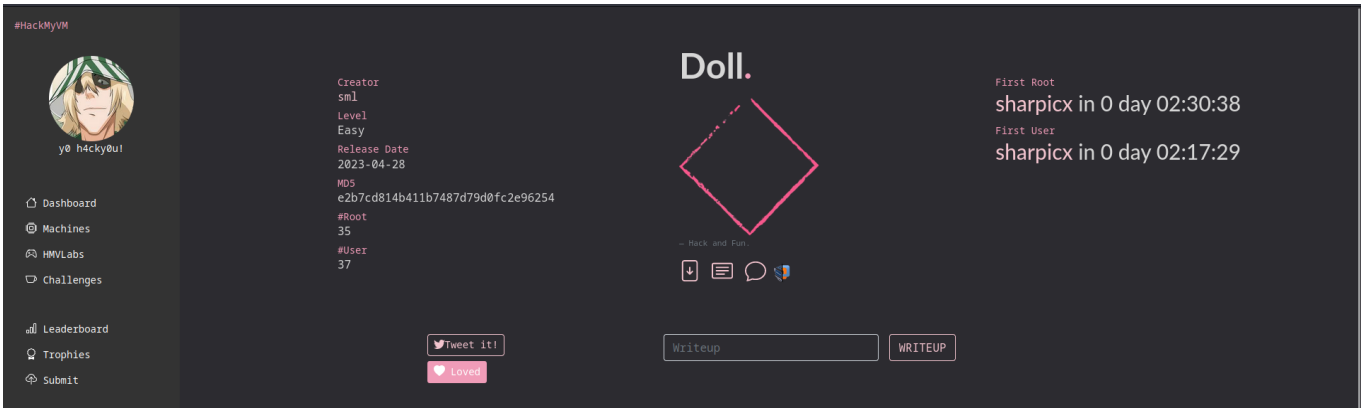
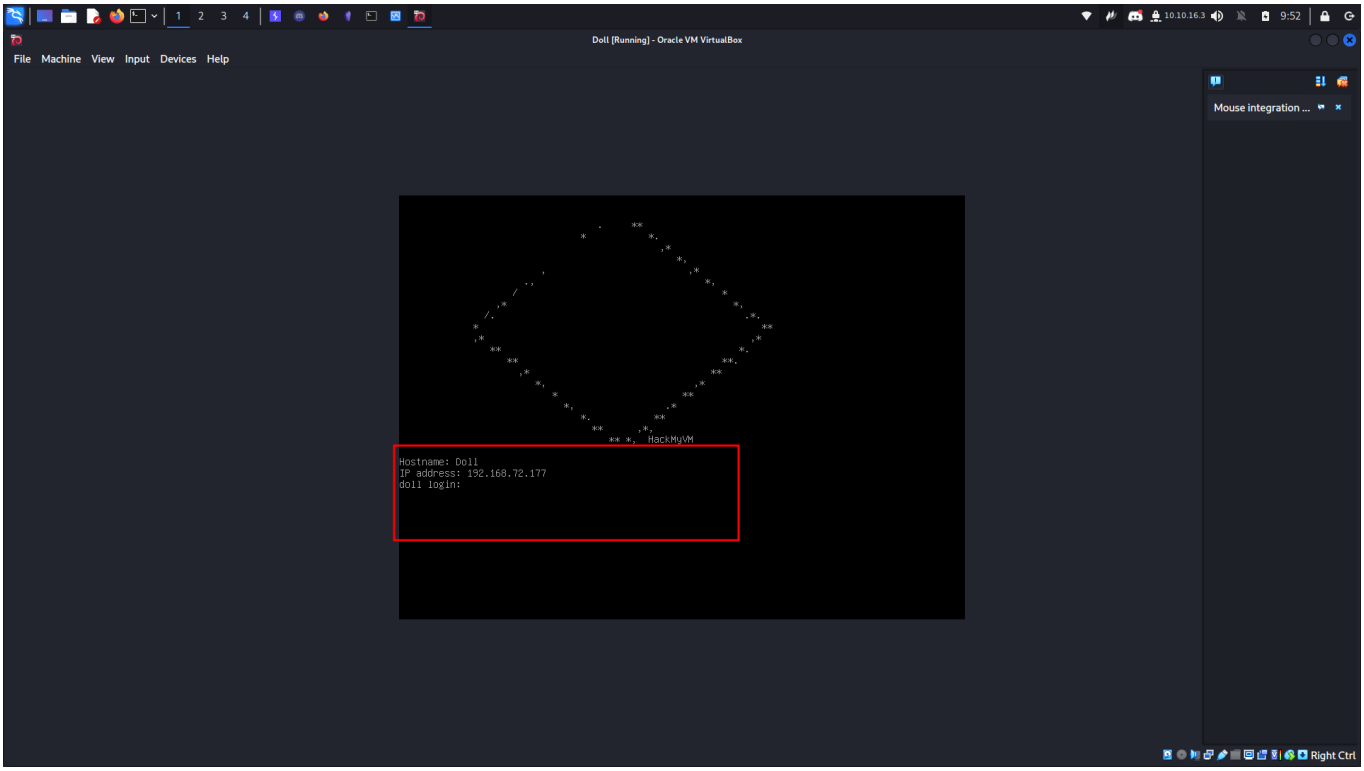
