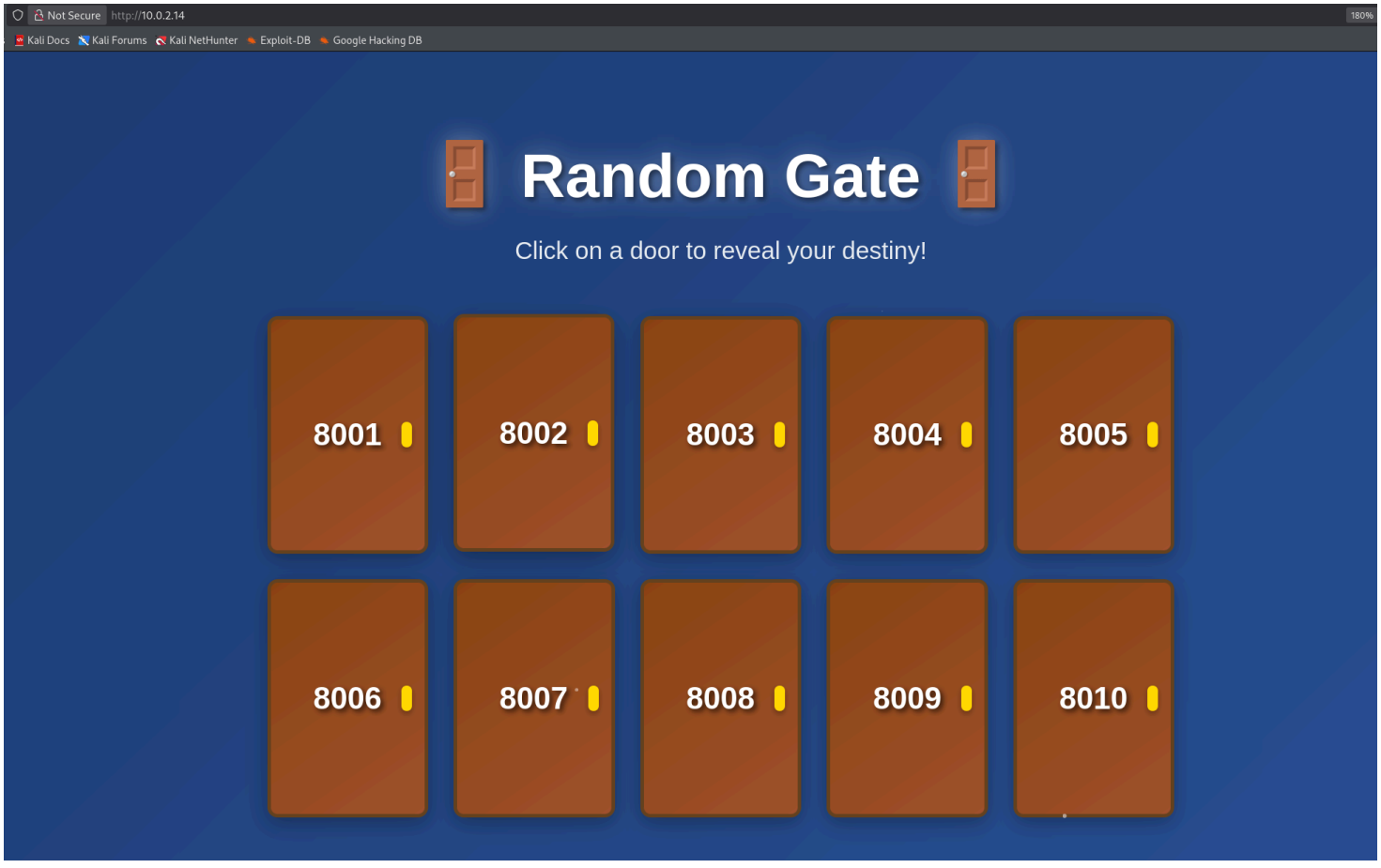
群友靶机-GameShell3

信息收集

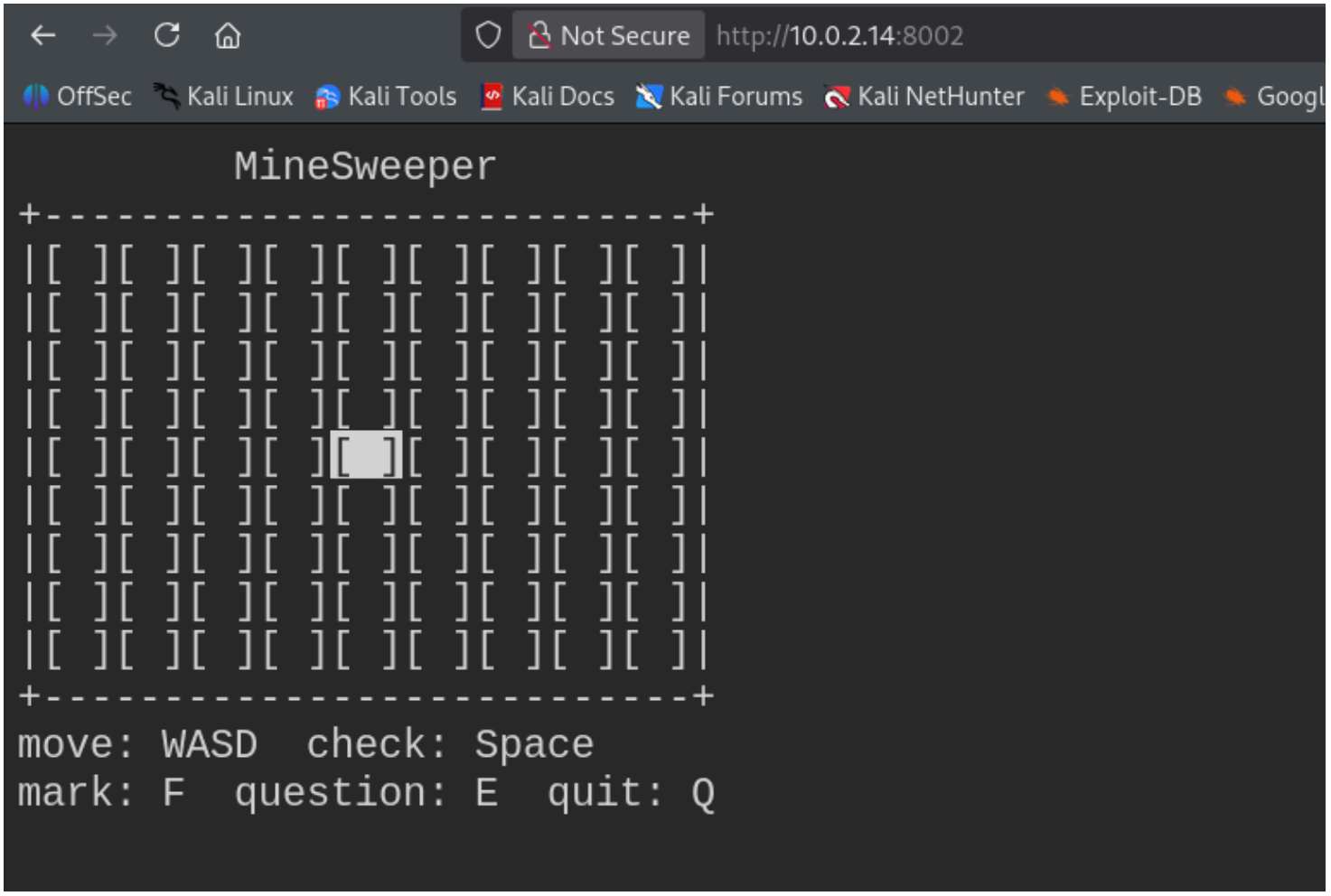
```
┌──(kali㉿kali)-[~/Desktop/maze-sec/gameshell3]
└─$ cat details.nmap
# Nmap 7.98 scan initiated Fri Dec 26 06:27:43 2025 as: /usr/lib/nmap/nmap -
p22,80,8001,8002,8003,8004,8005,8006,8007,8008,8009,8010 -A -oA details 10.0.2.14
Nmap scan report for 10.0.2.14
Host is up (0.00046s latency).

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-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
8002/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
8003/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)
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-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: Site doesn't have a title (text/html).
8006/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)
8007/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)
8008/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)
8009/tcp open  http    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
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
8010/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
MAC Address: 08:00:27:59:A4:3C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 10.0.2.14

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Dec 26 06:27:54 2025 -- 1 IP address (1 host up) scanned in 11.16
seconds
```

