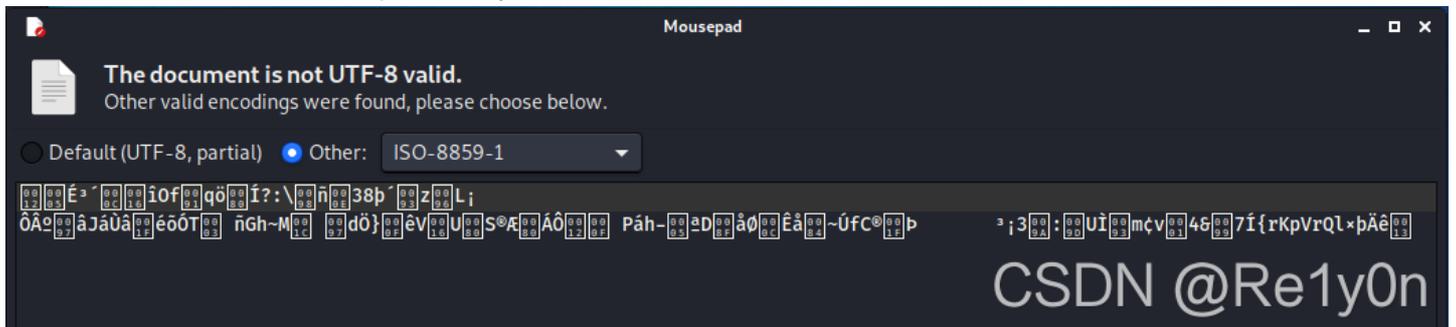
CSDN @Re1y0n

附件1解压wireshark打开，搜索关键词，当关键词为key时

```

Line-based text data (7 lines)
03-12-16 12:20PM 142588562 IDA Pro 6.5 Setup.exe\r\n
08-09-16 11:15AM 128 key.txt\r\n
08-10-16 11:29AM 240 key.zip\r\n
08-09-16 11:12AM 272 pub.key\r\n
08-09-16 11:11AM 891 test.key\r\n
04-15-16 10:38PM 7357556 000000.pdf\r\n
04-15-16 10:38PM 9871783 000000.pdf\r\n
  
```

foremost命令分离文件，在文件zip中发现key.txt文件，但是打开却是乱码



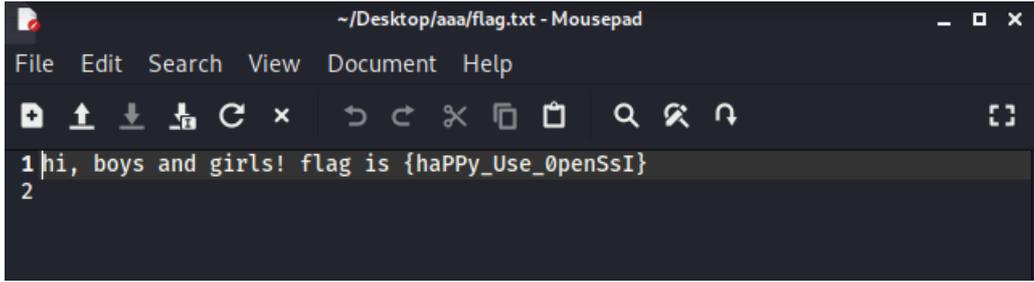
猜想可能需要密钥才能打开，搜索PRIVATE，followTCP流就可以看到密钥



新建rsa.txt文件，将密钥粘贴到rsa.txt中，要和key.txt放在一个目录下，openssl解密，得到flag.txt

```
openssl rsautl -decrypt -in key.txt -inkey rsa.txt -out flag.txt
-in 需要解密的文件 -inkey 密钥 -out 输出的文件
```

打开得到flag



MISCall:

