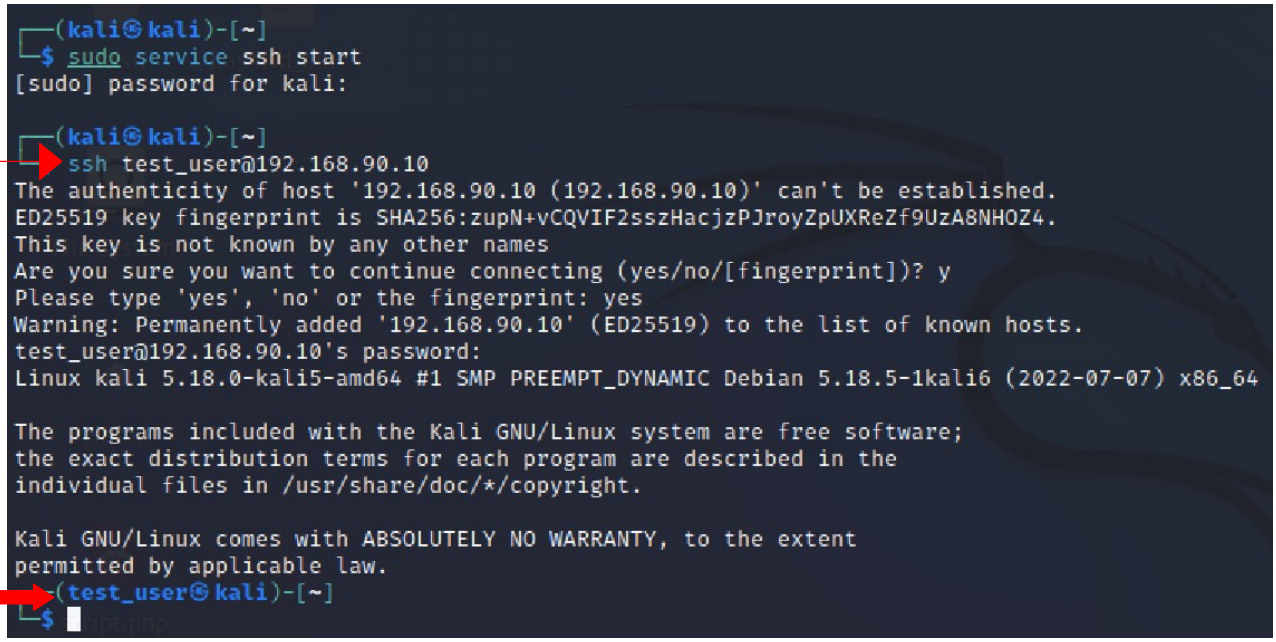
Authentication cracking con Hydra

La traccia di oggi ci chiedeva di provare il tool hydra per fare cracking delle username e delle password prima di un nuovo utente kali appena creato e successivamente della macchina meta.

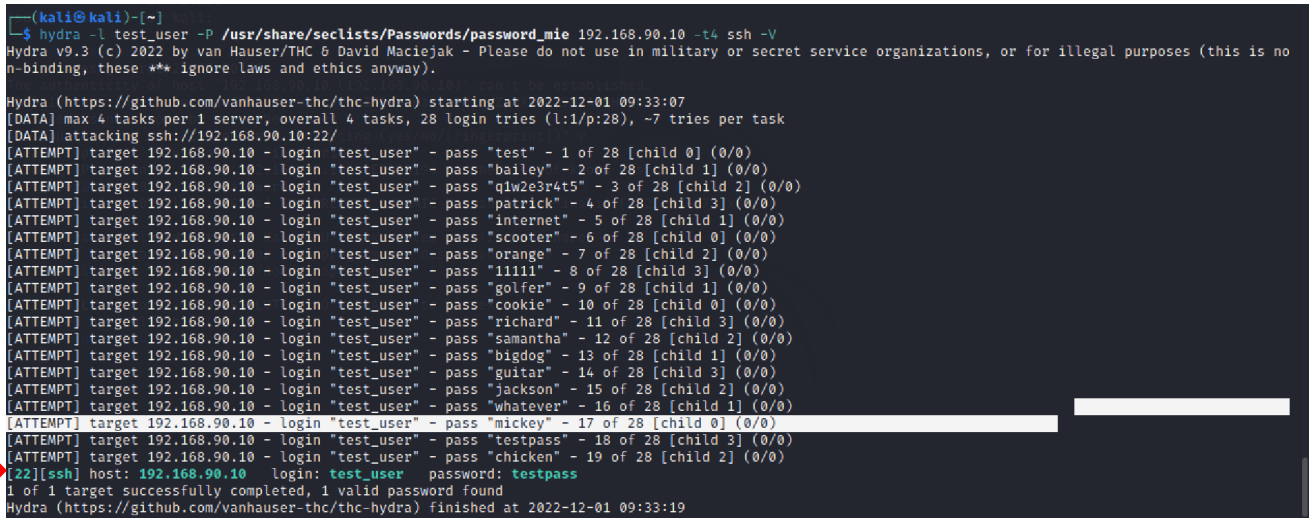
Creazione nuovo utente kali e test connessione SSH

