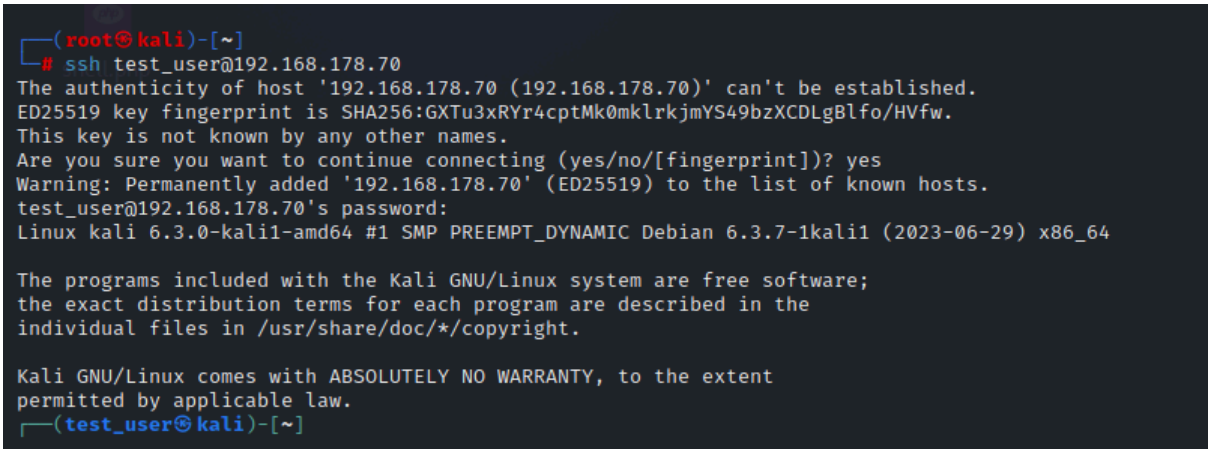
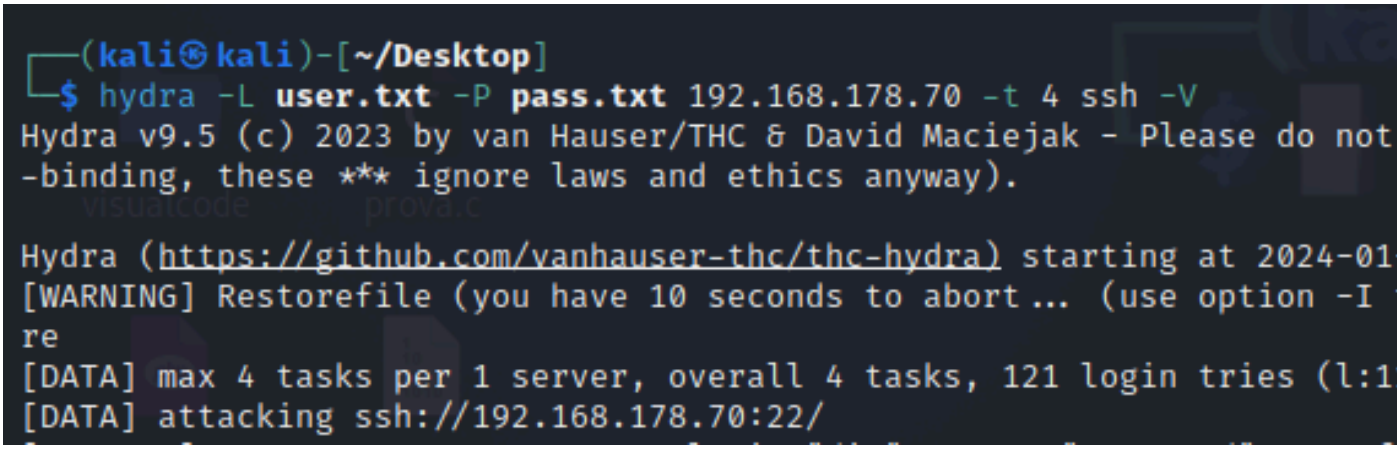
Nell'esercitazione di oggi vado a configurare un altro user sulla macchina kali, impostando come username "test_user_ e come password "testpass".

dopo aver creato lo user da attaccare attivo il servizio ssh con il comando "sudo service ssh start".
Per accedere all'altro user userò il comando "ssh test_user@192.168.178.70" quindi ssh nome utente@indirizzo_ip.
Se vogliamo modificare dei privilegi e altre opzioni dell'user lo possiamo fare sul file /etc/ssh/sshd_config.
Possiamo ora tornare all'user attaccante con lo stesso comando mostrato prima, così da poter vedere testare e quindi stabilire che c'è una connessione in SSH dell'user creato. Il comando da utilizzare è

