GameShell3

信息收集

主机发现

端口扫描

80端口

GetShell

权限提升

信息收集

主机发现

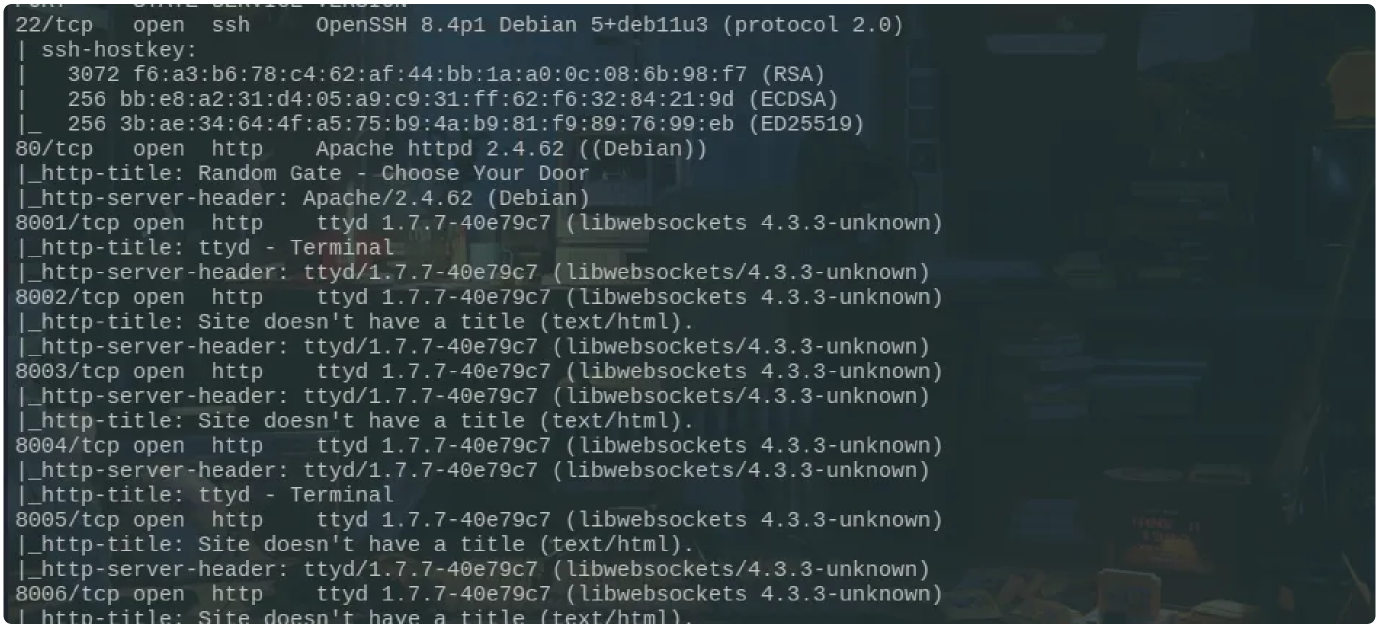
Plain Text

```
arp-scan -l
主机IP ： 192.168.21.55
```

