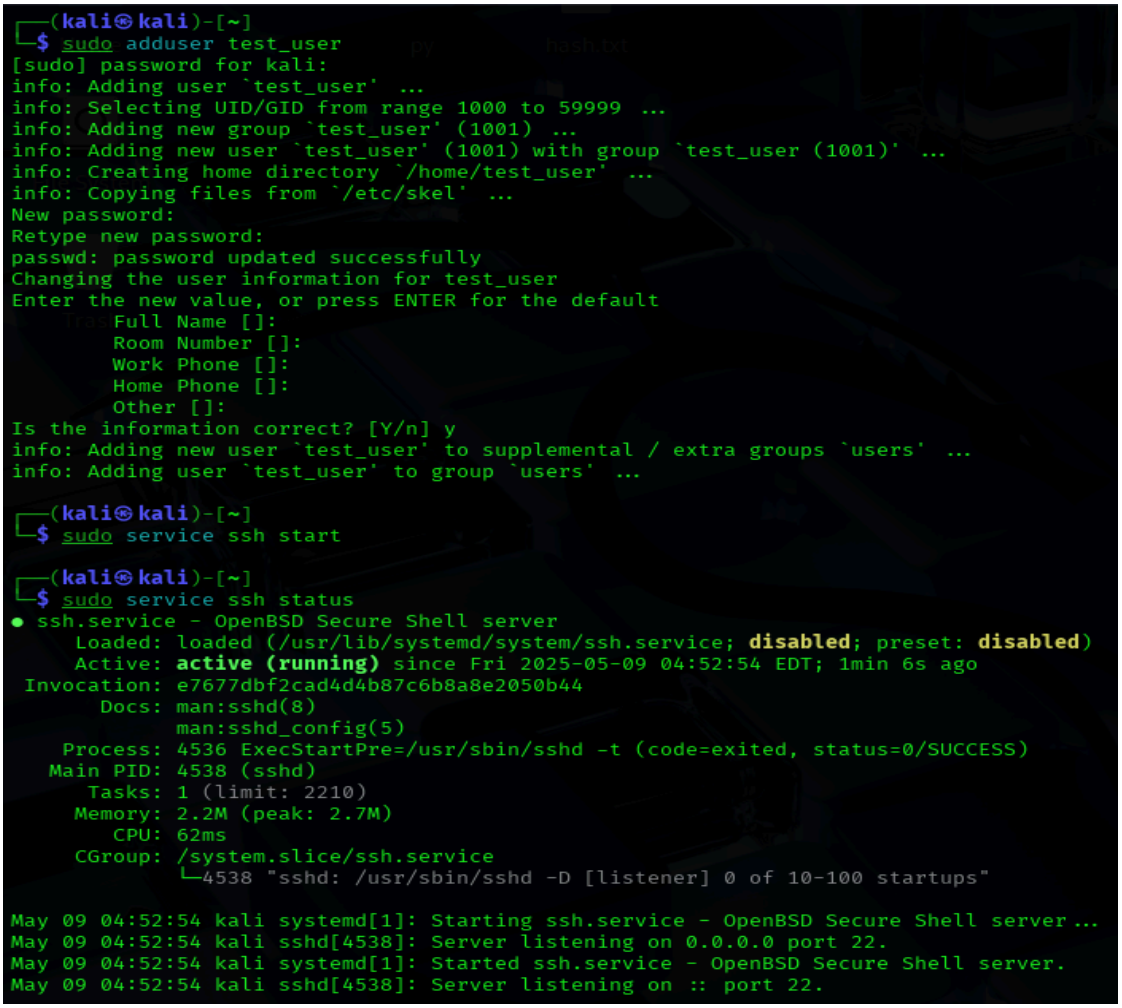
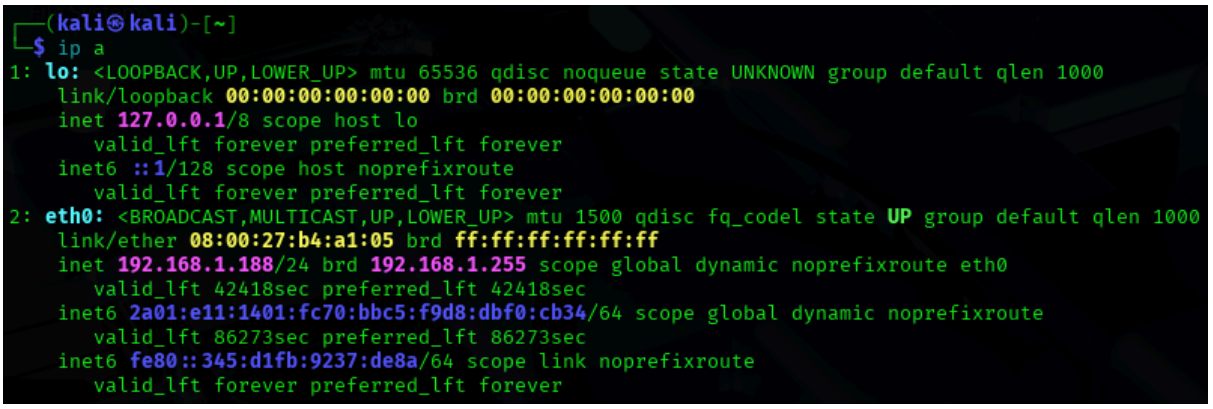
PROGETTO S6/L5: Hydra cracking

