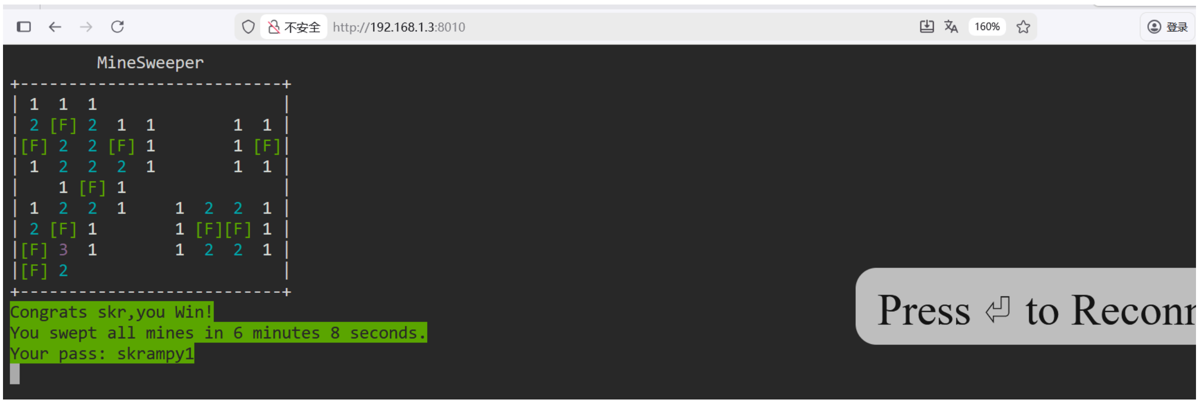
端口扫描

```
┌──(zsc㉿kali)-[~]
└─$ nmap -sT -p- -Pn -sV 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 14:05 CST
Nmap scan report for saga.local (192.168.1.3)
Host is up (0.00058s latency).
Not shown: 65523 closed tcp ports (conn-refused)
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))
8001/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8002/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8003/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8004/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8005/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8006/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8007/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8008/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8009/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
8010/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

访问80端口，是一个找随机门的小游戏，也没扫到其他目录。

8001-8010这几个端口都是扫雷小游戏，不过尝试了一下只有8010端口的小游戏可以交互（这个可交互的端口应该是随机的）

玩一玩扫雷小游戏，通关后得到一组凭证：skr:skkrampy1



```
         MineSweeper
+---------------------------+
| 1  1  1                   |
| 2 [F] 2  1  1        1  1 |
|[F] 2  2 [F] 1        1 [F]|
| 1  2  2  2  1        1  1 |
|    1 [F] 1                |
| 1  2  2  1     1  2  2  1 |
| 2 [F] 1        1 [F][F] 1 |
|[F] 3  1        1  2  2  1 |
|[F] 2                      |
+---------------------------+
Congrats skr,you Win!
You swept all mines in 6 minutes 8 seconds.
Your pass: skrampy1
```

登录shell，shell环境会自动断开连接，echo $TMOUT发现设置了5秒超时退出。

解决方法：临时禁用超时：unset TMOUT