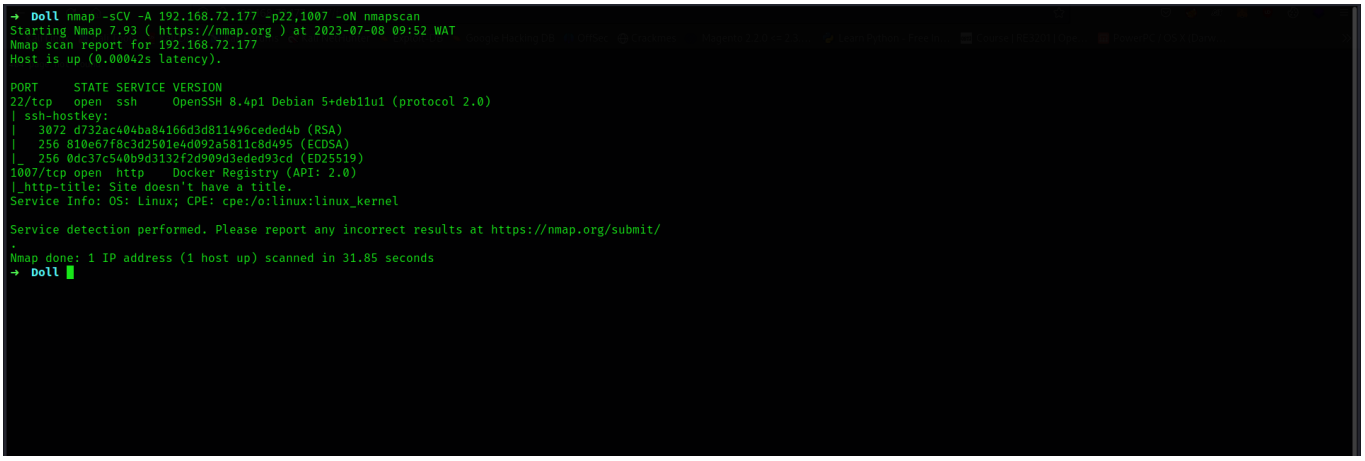