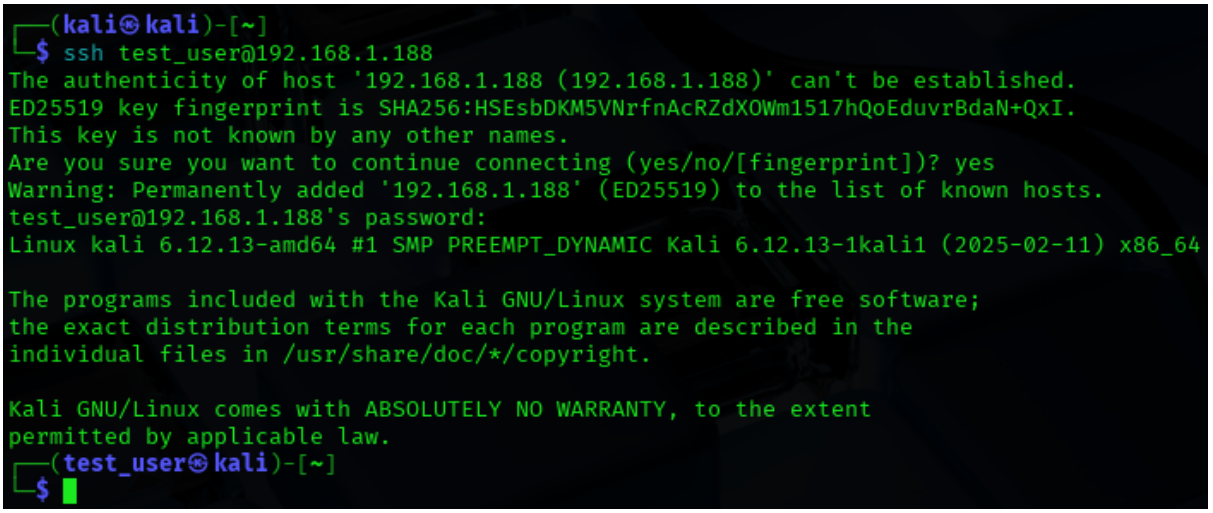
SSH



Prima di iniziare il cracking, seguendo da immagine sopra, creo un nuovo utente con il comando ***sudo adduser test_user***, seguendo poi tutte le istruzioni per completare l'utente "test_user" con la relativa password "testpass".
Ora avviamo il servizio SSH con il comando ***sudo service ssh start***. Se non appare nessun messaggio esplicito di attivazione dovrebbe essere tutto apposto, ma per verificarlo avviamo il comando ***sudo service ssh status*** dove nell'output dovremmo individuare ("active (running)").