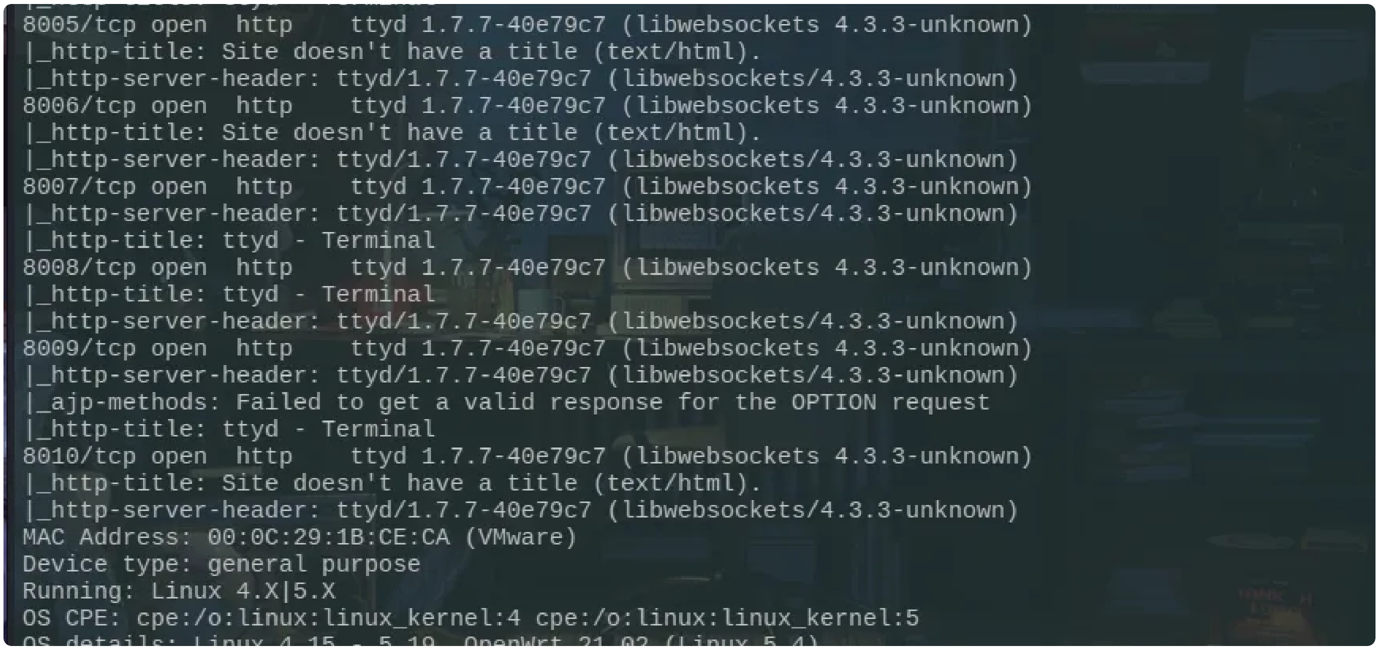
端口扫描

Plain Text

```
nmap -sS -A -T5 -p- 192.168.21.55
```



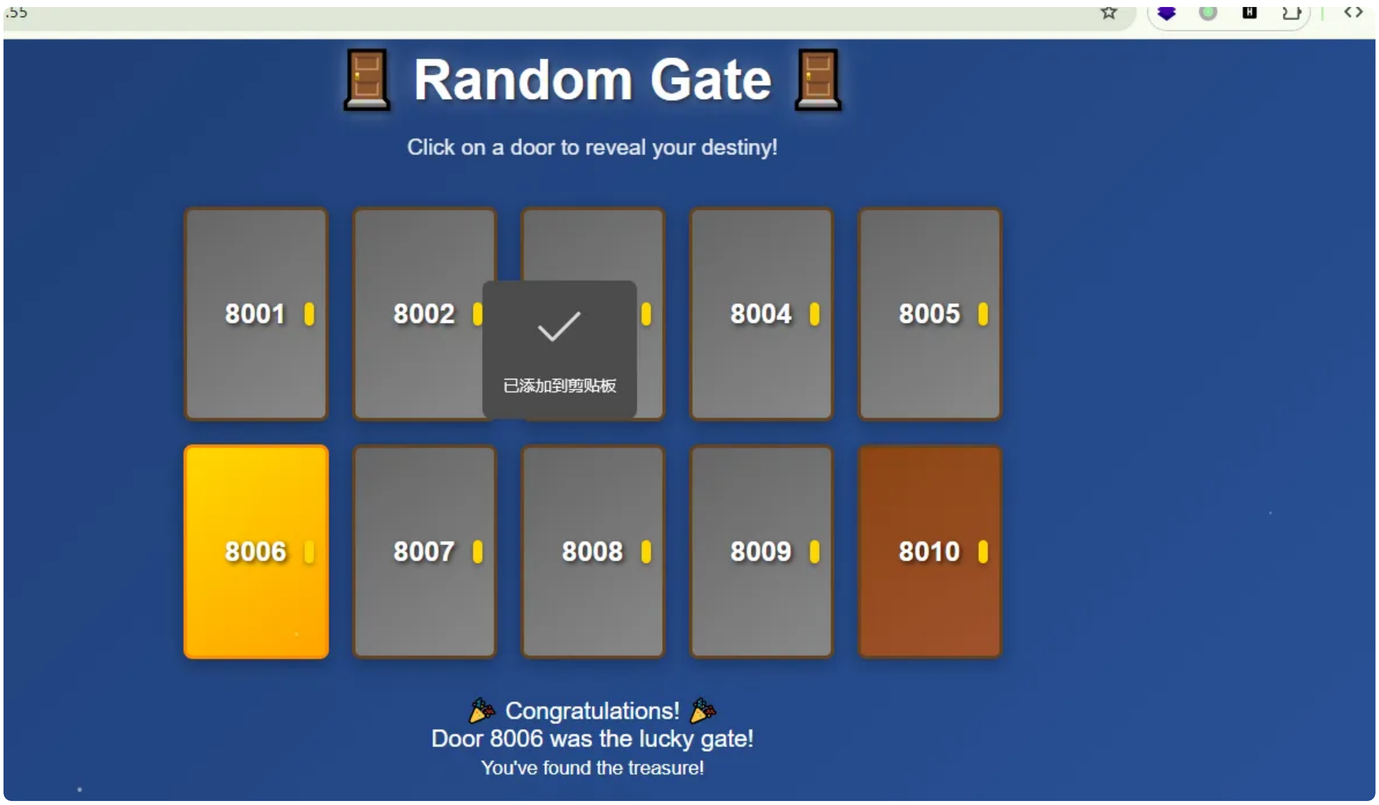
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Random Gate - Choose Your Door
|_http-server-header: Apache/2.4.62 (Debian)
8001/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: ttyd - Terminal
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8002/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8003/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
8004/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: ttyd - Terminal
8005/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8006/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
```