First thing let us get the machine IP address

After opening it in virtual box and it runs I'll see the IP



Nmap Scan:



Enumeration

On port 1007 runs `Docker Registry (API: 2.0)`

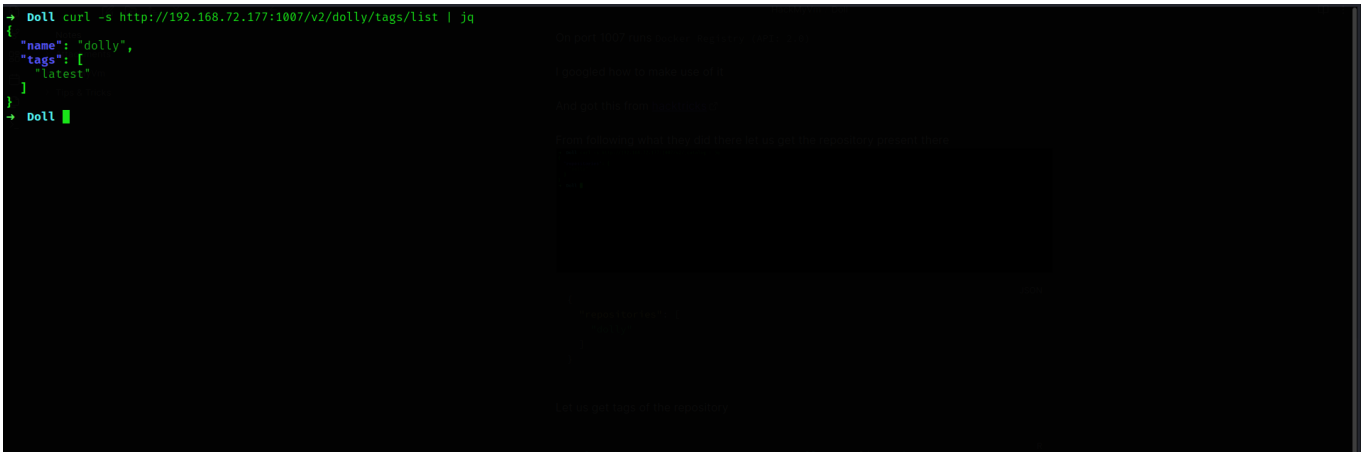
I googled how to enumerate it

And got this from hacktricks

From following what they did there let us get the repository present there


```
{
  "repositories": [
    "dolly"
  ]
}
```

Let us get tags of the repository




```
curl -s http://192.168.72.177:1007/v2/dolly/tags/list | jq
```

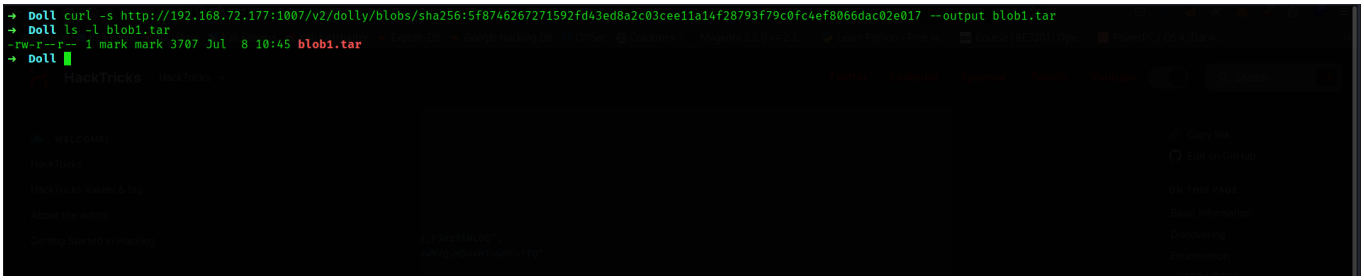
Now we get the manifests


```
curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest | jq
```