Come prima cosa andiamo ad attivare il servizio SSH con il comando **sudo service ssh start.** Ora creiamo un altro utente su Kali con il comando **sudo adduser** rinominiamo quest' utente **test_user** gli diamo come password **testpass.** Quindi per testare che la nostra conessione SSH sia avvenuta con successo usiamo il comando **ssh test_user@(IP_kali).** Come vediamo ci appare la shell del nuovo utente questo significa che la connessione è avvenuta con sucesso.

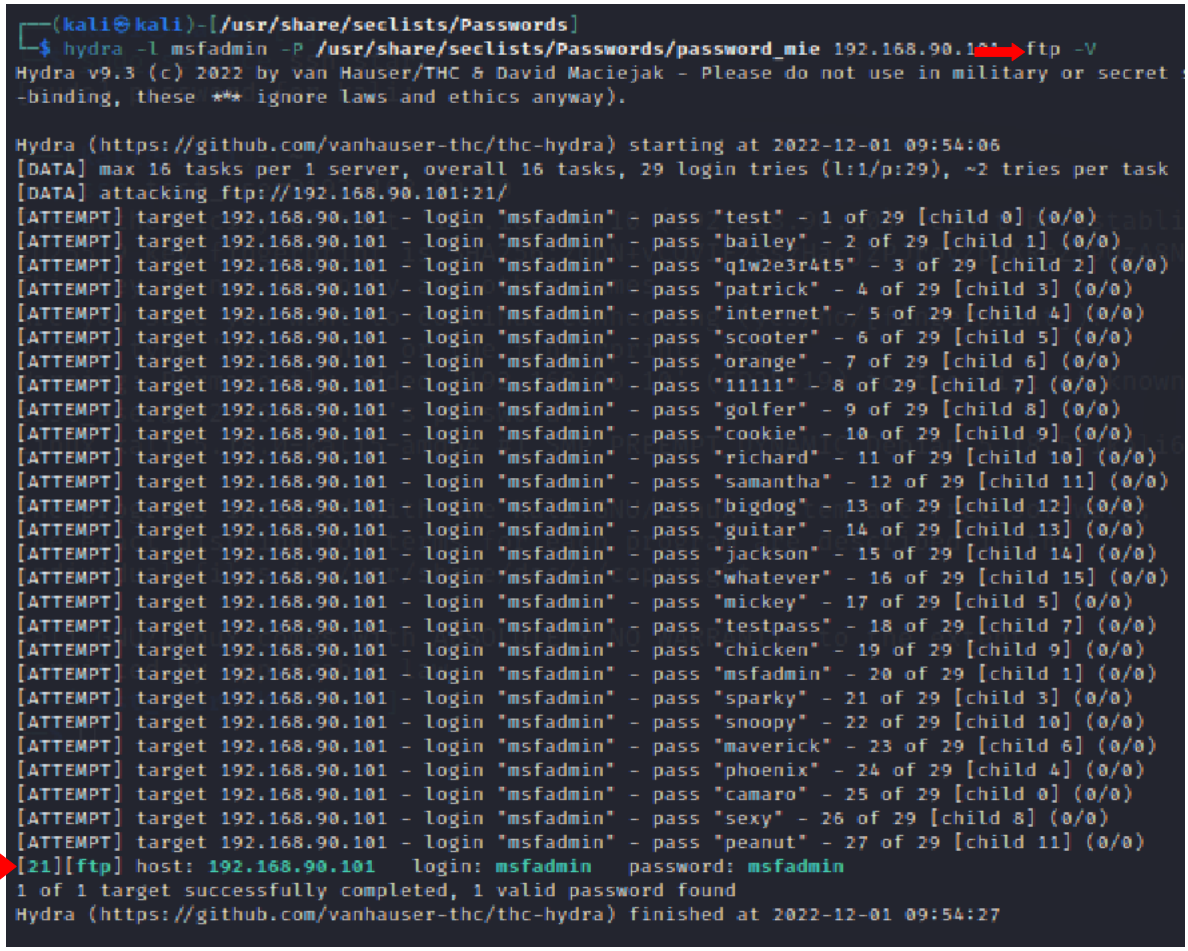


Cracking Authentication con hydra da Kali a Kali

Una volta appurato che la connessione SSH è avvenuta con sucesso passiamo Cracking Authentication con hydra in questo caso lo facciamo dal nostro utente kali verso l'utente appena creata. Il comando da lanciare è **hydra -l test_user -P /usr/share/seclists/Passwords/password_mie 192.168.90.10 -t4 ssh -V. Commentiamo il comando: -l** = userà l' username riportato di seguito; **-P** con questo comando si possono usare un elenco di password(con **-L** questo è possibile anche con