```
┌──(zsc㉿kali)-[~]
└─$ ssh skr@192.168.1.3
skr@192.168.1.3's password:
Linux GameShell3 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: Fri Dec 26 23:47:33 2025 from 192.168.1.5
skr@GameShell3:~$ echo $TMOUT
5
skr@GameShell3:~$ unset TMOUT
skr@GameShell3:~$ cat /home/skr/user.txt
flag{user-a2a53d2efdda06bc16093ad7b3551709}
```

拿到user flag：flag{user-a2a53d2efdda06bc16093ad7b3551709}

提权

运行linpeas脚本，发现一个磁盘映像文件hidden.img，

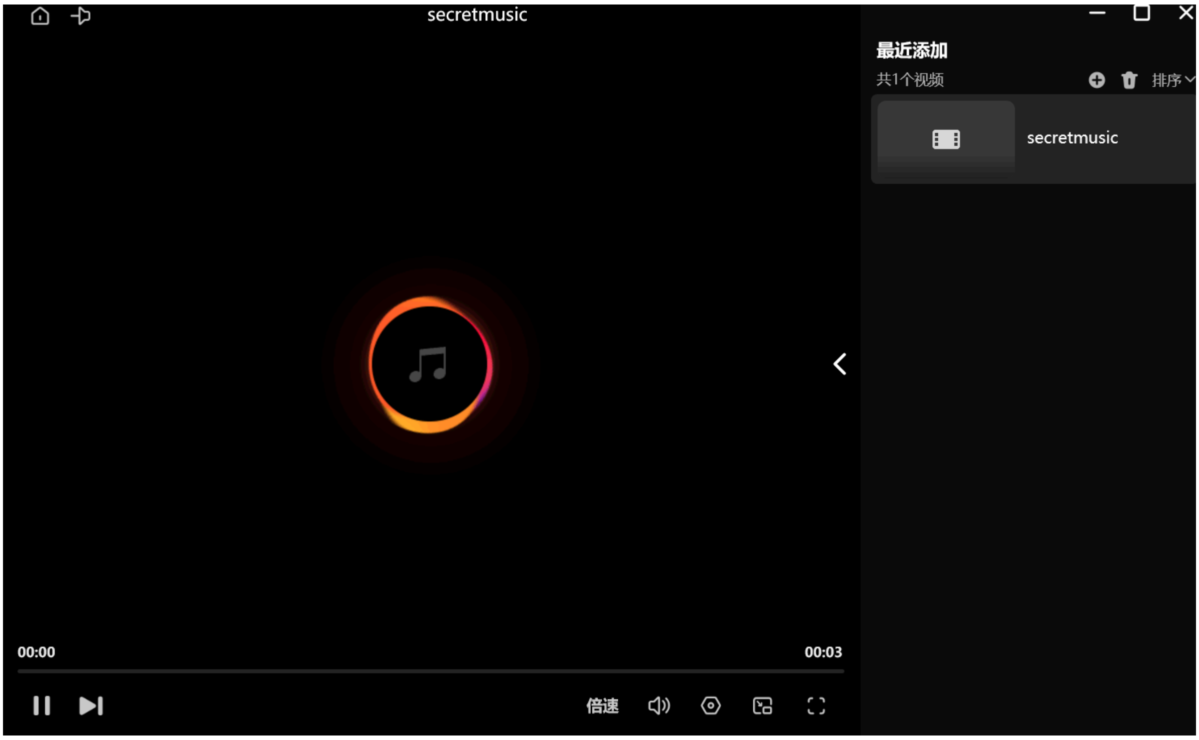
```
╔══════════╣ Backup folders
drwxr-xr-x 2 root root 4096 Nov 21 08:59 /var/backups
total 984
-rw-r--r-- 1 root root       51200 Nov 21 06:25 alternatives.tar.0
-rw-r--r-- 1 root root       21525 Aug 15 09:14 apt.extended_states.0
-rw-r--r-- 1 root root        2556 Apr  4  2025 apt.extended_states.1.gz
-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
```

下载到kali中并挂载到本地

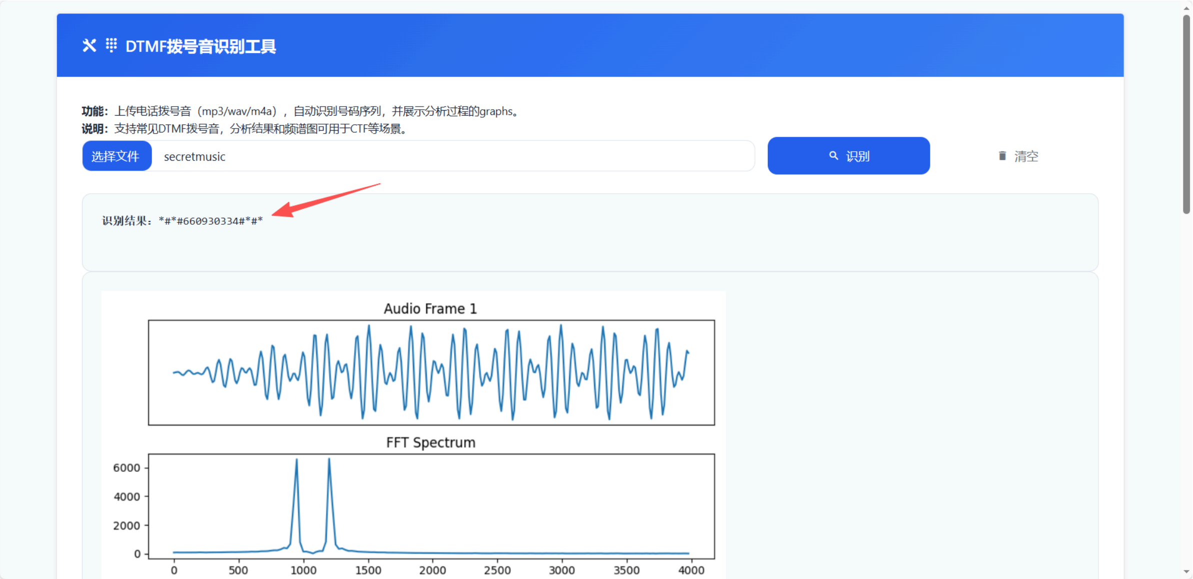
```
┌──(zsc㉿kali)-[~]
└─$ sudo mkdir /mnt/secret
[sudo] zsc 的密码：
# 尝试作为回环设备挂载
┌──(zsc㉿kali)-[/tmp]
└─$ sudo mount -o loop hidden.img /mnt/secret

┌──(zsc㉿kali)-[/tmp]
└─$ cd /mnt/secret

┌──(zsc㉿kali)-[/mnt/secret]
└─$ ls -al
总计 44
drwxr-xr-x 3 root root  1024 11月21日 21:57 .
drwxr-xr-x 3 root root  4096 12月27日 13:30 ..
drwx------ 2 root root 12288 11月21日 21:56 lost+found
-rwxr-xr-x 1 root root 27245 11月21日 21:01 secretmusic
```

将secretmusic下载下来，播放一下是一段3秒的手机拨号音频。这种音频称为双音多频（DTMF）

大家可以去dcode.fr了解：https://www.dcode.fr/dtmf-code#f0



我使用了一个在线的DTMF识别网站：https://tools.qsnctf.com/misc/dtmf_recognize



DTMF拨号音识别工具

功能：上传电话拨号音（mp3/wav/m4a），自动识别号码序列，并展示分析过程的graphs。
说明：支持常见DTMF拨号音，分析结果和频谱图可用于CTF等场景。

选择文件 secretmusic

识别结果：*#*#660930334#*#*

最终的识别结果为：

```
*#*#660930334#*#*
```

登录root

```
skr@GameShell3:~$ su
Password: *#*#660930334#*#*
root@GameShell3:/home/skr# id
uid=0(root) gid=0(root) groups=0(root)
root@GameShell3:/home/skr# cat /root/root.txt
flag{root-f0cc428ad5cb90aebdfc7aa4e778b2cc}
```