In object `v1Compatibility` has a password

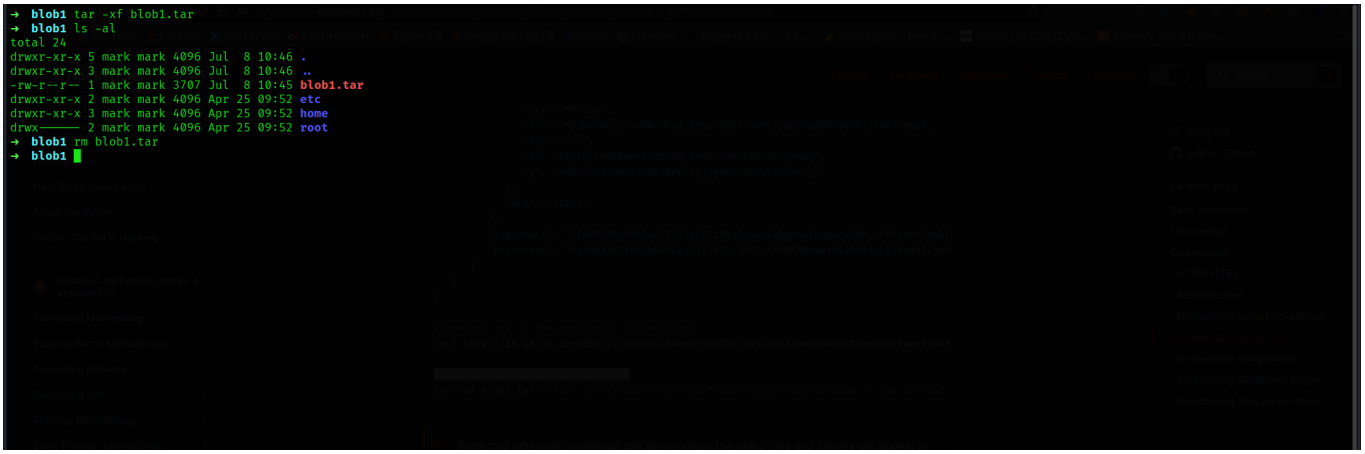

```
Password: devilcollectsit
```

Download one of the previously listed blobs



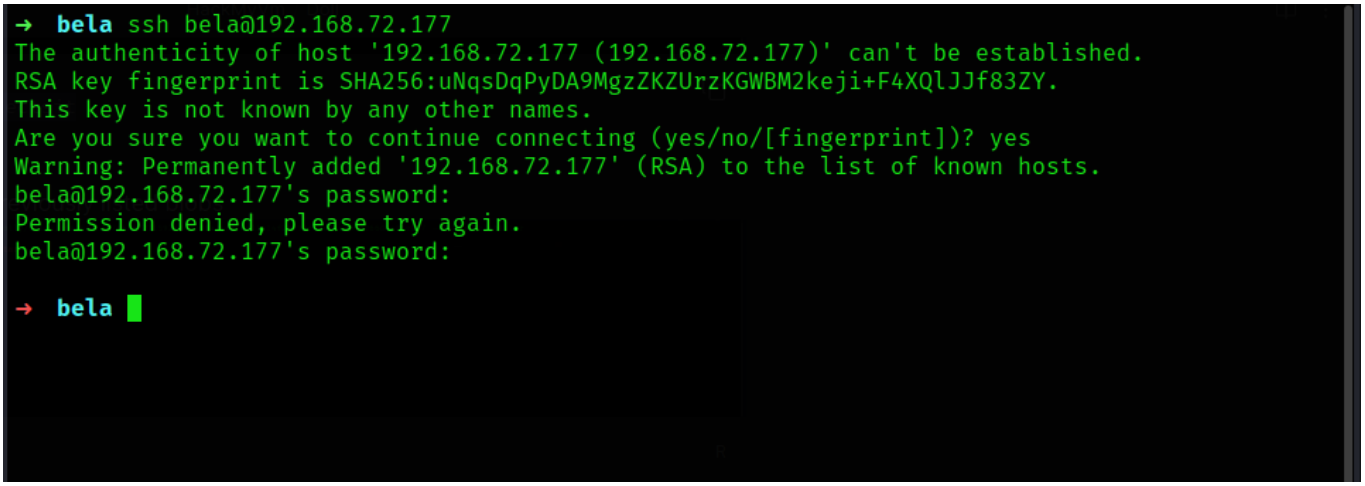

```
curl -s
http://192.168.72.177:1007/v2/dolly/blobs/sha256:5f8746267271592fd43ed8a2c03
cee11a14f28793f79c0fc4ef8066dac02e017 --output blob1.tar
```

Inspect the insides of each blob



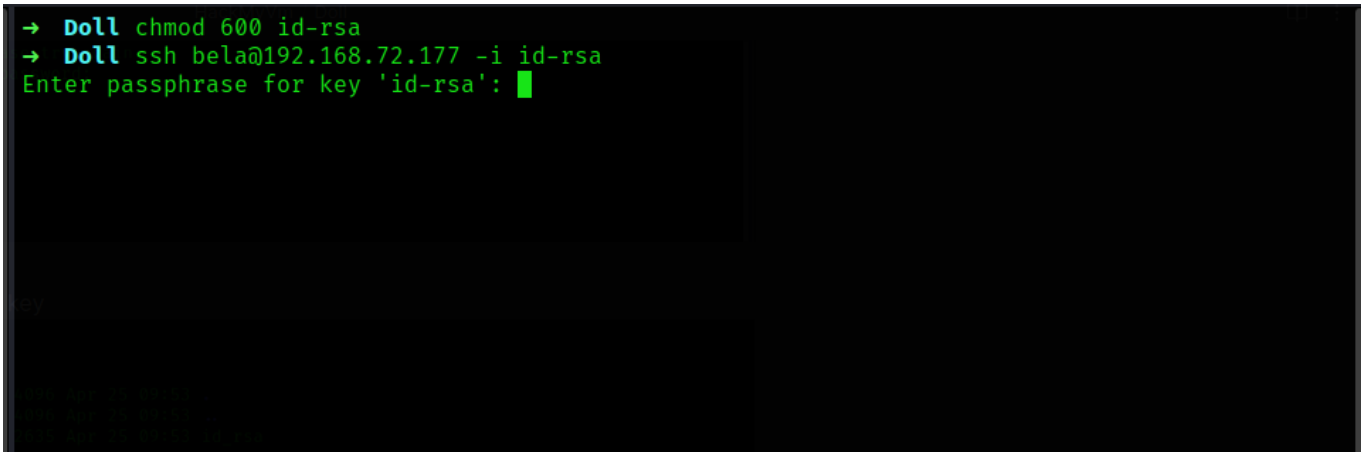
In the home directory there's a user named `bela`

