Progetto S6L5 – Authentication cracking con Hydra

INTRODUZIONE

L'esercizio di oggi ha un duplice scopo:
● Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.
L'esercizio si svilupperà in due fasi:

Esercizio:

● Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
● Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione http

PREFAZIONE

La prima parte si vedrà la **Macchina Virtuale Kali Linux ip 192.168.2.100** sulla quale sarà creato un nuovo utente**, test_user**, con password "**testpass**".
Sarà avviato **SSH e** verificata la sua configurazione.
Sarà testata la connessione ssh dell'utente creato, e sarà configurato Hydra per la sessione di cracking.
Tramite l'installazione di **SECLISTS** scaricheremo una collezione di username e password e utilizzeremo **Hydra** per recuperare quelle giuste.

La seconda parte sarà dedicata alla scelta del servizio da configurare, sarà scelto il protocollo ftp, e all'ottenimento dell'autenticazione con **HYDRA**

1. ESECUZIONE: Parte prima

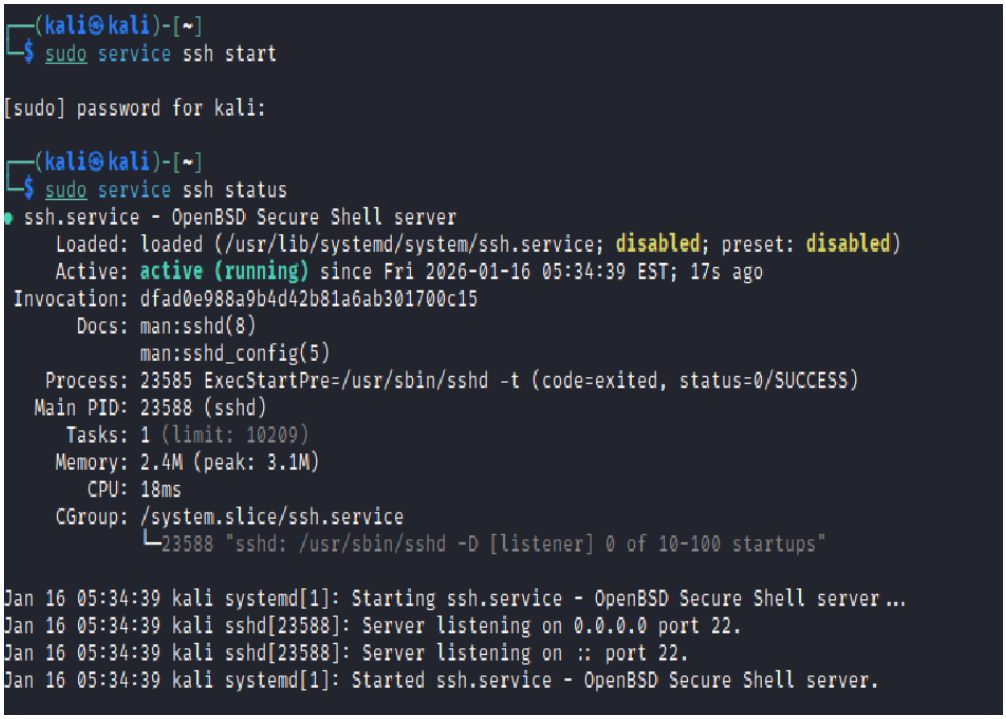
Creazione nuovo utente sulla **Macchina Virtuale Kali Linux**:

Da terminale Kali Linux, attraverso il **Terminale** con il comando:
sudo adduser test_user viene creato il nuovo utente, con password **testpass.**