80端口是一个找门的小游戏 不过没啥东西 结合扫描信息重心应该在和门对应的端口



800X端口都是类似这种的小游戏 不过无法交互



在经历了漫长的尝试后 突然发现某个可以交互了

成功拿下扫雷 并获得一组凭据 `skr:skrampy1`

```
┌──(venv)─(kali㉿kali)-[~/Desktop/maze-sec/gameshell3/dtmf-decoder]
└─$ ssh skr@10.0.2.14
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
skr@10.0.2.14'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 08:26:34 2025 from 10.0.2.3
skr@GameShell3:~$ id
uid=1000(skr) gid=1000(skr) groups=1000(skr)
skr@GameShell3:~$ sh
$
```

ssh上去之后经常下线 可以切成sh可以避免

提权

```
$ find / -type f -newermt "2025-11-14" ! -newermt "2025-12-20" ! -path '/proc/*' ! -
path '/sys/*' ! -path '/run/*' -readable 2>/dev/null
/usr/local/bin/start-ttyd.sh
/usr/local/bin/mine.sh
/home/skr/.bashrc
/home/skr/user.txt
/etc/subgid-
/etc/resolv.conf.dhclient-new.12700
/etc/hosts
/etc/subgid
/etc/passwd-
/etc/resolv.conf.dhclient-new.825
/etc/group-
/etc/subuid-
/etc/systemd/system/ttyd.service
/etc/resolv.conf.dhclient-new.499
/etc/subuid
/etc/group
/etc/resolv.conf.dhclient-new.412
/etc/issue
/etc/hostname
/etc/passwd
/var/www/html/index.html
/var/backups/hidden.img
/var/backups/alternatives.tar.0
/var/log/fontconfig.log
```

```
/var/log/apt/eipp.log.xz
/var/log/apt/history.log
/var/log/dpkg.log
/var/log/alternatives.log
/var/log/faillog
/var/log/journal/52a22a6e47cb4a5995fb43c3554baa0e/user-1000@000644184b0dc93d-
06613fd7a9f47a54.journal~
/var/lib/dpkg/info/lsof.list
/var/lib/dpkg/status
/var/lib/dpkg/status-old
/var/lib/apt/extended_states
/var/cache/apt/pkgcache.bin
$ ls -al /var/backups/hidden.img
-rw-r--r-- 1 root root 104857600 Nov 21 04:54 /var/backups/hidden.img
```

翻文件发现了 `hidden.img` 下载下来挂到本地看看

```
┌──(kali㉿kali)-[~/Desktop/maze-sec/gameshell3]
└─$ wget http://10.0.2.14:6666/hidden.img
--2025-12-26 08:34:14--  http://10.0.2.14:6666/hidden.img
Connecting to 10.0.2.14:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 104857600 (100M) [application/octet-stream]
Saving to: ‘hidden.img’

hidden.img                          100%
[=================================================>] 100.00M   103MB/s    in 1.0s

2025-12-26 08:34:15 (103 MB/s) - ‘hidden.img’ saved [104857600/104857600]


┌──(kali㉿kali)-[~/Desktop/maze-sec/gameshell3]
└─$ sudo mkdir -p /mnt/hidden_img

[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/maze-sec/gameshell3]
└─$ sudo mount -o loop hidden.img /mnt/hidden_img

┌──(kali㉿kali)-[~/Desktop/maze-sec/gameshell3]
└─$ cd /mnt

┌──(kali㉿kali)-[/mnt]
└─$ ls -la
total 9
drwxr-xr-x  3 root root 4096 Dec 26 08:34 .
drwxr-xr-x 19 root root 4096 Dec 24 21:16 ..
drwxr-xr-x  3 root root 1024 Nov 21 08:57 hidden_img

┌──(kali㉿kali)-[/mnt]
└─$ cd hidden_img
```

```
┌──(kali㉿kali)-[/mnt/hidden_img]
└─$ ls -la
total 44
drwxr-xr-x 3 root root  1024 Nov 21 08:57 .
drwxr-xr-x 3 root root  4096 Dec 26 08:34 ..
drwx------ 2 root root 12288 Nov 21 08:56 lost+found
-rwxr-xr-x 1 root root 27245 Nov 21 08:01 secretmusic
```