I tried to login with the credential gotten but it doesn't work

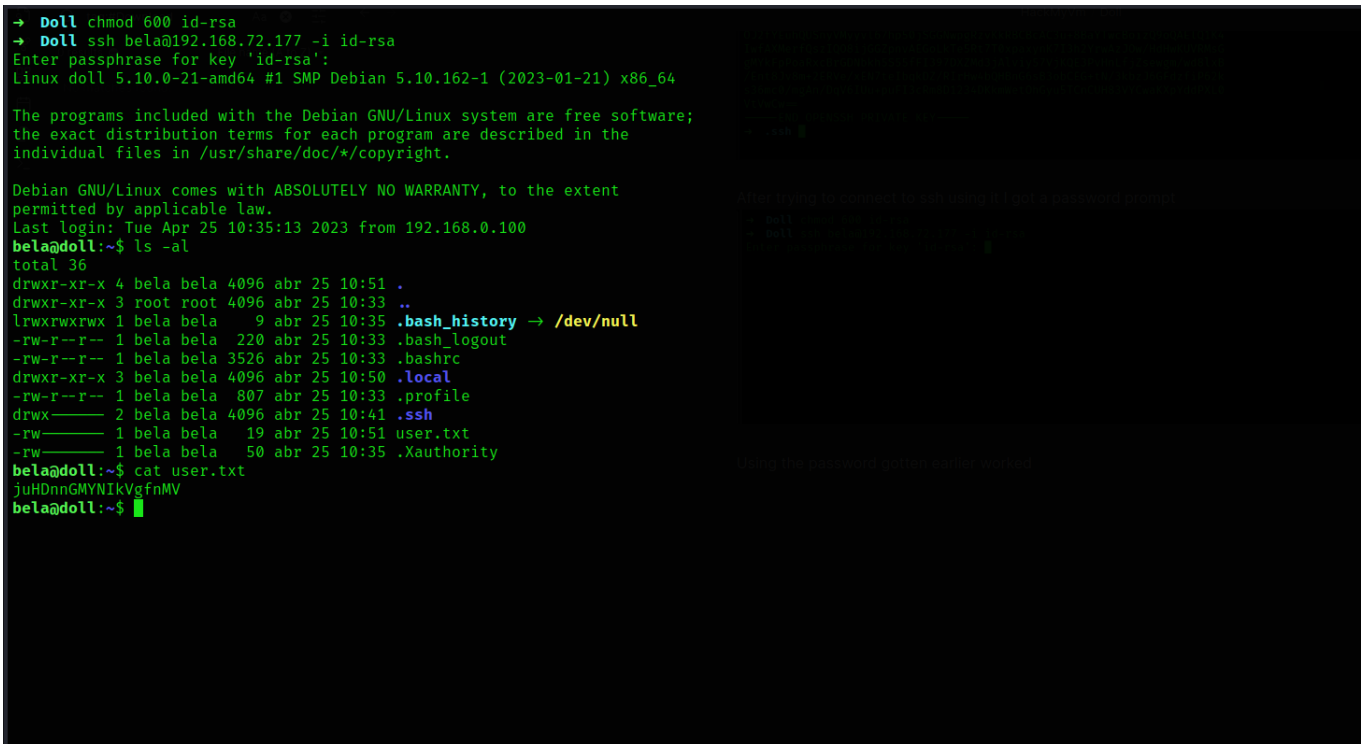


But the user has a ssh key

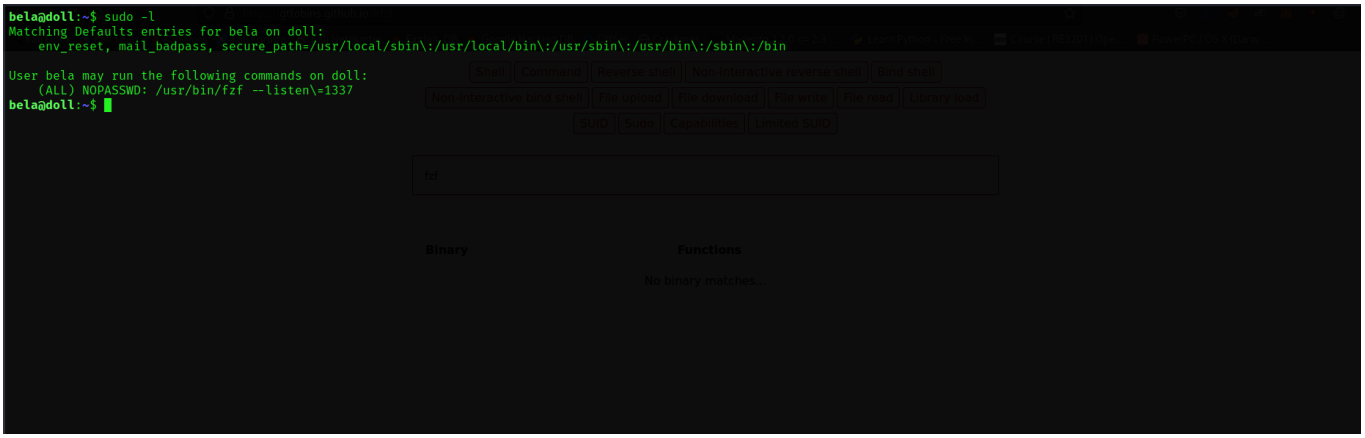
After trying to connect to ssh using it I got a password prompt