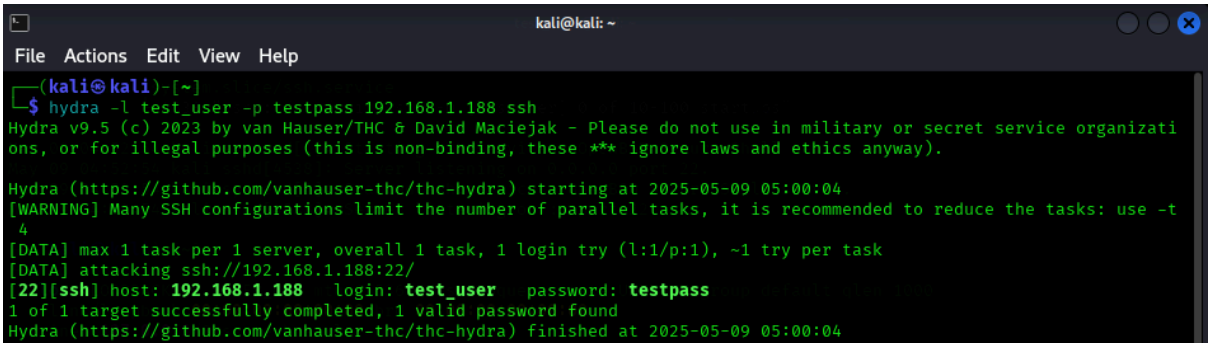
Prima di testare la connessione SSH vado a vedere l'IP della kali con ***ip a***.





Connettiamoci al server SSH usando l'utente "test_user" digitando nel terminale il comando ***ssh test_user@192.168.1.188***. Seguiamo le istruzioni e se è andato tutto bene dovremmo vedere il prompt dei comandi in ***(test_user@kali)-[~]***.

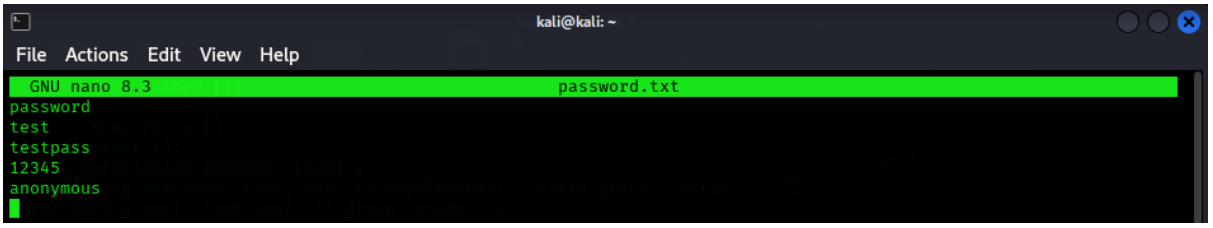
Ora utilizziamo Hydra per il cracking test dell'autenticazione SSH sapendo username e password, e per capire come funziona il comando Hydra.
Quindi nel terminale scriviamo ***hydra -l test_user -p testpass 192.168.1.188 ssh*** che dovrebbe trovare le credenziali corrette, tramite il servizio SSH porta 22.



Adesso invece utilizziamo Hydra per il cracking SSH simulando di non sapere username e password. Possiamo procedere scaricando una collezione di username e password, seclists, con il comando ***sudo apt install seclists***, che contiene elenchi di username e password piuttosto vasti, quindi ci metterà più tempo a trovarle.
Allora, a scopo dell'esercizio, per accorciare i tempi e aumentare le probabilità di successo, è possibile creare delle liste personalizzate.