MISCall 👍 24 最佳Writeup由我们是来学习的 · Cony提供

难度系数: ★★ 2.0

题目来源: noconname-2014-quals

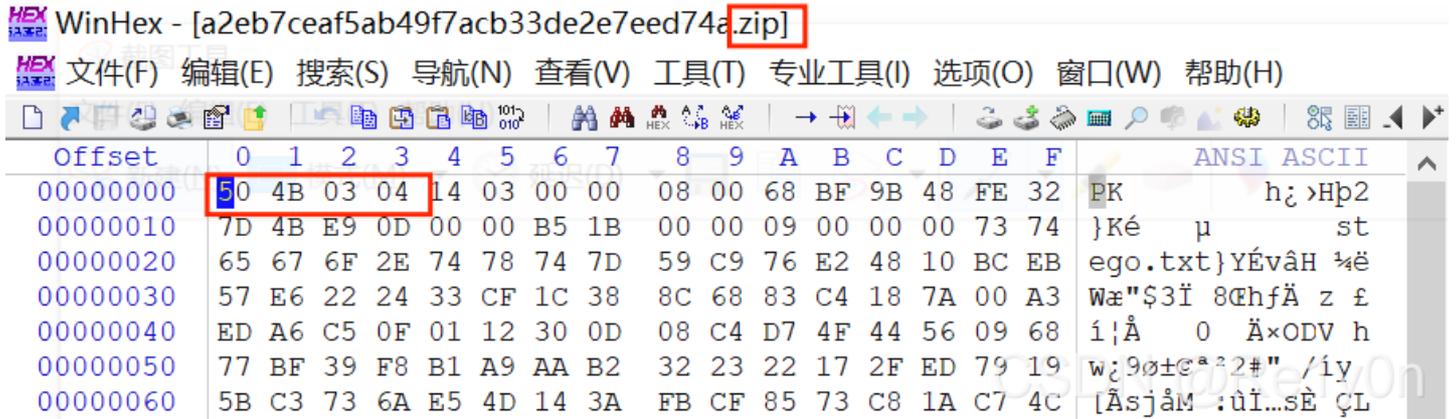
题目描述: 没有提示

题目场景: 暂无

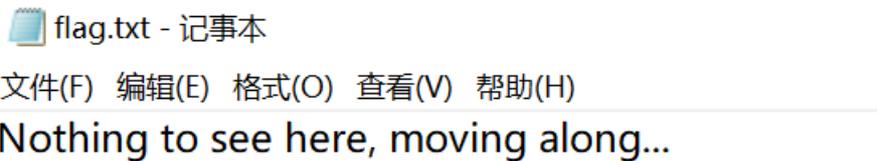
题目附件: 附件1

CSDN @Re1y0n

附件1是一个无后缀文件，winhex打开，发现时zip文件



解压得到flag.txt和.git文件



意料之外，这个git又有个问题该怎么处理，百度了一下，这问题而安用Linux信守不群，群越参考

以下解题过程是按照解题参考的实操

修改后缀然后解压

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
└─$ tar xvf a.bzip2
ctf/
ctf/flag.txt
ctf/.git/
ctf/.git/description
ctf/.git/refs/
ctf/.git/refs/heads/
ctf/.git/refs/heads/master
ctf/.git/refs/stash
ctf/.git/refs/tags/
ctf/.git/ORIG_HEAD
ctf/.git/logs/
ctf/.git/logs/refs/
ctf/.git/logs/refs/heads/
ctf/.git/logs/refs/heads/master
ctf/.git/logs/refs/stash
ctf/.git/logs/HEAD
ctf/.git/HEAD
ctf/.git/COMMIT_EDITMSG
ctf/.git/hooks/
```

查看git记录

```
(kali@kali)-[~/Desktop]
└─$ cd ctf
(kali@kali)-[~/Desktop/ctf]
└─$ git log
commit bea99b953bef6cc2f98ab59b10822bc42afe5abc (HEAD -> master)
Author: Linus Torvalds <torvalds@klaava.Helsinki.Fi>
Date: Thu Jul 24 21:16:59 2014 +0200

Initial commit
```

查看修改列表，储存列表中有一条记录

```
(kali@kali)-[~/Desktop/ctf]
└─$ git stash list
stash@{0}: WIP on master: bea99b9 Initial commit
```

校验列表中的存储文件

```
(kali@kali)-[~/Desktop/ctf]
└─$ git stash show
flag.txt | 25 ++++++
s.py | 4 +++
2 files changed, 28 insertions(+), 1 deletion(-)
```

把列表中的文件恢复

直接执行 git stash apply 时，会提示文件覆盖自动终止，可以先把flag.txt删除再执行