Using the password gotten earlier worked

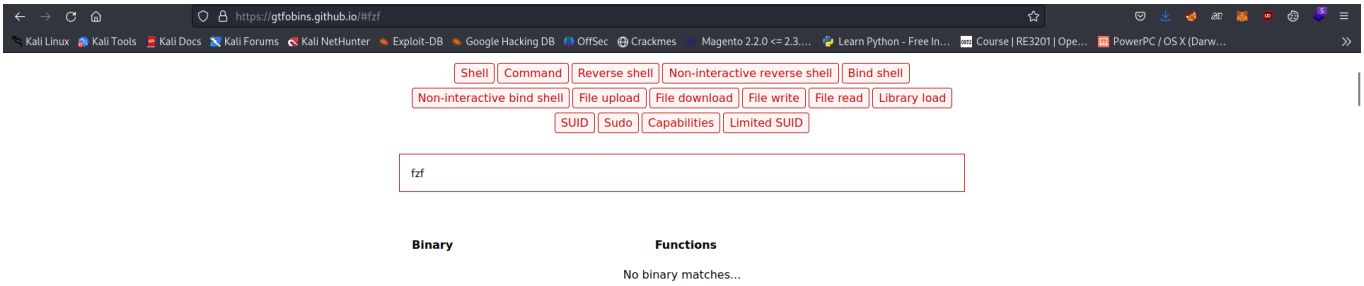


Checking for sudo permission shows this

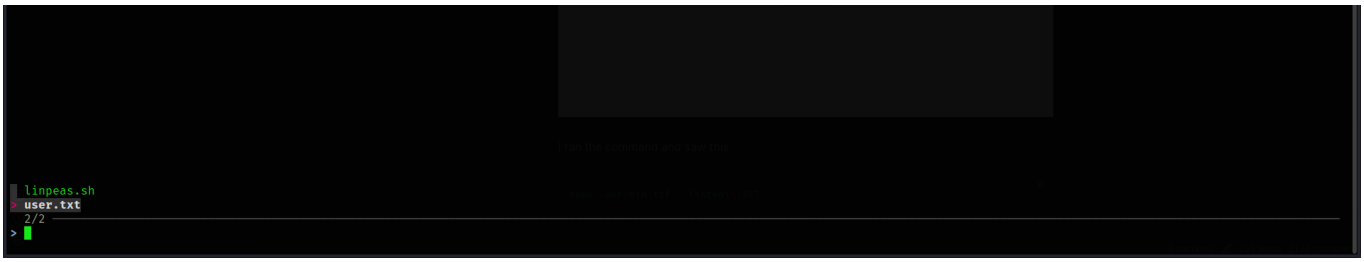



```
(ALL) NOPASSWD: /usr/bin/fzf --listen\=1337
```

I didn't get any when I searched it on [gtfobins]