gli username), la traccia ci chiedeva di usare un file scaricato precedentemente da seclists io per risparmiare tempo ne ho creato un mio più piccolo(**password_mie**); **IP** del target; **-T4 =** task che hydra compie contemporaneamente(per l' SSH va impostato -T4 di default è **-T16**);**ssh =** protocollo con cui svolgere il craking;**-V** = per controllare in live i tentativi. Come si può vedere dopo una serie di tentativi riusciremo poi ad entrare con la password e l'username.

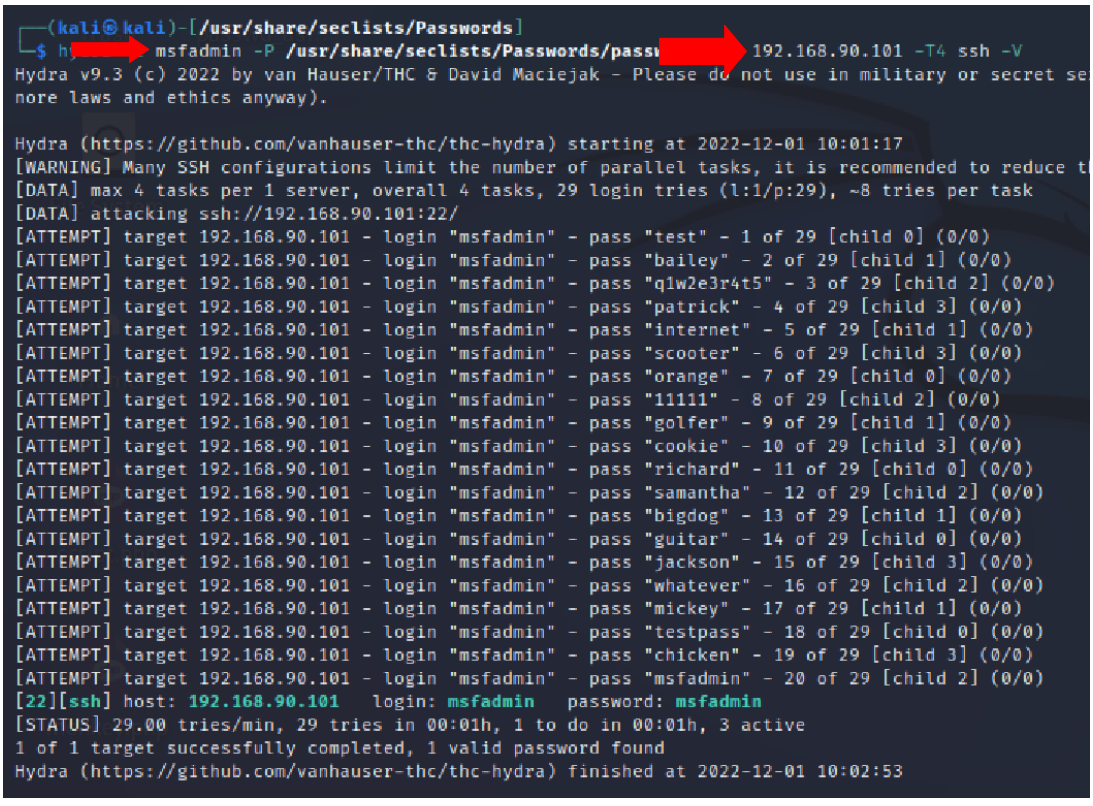


Ho poi provato il cracking con un altro protcollo(**FTP**), in questo caso il **-T** non va specificato andrà bene quello di default. Anche qui abbiamo riscontro positivo.



Cracking Authentication con hydra da Kali a Meta

La procedura per meta è praticamente la stessa ho cambiato solo l' **IP** su qui fare l' attacco e l' username(**msfadmin**).Anche qui ho avuto riscontro positivo dell' attacco.



Ho anche provato l' attacco verso meta con un altro protocollo(FTP), anche qui il risultato è stato positivo.