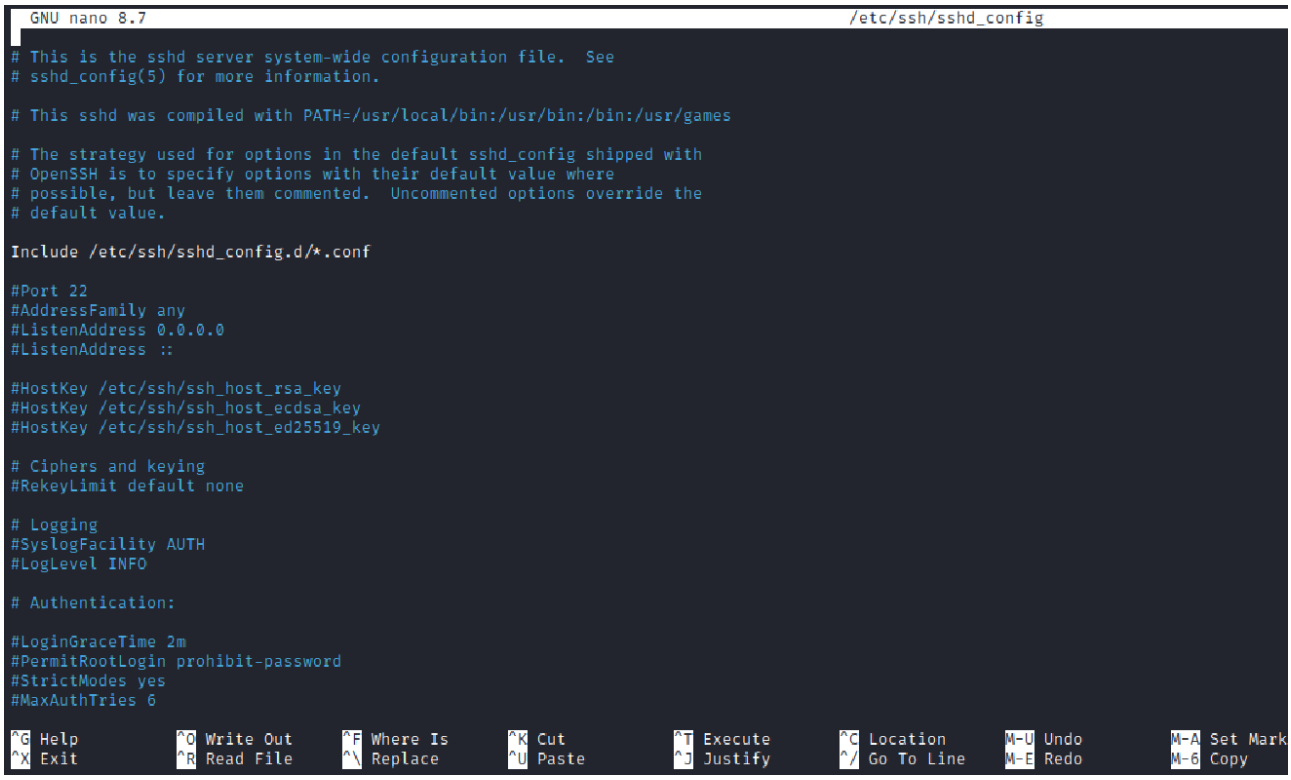
```
┌──(test_user㉿kali)-[~]
└─$ exit
logout
Connection to 192.168.2.100 closed.
```

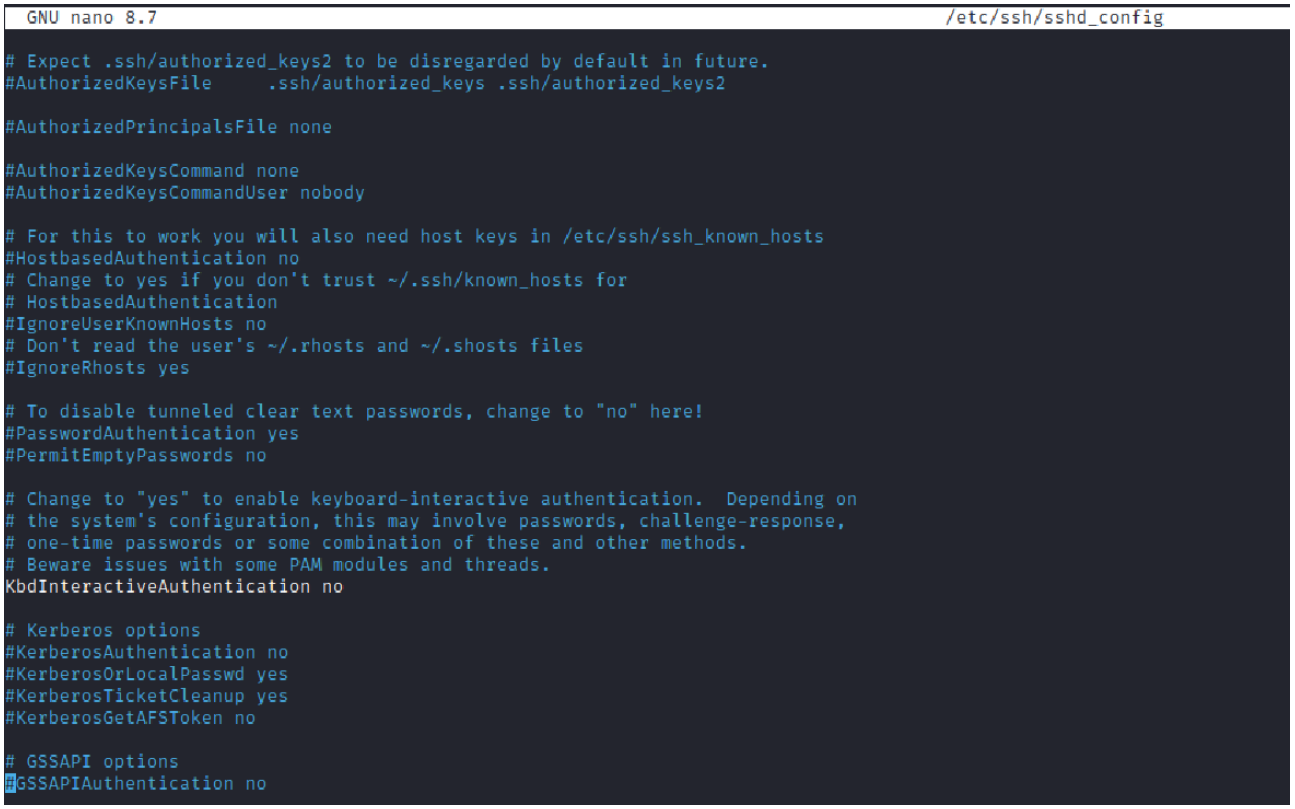
Avvio del SSH e verifica della sua configurazione:

attraverso il comando da Terminale **sudo ssh service start** attivo il servizio ssh, e controllo con **sudo service ssh status** che si attivo