```
|_http-title: ttyd - Terminal
8005/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8006/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8007/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: ttyd - Terminal
8008/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: ttyd - Terminal
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8009/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_ajp-methods: Failed to get a valid response for the OPTION request
|_http-title: ttyd - Terminal
8010/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
MAC Address: 00:0C:29:1B:CE:CA (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
```

端口开放了好多

`80`端口

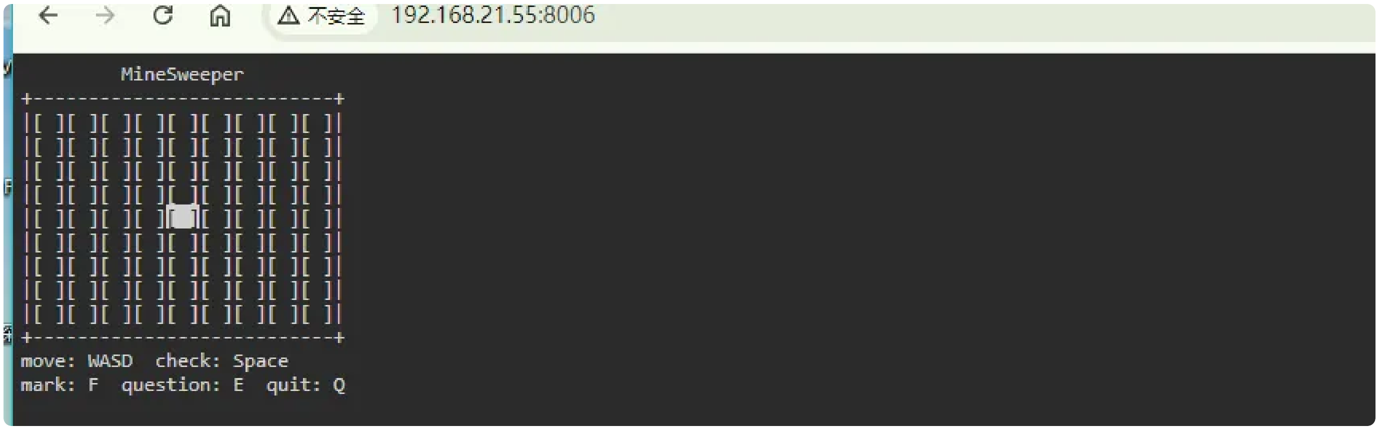


Random Gate

Click on a door to reveal your destiny!

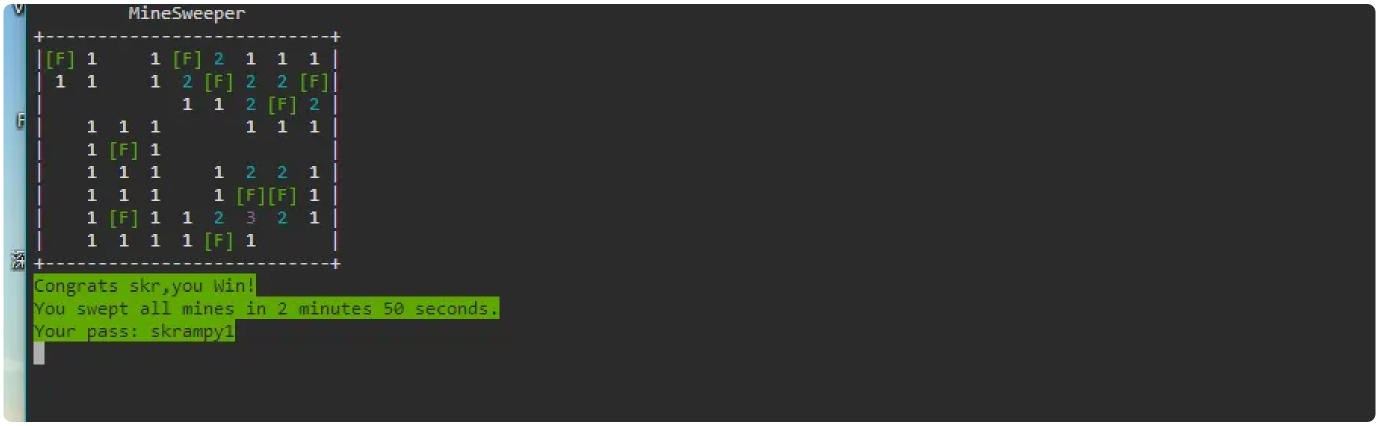
Congratulations!
Door 8006 was the lucky gate!
You've found the treasure!

提示 `8006`