发现了 `secretmusic` 听了一下感觉和打电话的拨号声挺像的

关键词搜索 找到了DTMF

音频隐写汇总

一、电话号码dtmf识别。

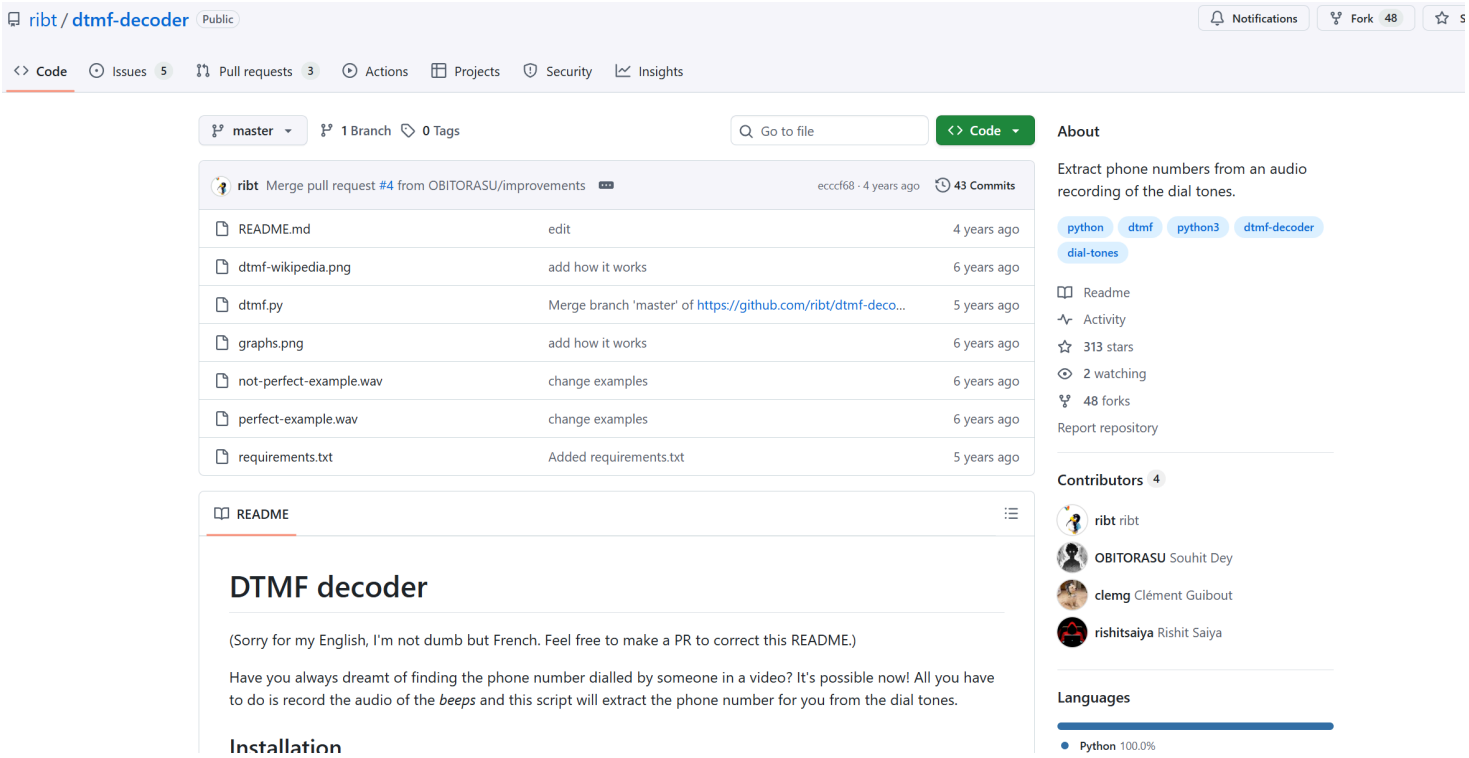
> 题源-moectf2021新生赛。因为比赛没结束，所有音频文件不能放上来。

下载之后是wav音频文件：

直接打开听一下，很容易就能发现他是电话号码那个拨号的声音。实际上这是DTMF。

> 拉到Adobe Audition里面是下面这个样子。我们可以手动比照上面那个表格得到数字，也可以用dtmf2num.exe自动解码。

github上面找一个高star的工具 dtmf-decoder




```
┌──(venv)─(kali㉿kali)-[~/Desktop/maze-sec/gameshell3/dtmf-decoder]
└─$ python dtmf.py
usage: dtmf.py [-h] [-v] [-l] [-r] [-d] [-t F] [-i T] file
dtmf.py: error: the following arguments are required: file

┌──(venv)─(kali㉿kali)-[~/Desktop/maze-sec/gameshell3/dtmf-decoder]
└─$ python dtmf.py ../secretmusic
*#*#660930334#*#*
```

成功解出密码 `*#*#660930334#*#*`

```
$ su root
Password:
root@GameShell3:/var/backups# id
uid=0(root) gid=0(root) groups=0(root)
```

结束