Gameshell3

获取靶机地址：
https://maze-sec.com/
qq群：660930334

配置：

靶机用VirtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334
1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式

```
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33

reboot -f
```

主机发现

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.44.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-26 07:48 EST
Nmap scan report for 192.168.44.157
Host is up (0.00013s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8007/tcp open  ajp12
8008/tcp open  http
8009/tcp open  ajp13
8010/tcp open  xmpp
MAC Address: 00:0C:29:D2:A5:B6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

这里不止这个但是太多了就不用nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.157的图了

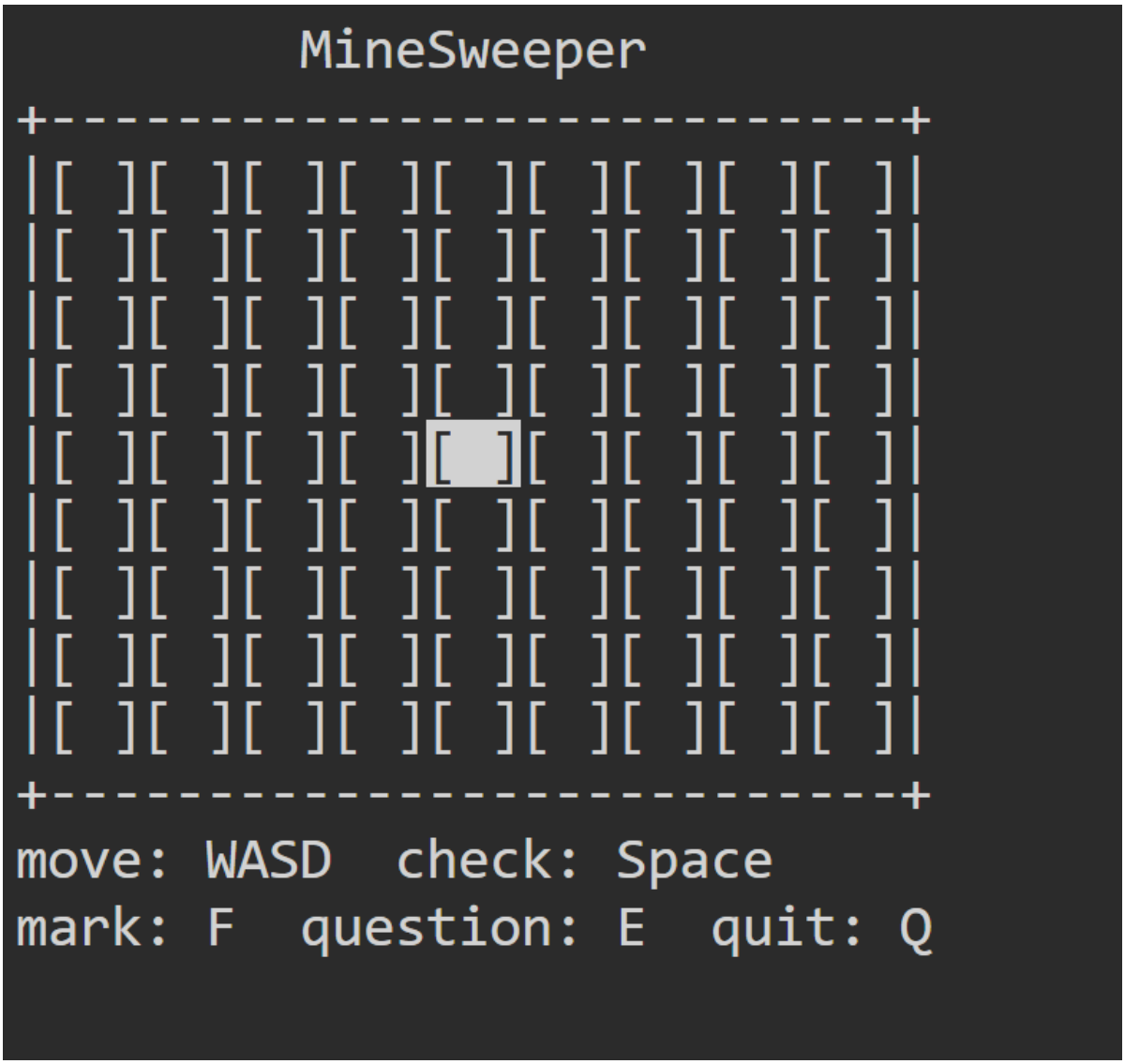
就是22,80以及Web终端服务ttyd 1.7.7映射到8001-8010端口

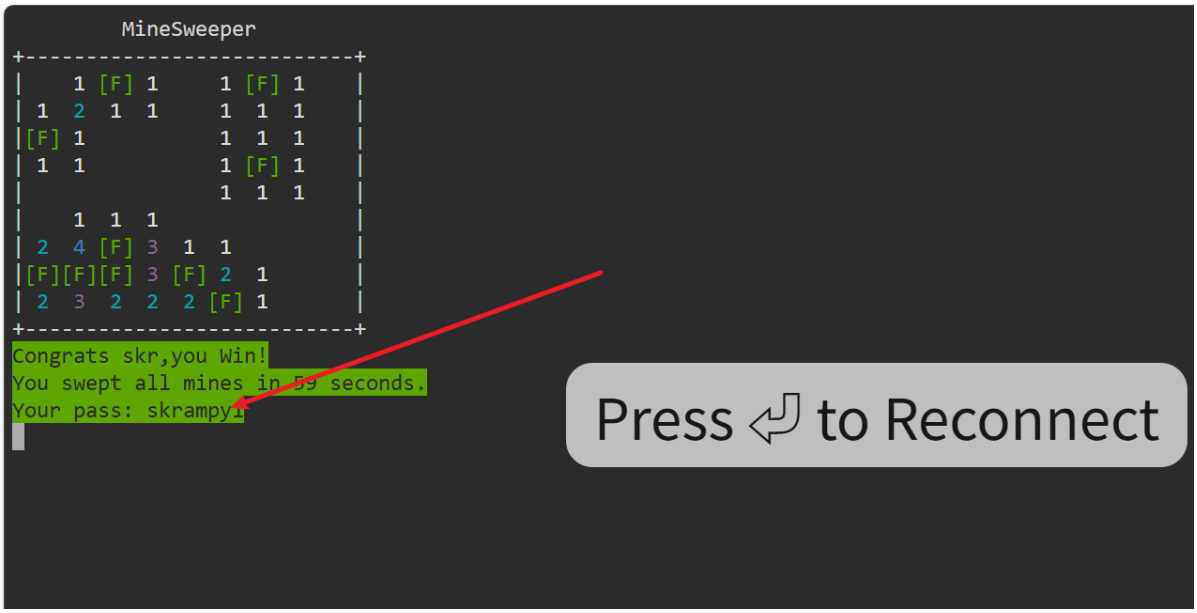
80端口探测

是一个前端小页面，可以联想到那10个端口，分别去点只有一个是亮的，那就很正常的可以联想的到去访问那个端口。

8009端口探测

当然了，因为这个是随机映射的，不一定只有8009端口
进去之后发现是一个扫雷小游戏，来都来了那就打一把吧
通关之后会给出一个用户skr和密码skrampy1





ssh连接

```
ssh skr@192.168.44.157
这时候发现每次连上去之后一下子就断开一下子就断开
显示是长时间无操作端口，那就看看设置的时间 发现是5秒内
设置一下就好了export TMOUT=3600
```

```
skr@GameShell3:~$ echo $TMOUT
5
skr@GameShell3:~$
```

flag1

```
skr@GameShell3:~$ ls -la
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    50 Dec 26 08:14 .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}
skr@GameShell3:~$
```

信息探测

```
发现啥都看不到sudo，定时任务，那就再看看有啥特殊文件喽
```

```
skr@GameShell3:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for skr:
Sorry, user skr may not run sudo on GameShell3.
skr@GameShell3:~$ crontab -l
no crontab for skr
skr@GameShell3:~$
```

```
skr@GameShell3:~$ find / -type f -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
skr@GameShell3:~$
```

最后在备份文件夹/backup下找到了一个隐藏的镜像文件

```
skr@GameShell3:/var$ cd backups/
skr@GameShell3:/var/backups$ ls -la
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
skr@GameShell3:/var/backups$
```

挂载探索

把hidden下载下来，在本地挂载起来看看

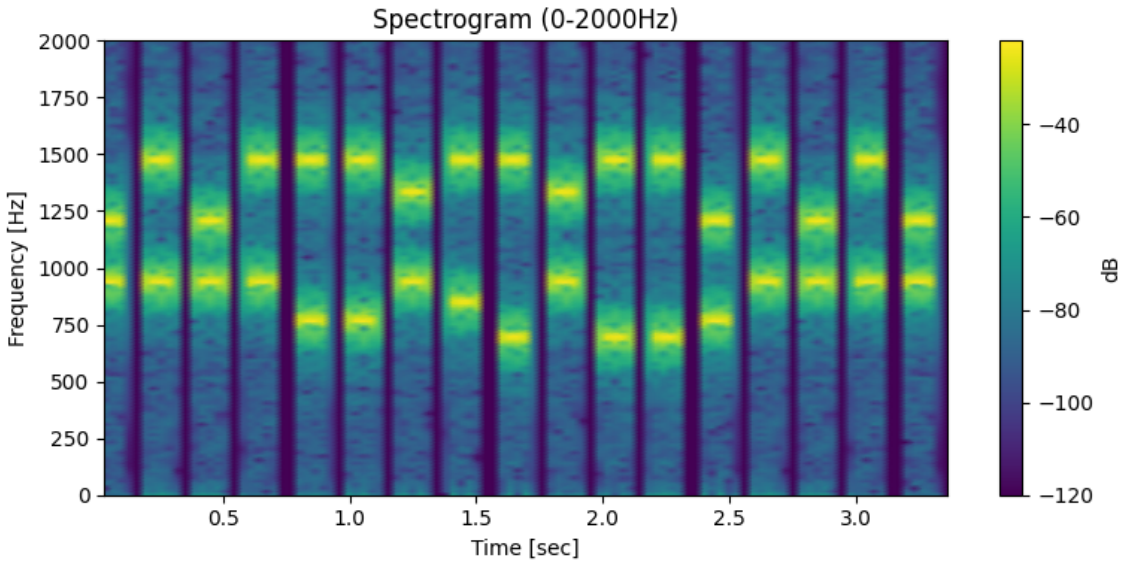
```
mkdir /mnt/hidden
mount -o loop /home/kali/hidden.img /mnt/hidden
```

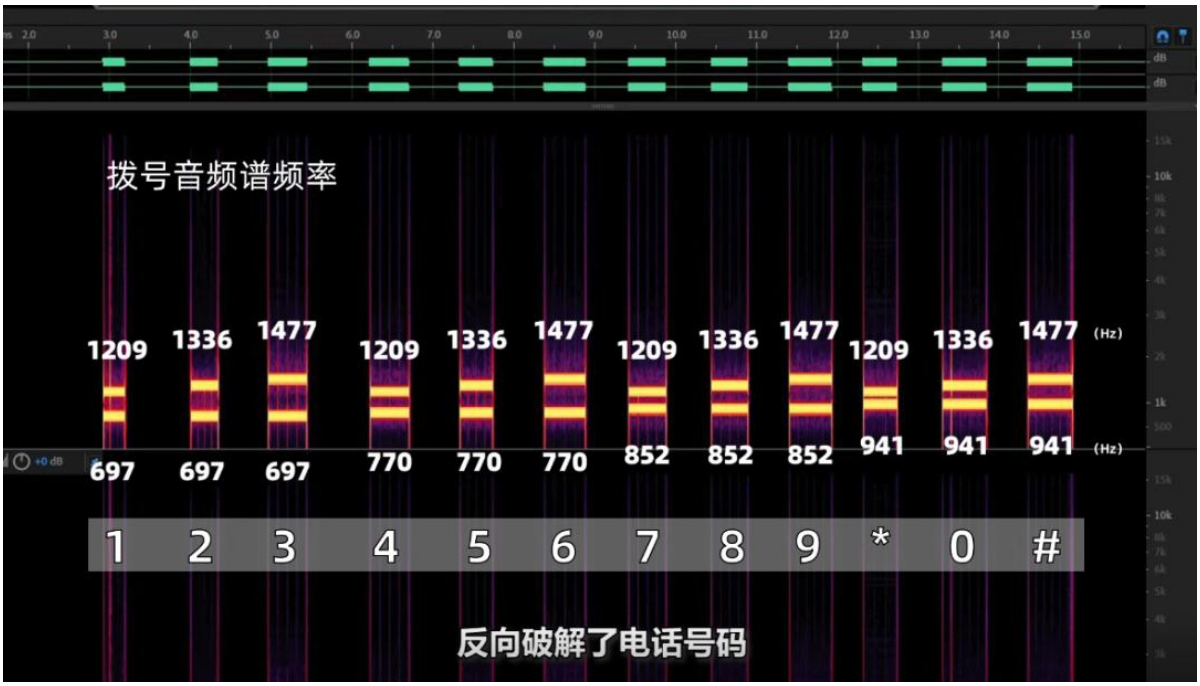
获得了一段密码的音频

```
┌──(root㉿kali)-[/home/kali]
└─# cd /mnt/hidden

┌──(root㉿kali)-[/mnt/hidden]
└─# ls -la
total 44
drwxrwxrwx 3 root root  1024 Nov 21 08:57 .
drwxr-xr-x 3 root root  4096 Dec 26 05:53 ..
drwx------ 2 root root 12288 Nov 21 08:56 lost+found
-rwxr-xr-x 1 root root 27245 Nov 21 08:01 secretmusic

┌──(root㉿kali)-[/mnt/hidden]
└─#
```

音频破解

根据频率猜测是手机拨号音，于是打算用耳朵听出来密码，展示一下自己
结果发现所有音都是长一个样的，所以还是靠科学吧






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

flag2

```
ssh root@192.168.44.157
```

```
┌──(root㉿kali)-[/mnt/hidden]
└─# ssh root@192.168.44.157
root@192.168.44.157'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.
root@GameShell3:~# ls -la
total 36
drwx------  6 root root 4096 Nov 21 09:52 .
drwxr-xr-x 18 root root 4096 Dec 26 02:52 ..
-rw-------  1 root root    0 Nov 21 09:52 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  4 root root 4096 Apr  4  2025 .cache
drwx------  3 root root 4096 Apr  4  2025 .gnupg
drwxr-xr-x  3 root root 4096 Mar 18  2025 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   44 Nov 21 09:34 root.txt
drwx------  2 root root 4096 Nov 21 04:52 .ssh
root@GameShell3:~# cat root.txt
flag{root-f0cc428ad5cb90aebdfc7aa4e778b2cc}
root@GameShell3:~#
```