```
kali@kali: ~/Desktop/ctf
File Actions Edit View Help
(kali@kali)-[~/Desktop/ctf]
└─$ rm flag.txt
```

```
(kali@kali) [~/Desktop/ctf]
└─$ ls

(kali@kali) [~/Desktop/ctf]
└─$ git stash apply
On branch master
Changes to be committed:
  (use "git restore --staged <file> ..." to unstage)
        new file:   s.py

Changes not staged for commit:
  (use "git add <file> ..." to update what will be committed)
  (use "git restore <file> ..." to discard changes in working directory)
        modified:   flag.txt

(kali@kali) [~/Desktop/ctf]
└─$
```

运行s.py得到flag

```
(kali@kali) [~/Desktop/ctf]
└─$ ./s.py
NCN4dd992213ae6b76f27d7340f0dde1222888df4d3

(kali@kali) [~/Desktop/ctf]
└─$
```

如来十三掌：

菜狗为了打败菜猫，学了一套如来十三掌

如来十三掌

👍 148 最佳Writeup由flag{not_here} • 渣渣禹提供

难度系数：★★★★ 3.0

题目来源：暂无

题目描述：菜狗为了打败菜猫，学了一套如来十三掌。

题目场景：暂无

题目附件：[附件1](#)

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

附件1:

「夜哆悉諳多苦奢陀奢諦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苦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吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧幡亦醞吶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」

如果不是看了别人的writeup，怎么能想到“与佛论禅”这个玩意儿

与佛论禅

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

心不动，万物皆不动

佛曰：夜哆悉諳多苦奢陀奢諦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

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

然后进行rot13解码

rot13

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

Rot13 编码 Rot13 解码 拷贝 剪切 粘贴 清除

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

最后base64解码得到flag

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果: 编/解码后自动全选

flag{bdscjhbkmfrdhbvckijndskvbkjdsab}

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

离谱，想不到真就一点都做不出来

give_you_flag:

give_you_flag  99 最佳Writeup由testtestzrs提供

难度系数:  4.0

题目来源: 暂无

题目描述: 菜狗找到了文件中的彩蛋很开心, 给菜猫发了个表情包

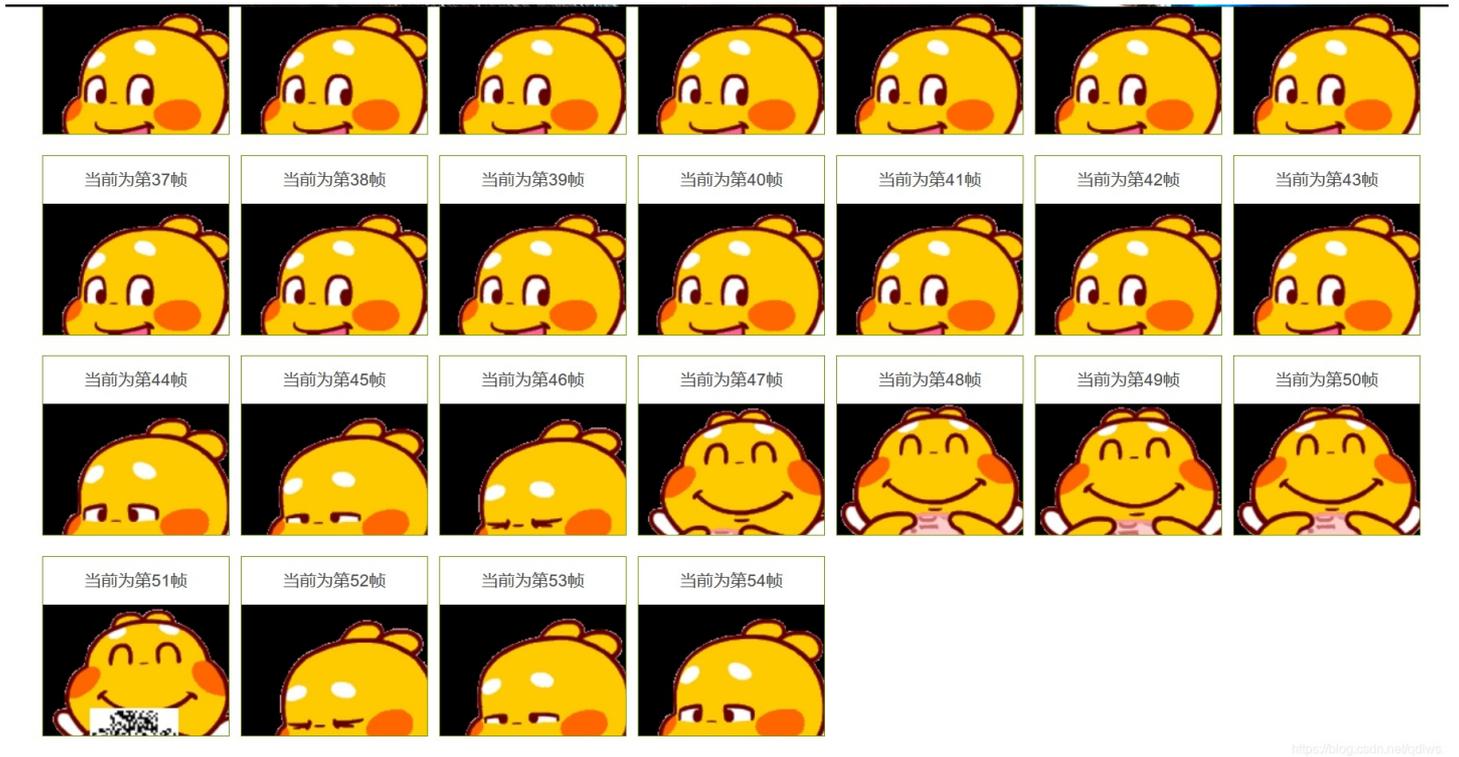
题目场景: 暂无

题目附件: [附件1](#)

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

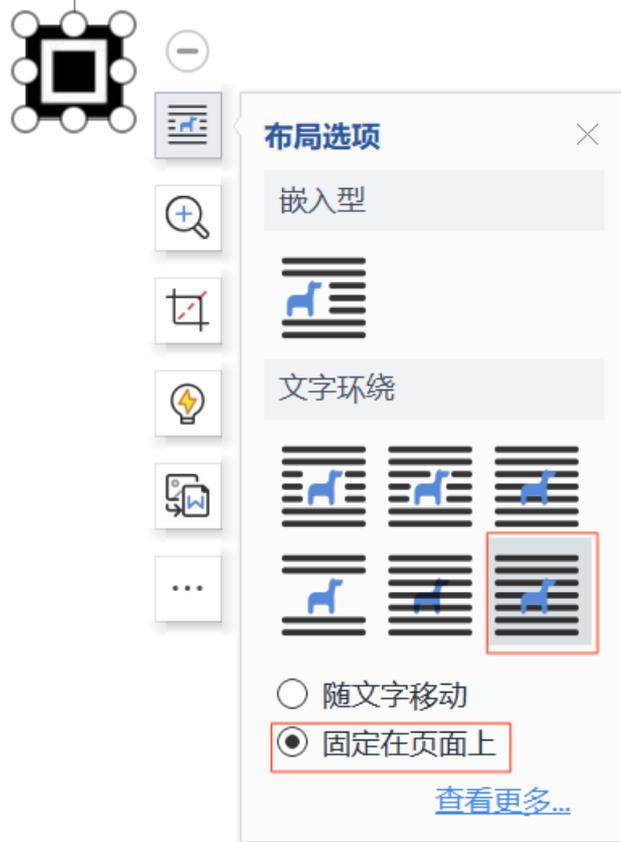
附件是一个动图, 动图的播放过程中出现了一个二维码, 但是因为太快扫不上, 然后我就录频录下来, 使用0.25倍速观看, 然后发现这个二维码少了二维码定位符号, 使用在线工具 <https://www.qtool.net/gif> 分解GIF动画

将第51帧保存下来



将保存的图片用word打开调整到合适大小, 建议调小一点, 图片放大会比较模糊, 将三个二维码定位符号放于三个角不断的调整位置直到能够扫上为止







用微信扫一扫得到flag



flag{e7d478cf6b915f50ab1277f78502a2c5}

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