```
        MineSweeper
+---------------------------+
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
|[ ][ ][ ][ ][ ][ ][ ][ ][ ]|
+---------------------------+
move: WASD  check: Space
mark: F  question: E  quit: Q
```

是一个扫雷游戏，玩一下

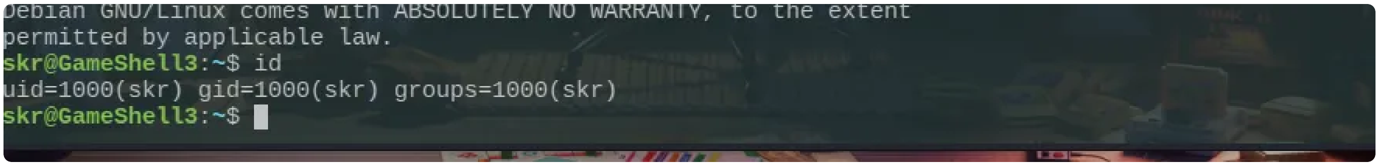


```
        MineSweeper
+---------------------------+
|[F] 1     1 [F] 2  1  1  1 |
| 1  1     1  2 [F] 2  2 [F]|
|             1  1  2 [F] 2 |
|    1  1  1        1  1  1 |
|    1 [F] 1                |
|    1  1  1     1  2  2  1 |
|    1  1  1     1 [F][F] 1 |
|    1 [F] 1  1  2  3  2  1 |
|    1  1  1  1 [F] 1       |
+---------------------------+
Congrats skr,you Win!
You swept all mines in 2 minutes 50 seconds.
Your pass: skrampy1
```

发现账号密码 `skr:skrampy1`

GetShell

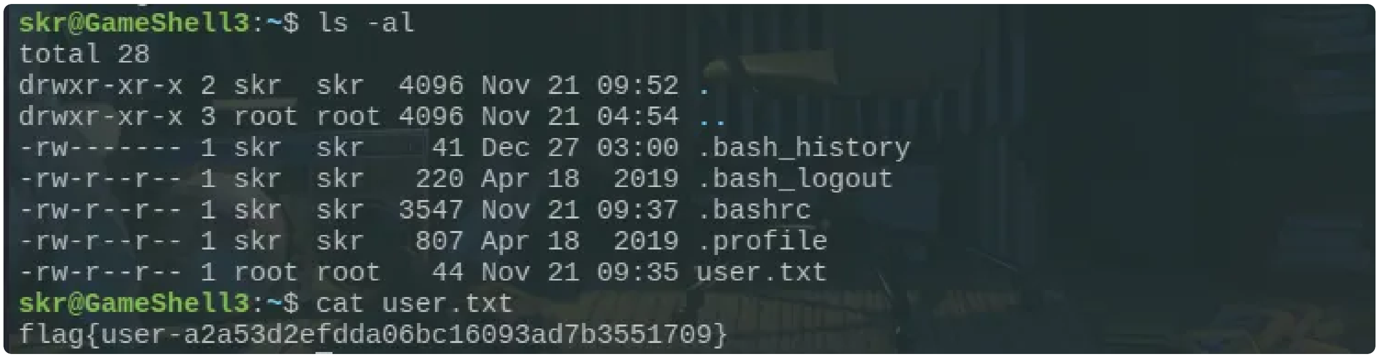
```
ssh skr@192.168.21.55
skrampy1
```



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
skr@GameShell3:~$ id
uid=1000(skr) gid=1000(skr) groups=1000(skr)
skr@GameShell3:~$
```

成功登录

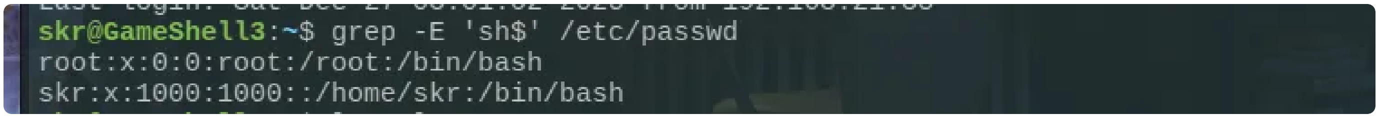
权限提升



```
skr@GameShell3:~$ ls -al
total 28
drwxr-xr-x 2 skr  skr  4096 Nov 21 09:52 .
drwxr-xr-x 3 root root 4096 Nov 21 04:54 ..
-rw------- 1 skr  skr    41 Dec 27 03:00 .bash_history
-rw-r--r-- 1 skr  skr   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 skr  skr  3547 Nov 21 09:37 .bashrc
-rw-r--r-- 1 skr  skr   807 Apr 18  2019 .profile
-rw-r--r-- 1 root root   44 Nov 21 09:35 user.txt
skr@GameShell3:~$ cat user.txt
flag{user-a2a53d2efdda06bc16093ad7b3551709}
```