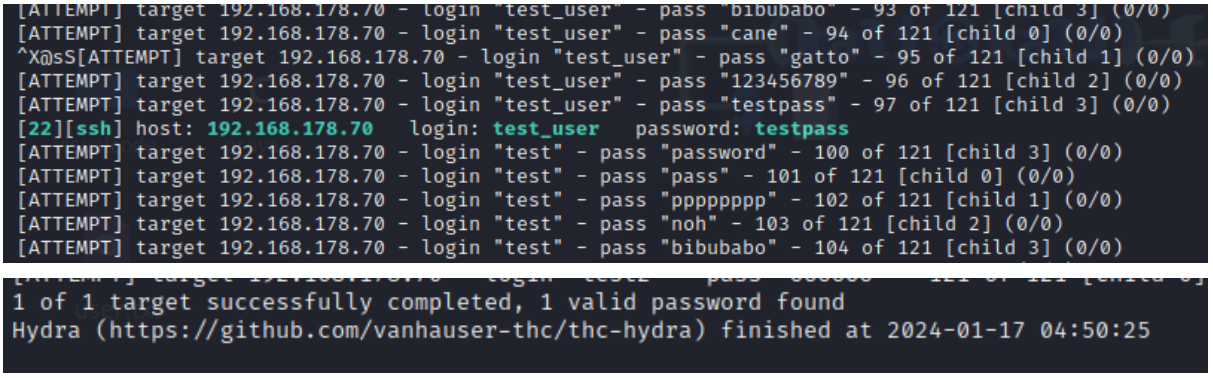


Per effettuare l'attacco bruteforce su ssh con hydra eseguirò il seguente comando, dove -L serve la lista degli username -P per la lista delle password, poi l'indirizzo ip della macchina,

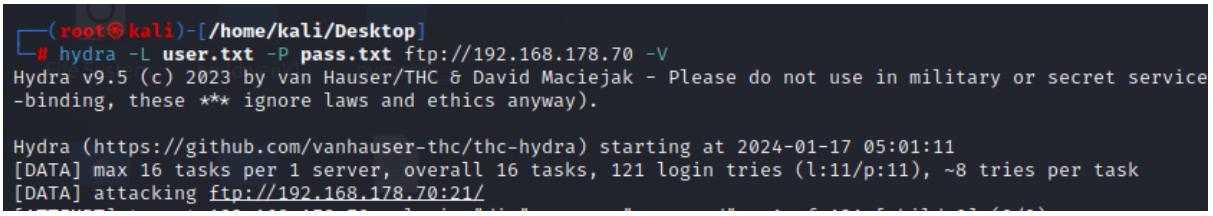
-t 4 per fare 4 task contemporaneamente, ssh è il servizio su cui stiamo facendo l'attacco e -V per mostrarci live i tentativi dell'attacco.



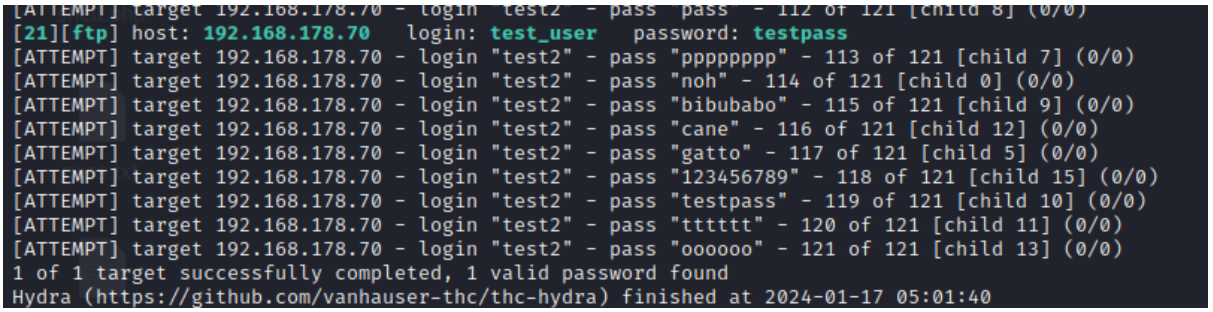
Quando avrà trovato username e password vedremo questo:



Per fare questo attacco sul servizio ftp, basta installare il servizio con il comando "sudo apt-get install vsftpd" e attivarlo con "service vsftpd start".
Quando andremo ad eseguire il comando brute force cambierà la sintassi in base al servizio che attacchiamo. In questo caso il comando è:



e il risultato sarà come quello eseguito per il servizio ssh.



da notare come nella riga dell'username e password trovate, all'inizio della stringa leggiamo tra parentesi quadre 21 per ftp e 22 per ssh che sono le porte dei servizi.