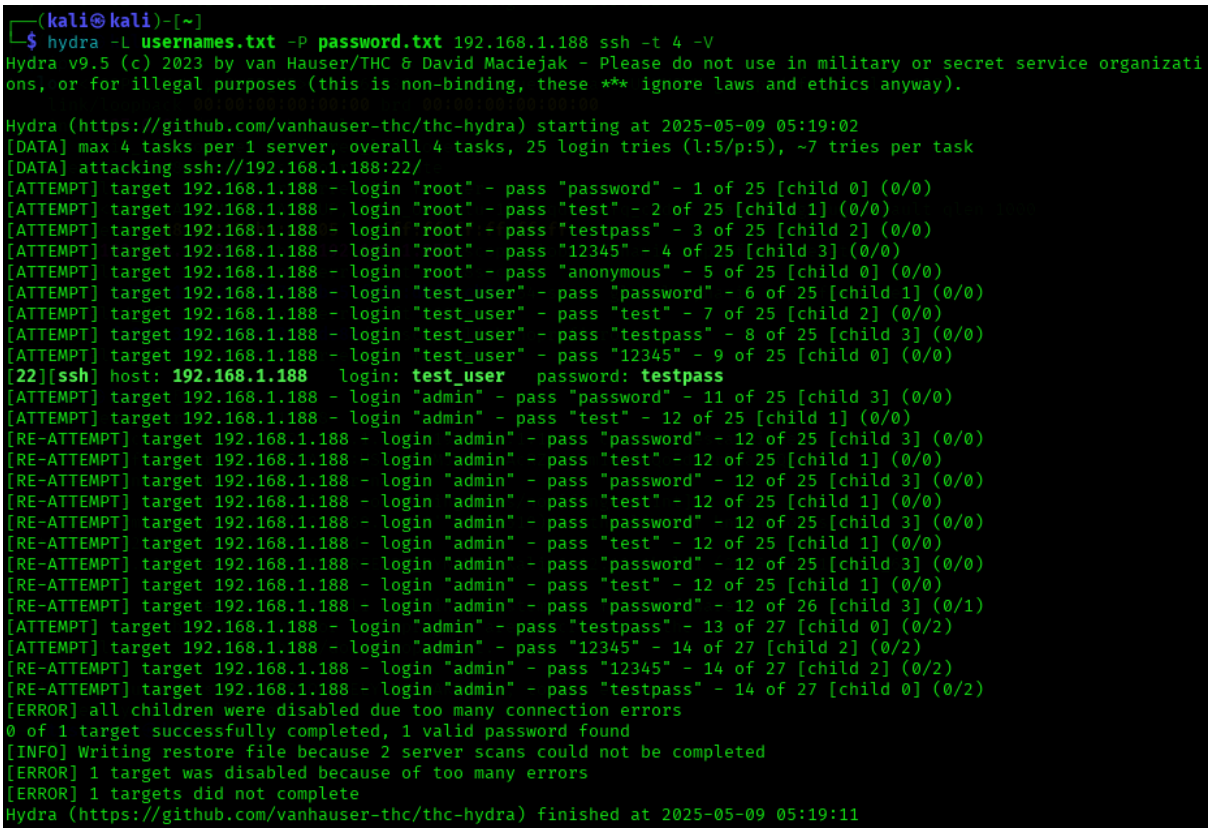
```
┌──(kali㉿kali)-[~]
└─$ nano usernames.txt

┌──(kali㉿kali)-[~]
└─$ nano password.txt
```

```
  GNU nano 8.3                          usernames.txt
root
test_user
admin
anonymous
user
```



```
  GNU nano 8.3                          password.txt
password
test
testpass
12345
anonymous
```

Eseguendo adesso il comando ***hydra -L usernames.txt -P passwords.txt 192.168.1.188 ssh -t 4 -V*** Hydra prova diverse combinazioni finchè non trova quella corretta.



```
┌──(kali㉿kali)-[~]
└─$ hydra -L usernames.txt -P password.txt 192.168.1.188 ssh -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:19:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.1.188:22/
[ATTEMPT] target 192.168.1.188 - login "root" - pass "password" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "test" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "testpass" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "12345" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "anonymous" - 5 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "password" - 6 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "test" - 7 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "testpass" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "12345" - 9 of 25 [child 0] (0/0)
[22][ssh] host: 192.168.1.188   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 26 [child 3] (0/1)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "testpass" - 13 of 27 [child 0] (0/2)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "12345" - 14 of 27 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "12345" - 14 of 27 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "testpass" - 14 of 27 [child 0] (0/2)
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:19:11
```