查看可登录用户

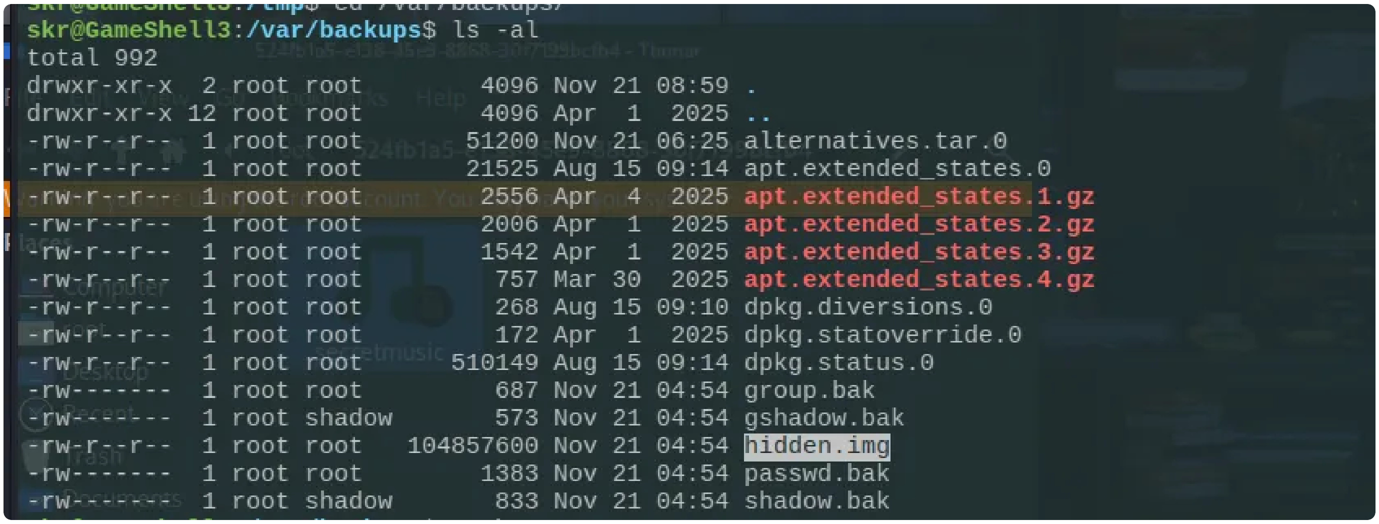
```
grep -E 'sh$' /etc/passwd
```



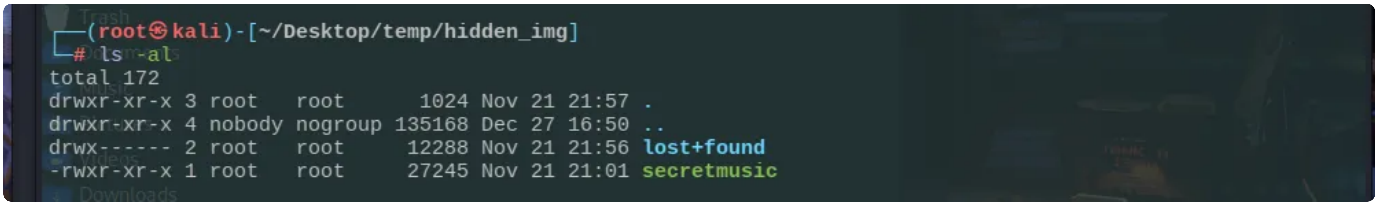
```
skr@GameShell3:~$ grep -E 'sh$' /etc/passwd
root:x:0:0:root:/root:/bin/bash
skr:x:1000:1000::/home/skr:/bin/bash
```

但是会自动退出，删除 `.bashrc` 文件最后两行，并执行 `source ~/.bashrc` 即可

在 `/var/backups` 发现一个 `hidden.img` 文件，弄到本地挂载之后发现一个 `secretmusic` 音频文件

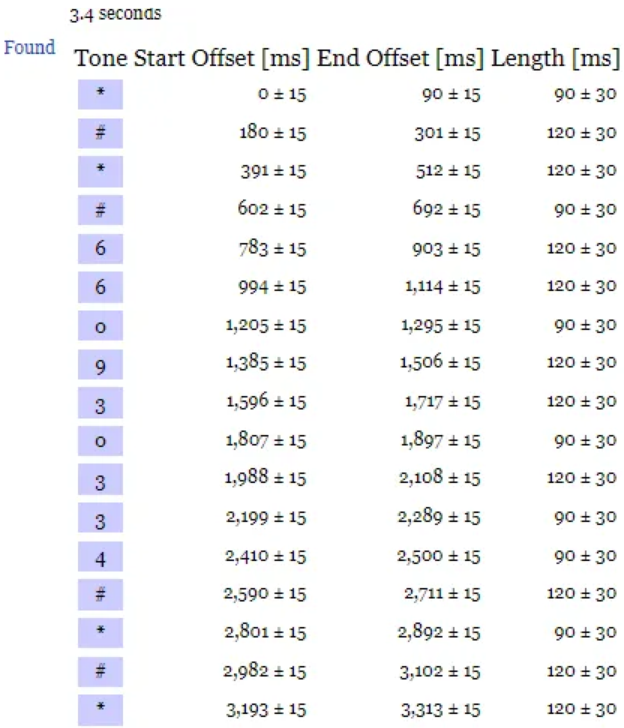


```
skr@GameShell3:/var/backups$ ls -al
total 992
drwxr-xr-x  2 root root      4096 Nov 21 08:59 .
drwxr-xr-x 12 root root      4096 Apr  1  2025 ..
-rw-r--r--  1 root root     51200 Nov 21 06:25 alternatives.tar.0
-rw-r--r--  1 root root     21525 Aug 15 09:14 apt.extended_states.0
-rw-r--r--  1 root root      2556 Apr  4  2025 apt.extended_states.1.gz
-rw-r--r--  1 root root      2006 Apr  1  2025 apt.extended_states.2.gz
-rw-r--r--  1 root root      1542 Apr  1  2025 apt.extended_states.3.gz
-rw-r--r--  1 root root       757 Mar 30  2025 apt.extended_states.4.gz
-rw-r--r--  1 root root       268 Aug 15 09:10 dpkg.diversions.0
-rw-r--r--  1 root root       172 Apr  1  2025 dpkg.statoverride.0
-rw-r--r--  1 root root    510149 Aug 15 09:14 dpkg.status.0
-rw-------  1 root root       687 Nov 21 04:54 group.bak
-rw-------  1 root shadow     573 Nov 21 04:54 gshadow.bak
-rw-r--r--  1 root root 104857600 Nov 21 04:54 hidden.img
-rw-------  1 root root      1383 Nov 21 04:54 passwd.bak
-rw-------  1 root shadow     833 Nov 21 04:54 shadow.bak
```



```
┌──(root㉿kali)-[~/Desktop/temp/hidden_img]
└─# ls -al
total 172
drwxr-xr-x 3 root   root      1024 Nov 21 21:57 .
drwxr-xr-x 4 nobody nogroup 135168 Dec 27 16:50 ..
drwx------ 2 root   root     12288 Nov 21 21:56 lost+found
-rwxr-xr-x 1 root   root     27245 Nov 21 21:01 secretmusic
```

放到网站 `http://dialabc.com/sound/detect/index.html`

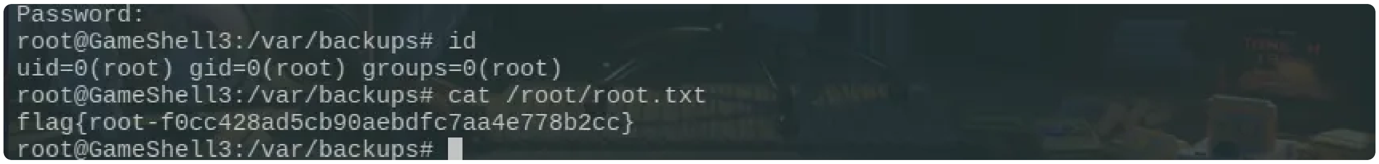


3.4 seconds

Found

Tone	Start Offset [ms]	End Offset [ms]	Length [ms]
*	0 ± 15	90 ± 15	90 ± 30
#	180 ± 15	301 ± 15	120 ± 30
*	391 ± 15	512 ± 15	120 ± 30
#	602 ± 15	692 ± 15	90 ± 30
6	783 ± 15	903 ± 15	120 ± 30
6	994 ± 15	1,114 ± 15	120 ± 30
0	1,205 ± 15	1,295 ± 15	90 ± 30
9	1,385 ± 15	1,506 ± 15	120 ± 30
3	1,596 ± 15	1,717 ± 15	120 ± 30
0	1,807 ± 15	1,897 ± 15	90 ± 30
3	1,988 ± 15	2,108 ± 15	120 ± 30
3	2,199 ± 15	2,289 ± 15	90 ± 30
4	2,410 ± 15	2,500 ± 15	90 ± 30
#	2,590 ± 15	2,711 ± 15	120 ± 30
*	2,801 ± 15	2,892 ± 15	90 ± 30
#	2,982 ± 15	3,102 ± 15	120 ± 30
*	3,193 ± 15	3,313 ± 15	120 ± 30

`*#*#660930334#*#*` 发现该数据为 `root` 密码



```
Password:
root@GameShell3:/var/backups# id
uid=0(root) gid=0(root) groups=0(root)
root@GameShell3:/var/backups# cat /root/root.txt
flag{root-f0cc428ad5cb90aebdfc7aa4e778b2cc}
root@GameShell3:/var/backups# 
```

提权成功