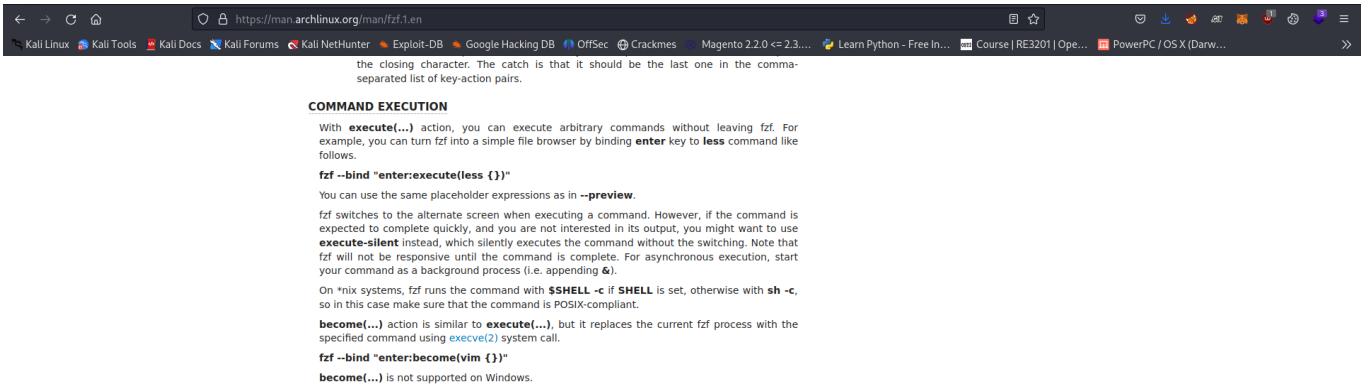
I ran the command and saw this



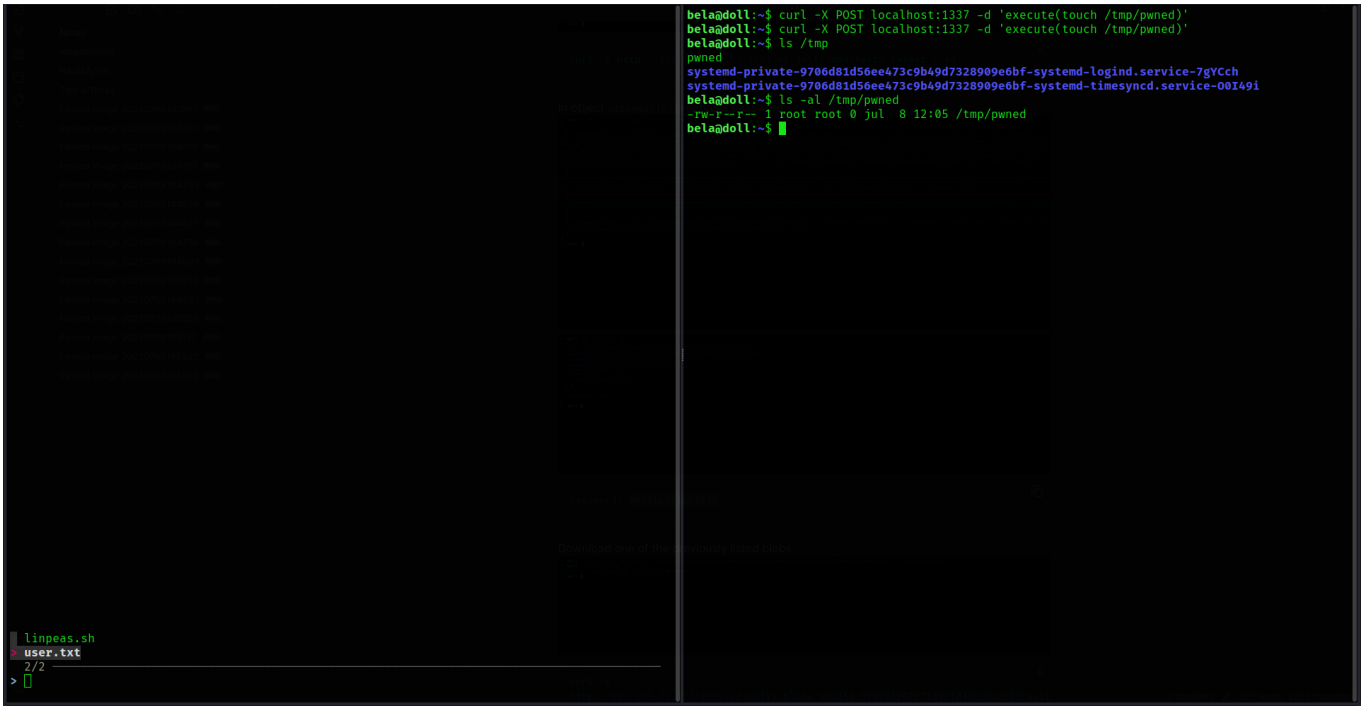

```
sudo /usr/bin/fzf --listen\=1337
```