FTP

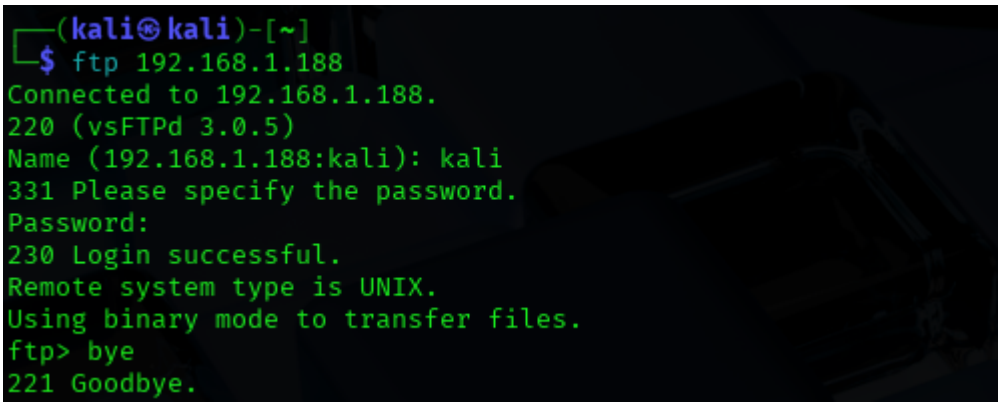
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:3 https://packages.microsoft.com/repos/code stable/main armhf Packages [19.5 kB]
Get:4 https://packages.microsoft.com/repos/code stable/main amd64 Packages [19.2 kB]
Get:5 https://packages.microsoft.com/repos/code stable/main arm64 Packages [19.4 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:7 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.0 MB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Fetched 73.5 MB in 6s (12.1 MB/s)
1218 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1218
  Download size: 143 kB
  Space needed: 352 kB / 61.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 1s (164 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 411768 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/
empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
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 (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

Per craccare l'autenticazione FTP con Hydra, installo e verifico il servizio FTP usando i comandi ***sudo apt update*** e ***sudo apt install vsftpd***.

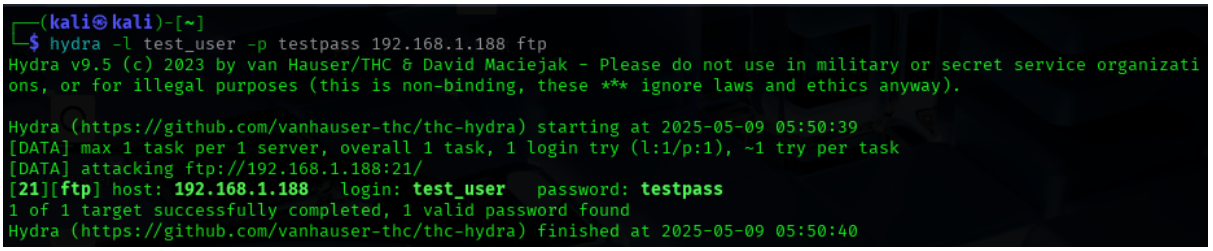
Poi avvio il servizio FTP con il comando ***sudo service vsftpd start***, se non appare nessun messaggio esplicito di attivazione il servizio è attivo ma per verificare usiamo il comando ***sudo service vsftpd status***, nel quale dovremmo vedere nell'output ("active (running)").

