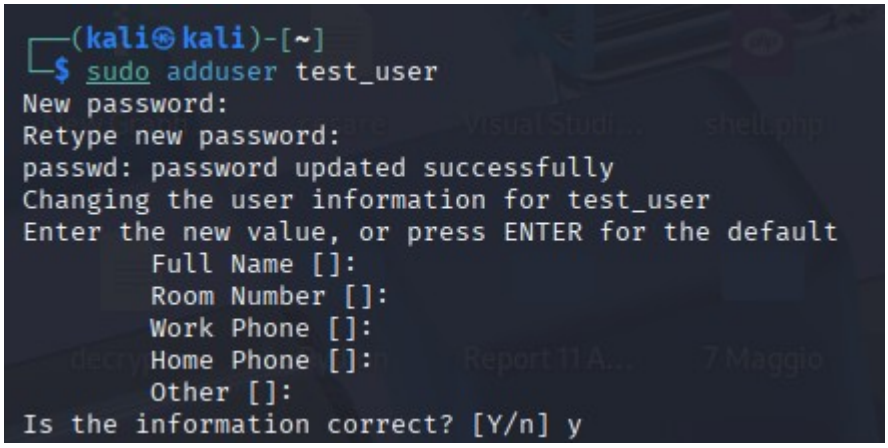
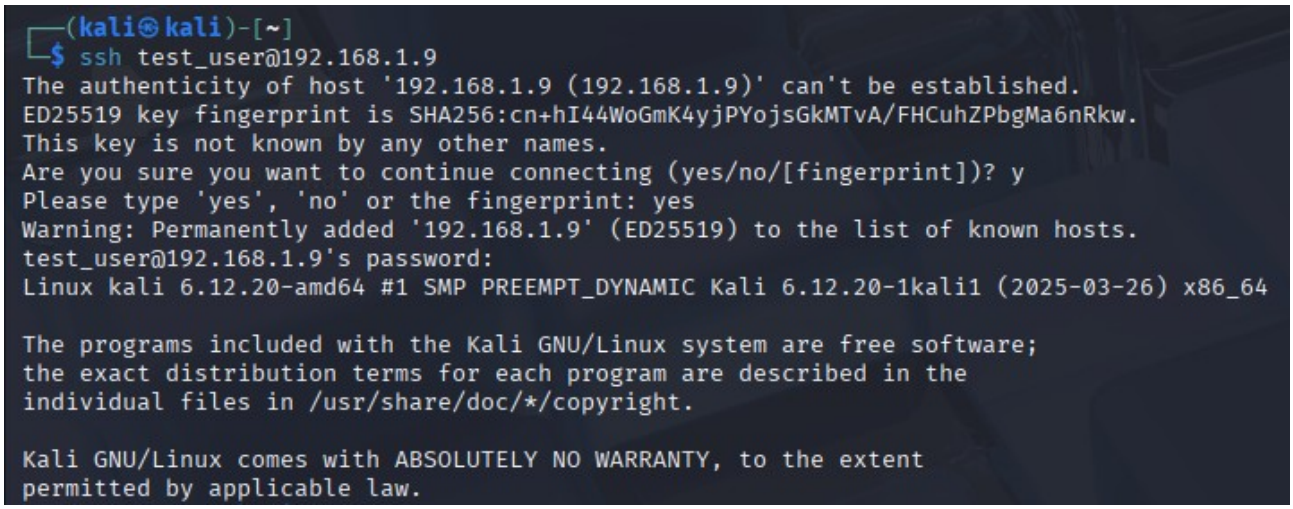
Cracking password con Hydra

1.Nell esercizio di oggi andremo ad eseguire un attacco di brute force sulla nostra macchina kali utilizzando il programma hydra.

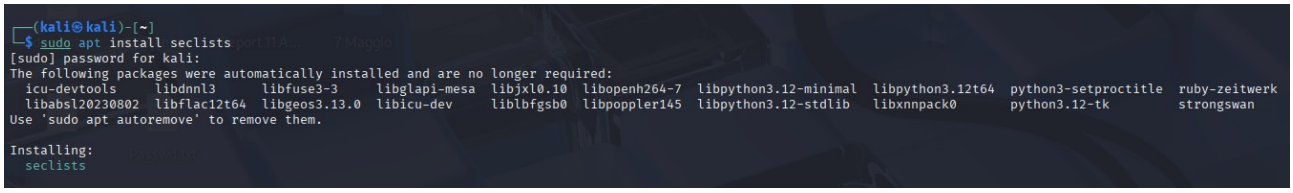
Come prima cosa andiamo a creare un nuovo utente con la propria password. Questo sarà il nostro target da “exploitare”.



Andiamo successivamente ad attivare il servizio **ssh** per avviare una connessione remota tramite la porta **22**



Una volta creato il nostro utente andiamo ad istallare una libreria di utenti e password da far utilizzare a Hydra (**seclists**)

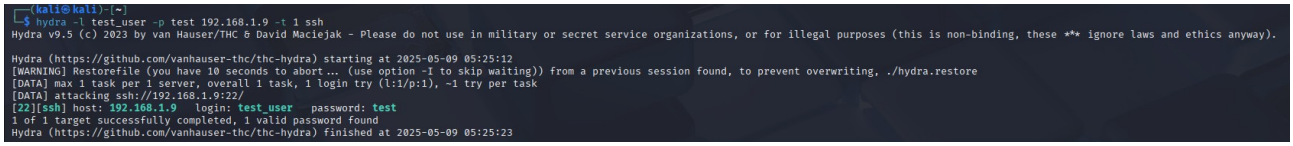


Passiamo poi ad attaccare l'autenticazione SSH con Hydra con il seguente comando,

Dove troviamo l'ip della nostra kali, il **numero di thread**, ovvero **quanti tentativi simultanei** vengono fatti in parallelo durante l'attacco, in questo caso **1**, **–L**, e **–P** si usano se vogliamo utilizzare delle liste per l'attacco a dizionario, -**V** per vedere in tempo reale i tentativi di crack e **-f** per dire di fermarsi quando trova la password e l'utente corretti.

Questo metodo e efficace ma molto tedioso.

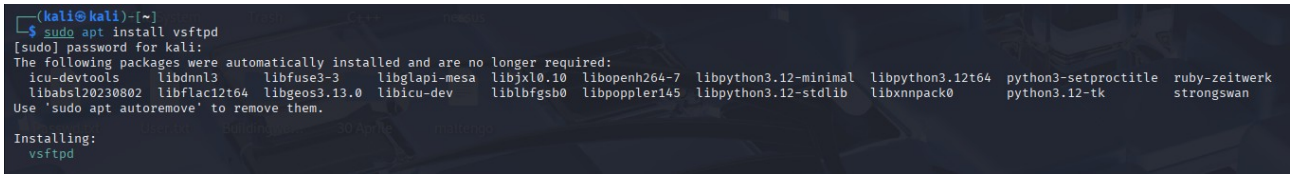
Per velocizzare e per dare una dimostrazione del funzionamento di hydra, andremo ad utilizzare quest'altro comando

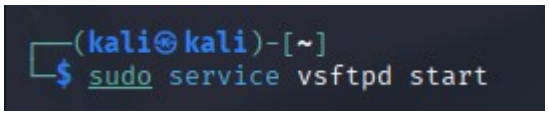


Nel nostro caso, conosciamo già il nome utente e la password, , quindi non bisogna inserire libreria di nomi utente e password da far utilizzare a hydra, ma basta inserire le credenziali da noi conosciute, andando, inoltre, a modificare **-l e -p** in minuscole, siccome vogliamo utilizzare un singolo username ed una singola password.

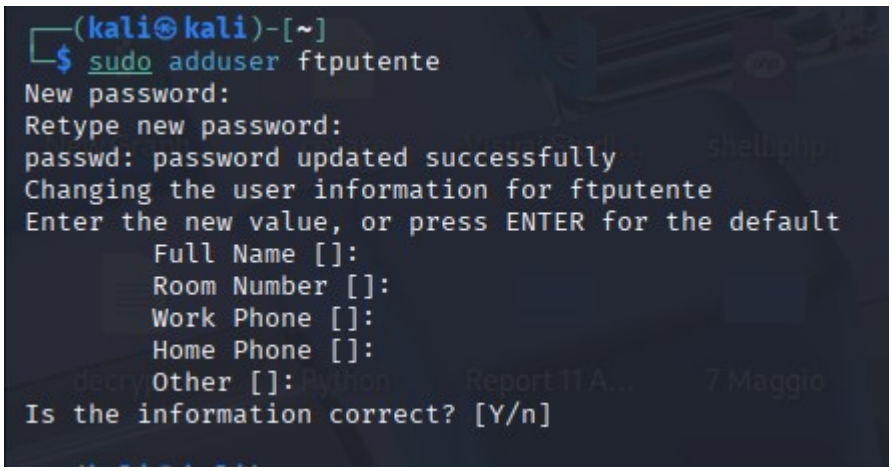
2. Per la seconda parte dell'esercizio andiamo a craccare un altro servizio con hydra: **FTP**

Andiamo ad istallare il servizio e poi avviamolo.

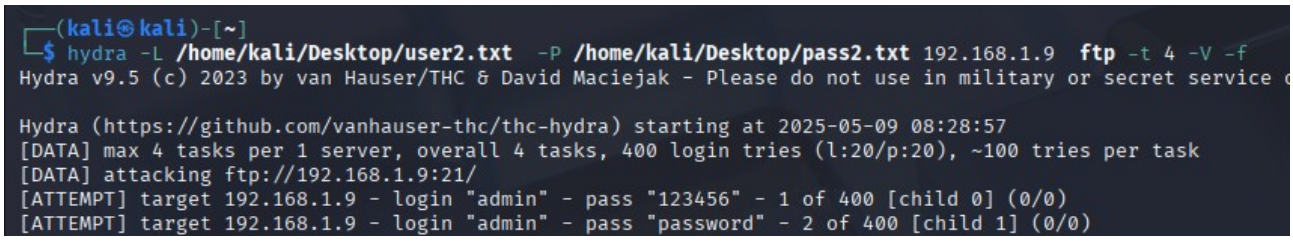




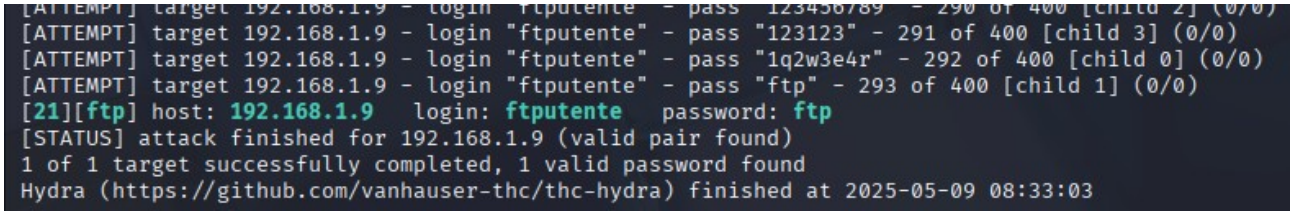
Andiamo nuovamente a creare un utente con la propria password.



Sempre per accorciare i tempi, utilizziamo delle liste utenti e password create da noi.



Alla fine hydra ci restituirà i dati corretti che si trovavano nelle liste che abbiamo creato.



3. **Considerazioni finali**

Questi test dimostrano che l'utilizzo di **password deboli, o troppo comuni,** e servizi non sicuri possano esporre a **gravi rischi di compromissione**.