It seems to be doing file list but what I want is a shell

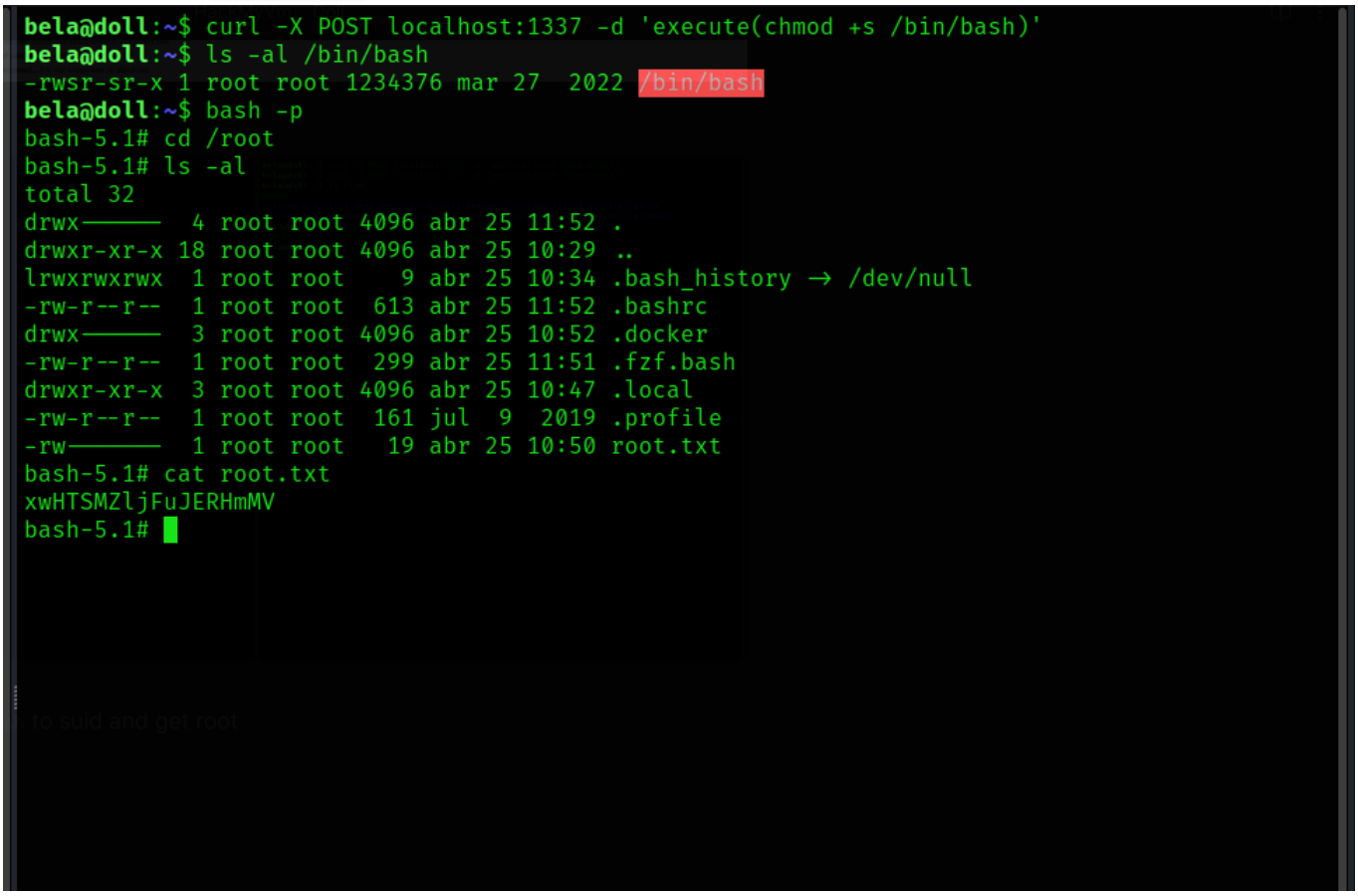
I then googled how to run command using fzf and got [this]



Doing it works



Now I can set `/bin/bash` to suid and get root



What I have learnt:

- Enumerating docker registry
- Taking advantage of sudo permission

#docker #registry #sudo