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

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-05-09 05:42:43 EDT; 29s ago
 Invocation: a1b2b1265b354612b3fd0da447bcf0b5
    Process: 28432 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 28433 (vsftpd)
      Tasks: 1 (limit: 2210)
     Memory: 796K (peak: 1.7M)
        CPU: 14ms
     CGroup: /system.slice/vsftpd.service
             └─28433 /usr/sbin/vsftpd /etc/vsftpd.conf

May 09 05:42:43 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
May 09 05:42:43 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

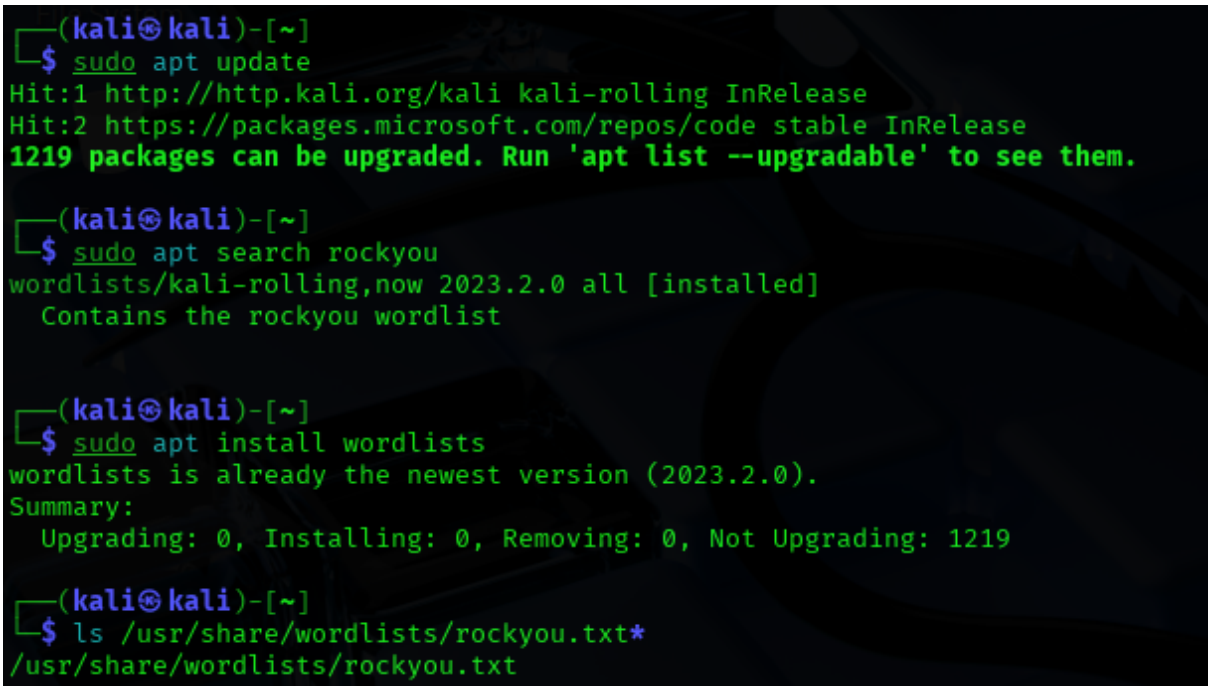
Fatto questo possiamo provare a connetterci al server FTP localmente, per verificare che il server FTP risponda sulla macchina locale. Quindi nel terminale inviamo il comando ***ftp 192.168.1.188*** facendo login con le credenziali dell'utente "kali".



Riusciti ad accedere al server FTP con le credenziali dell'utente "kali" usiamo Hydra per craccare l'autenticazione FTP usando il comando ***hydra -l test_user -p testpass 192.168.1.188 ftp*** che ci mostrerà le credenziali dell'utente "test_user" tramite il servizio FTP alla porta 21.



Adesso provo a craccare l'autenticazione FTP sempre con Hydra ma usando la wordlist "rockyou.txt", quindi seguo i passaggi come sotto in figura.



Infine provo usando il comando ***hydra -l testftp -P /usr/share/wordlists/rockyou.txt 127.0.0.1 ftp -v*** che mi darà come output: