

| GameShell 3

| GameShell 3

| 主机扫描

```
sudo arp-scan -I eth0 --localnet
```



```
export ip=192.168.56.167
```

| 端口扫描

```
rustscan -a $ip --ulimit 5000 -- -sV -sC
```

| 扫雷



本以为按照道理来说就是 8005 端口，但是发现如何移动都动不了，最后发现原来是骗人的，哈哈，动不了就不对，找个能动的端口就正确了

```
skr:skrampy1
```

```
skr@GameShell3:~$ cat user.txt
flag{user-a2a53d2efdda06bc16093ad7b3551709}
```

提权

Skr -> root

可以先配置一下 SSH 免密，这样可能会方便一点，不要输入一次命令再输入密码

```
ssh skr@$ip "cat ~/.bashrc"
```

```
# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
TMOUT=5
export TMOUT
```

所以是这个导致连接了就断开，再次连接，直接 `unset`

```
unset TMOUT
```

然后删除最后两行

```
Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (Limit 70)
-rw-r--r-- 1 skr skr 128546 Dec 26 08:03 /tmp/linpeas.txt
-rwxr-xr-x 1 skr skr 975444 Dec 26 08:01 /tmp/linpeas.sh
-rwxr--r-- 1 skr skr 3104768 Dec 26 08:01 /tmp/pspy64
-rw-r--r-- 1 root root 104857600 Nov 21 04:54 /var/backups/hidden.img
-rw-r--r-- 1 root root 51200 Nov 21 06:25 /var/backups/alternatives.tar.0
```

这个感觉就在说我有问题，你快来看，而且我还发现了一个东西

```
skr@GameShell3:~$ find / \( -path /proc -o -path /sys -o -path /run -o -path /dev -o -path /var -o -path /etc -o -path /boot -o -path /usr \) -prune -o -user root -print 2>/dev/null
/
/root
/initrd.img.old
/vmlinuz.old
/vmlinuz
/lib32
/libx32
/tmp
/tmp/.Test-unix
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/systemd-private-528b0f70ac134cffbef6480c28cece4f-systemd-timesyncd.service-gUEZM1
/tmp/systemd-private-528b0f70ac134cffbef6480c28cece4f-systemd-logind.service-V3KkhH
/tmp/.XIM-unix
/tmp/.X11-unix
/tmp/systemd-private-528b0f70ac134cffbef6480c28cece4f-apache2.service-40oCbi
/home
/home/skr/user.txt
/lost+found
/initrd.img
/opt
/media
/media/cdrom
/media/cdrom0
/sbin
/mnt
/mnt/.hidden
/bin
/lib64
/srv
/lib
```

应该是之前挂载时候留下来的记录，我们下载一下用 Diskgenius 打开，然后导出出来一个 `secretmusic` 文件，这个文件是 `.wav` 格式的，打开听了一下 `dtmf` 拨号声

```
$ dtmf2num secretmusic.wav
```

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

直接作为 root 密码 ssh 连接

```
root@GameShell13:~# cat root.txt  
flag{root-f0cc428ad5cb90aebdfc7aa4e778b2cc}
```