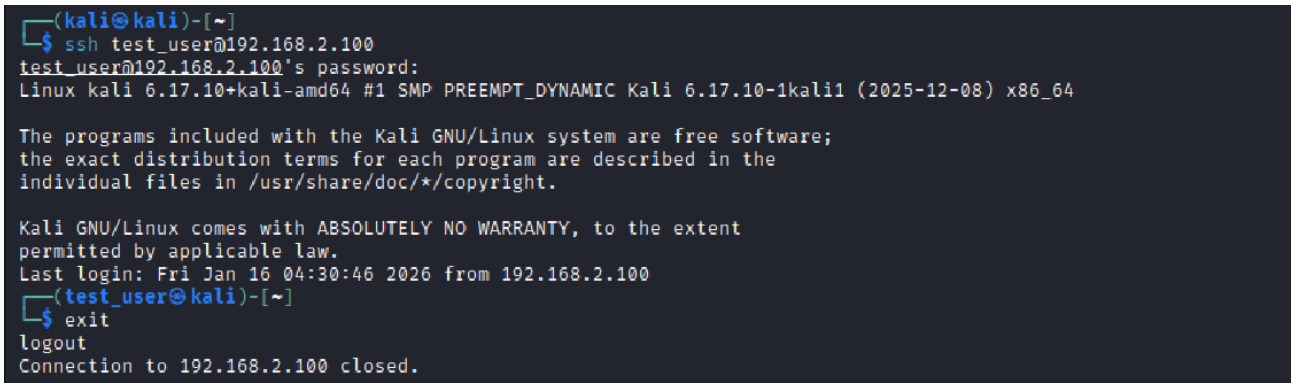


seguendo il path /**etc/ssh/sshd_config**, con il comando **sudo nano /etc/ssh/sshd_config** visualizzo il contenuto del file senza apportare alcuna modifica





Manualmente procedo con ssh test_user@192.168.2.100

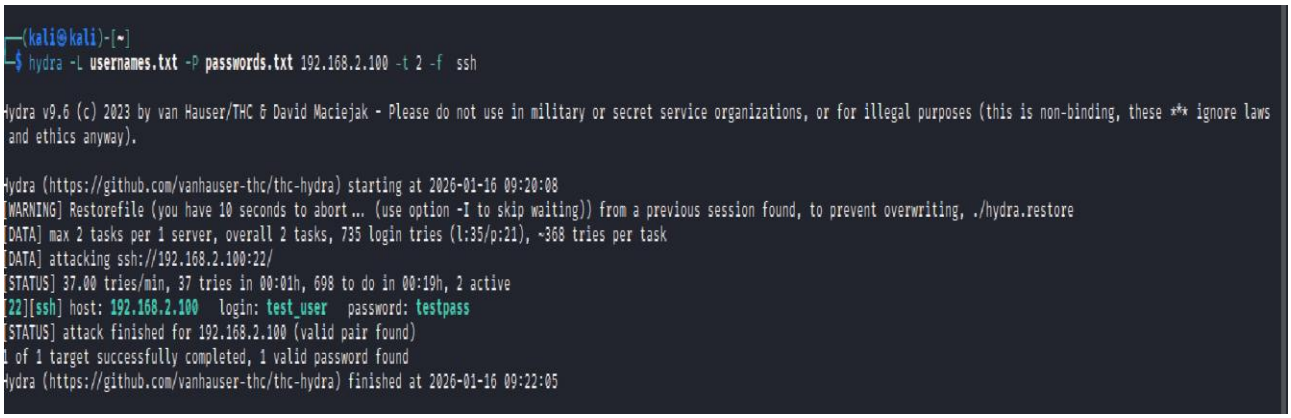


Inserisco lo username **test_user e testpass** all'interno della cartella xato-usernames.txt, li inserisco sui file usernames.txt e passwords.txt e riduco il numero della lista a 20, nella quale all'interno ci sono rispettivamente test_user e testpass.
Normalmente non andrebbe fatto ma il numero delle liste è alto e si necessita di ridurre i tempi di esecuzione.

Avvio Hydra:
hydra -L usernames.txt -P passwords.txt 192.168.2.100 -t 2 ssh trovando le credenziali.

-L usernames.txt si riferisce alla lista di nomi utenti contenute in username.txt
-**P passwords.txt** si riferisce alla lista di passwords
192.168.2.100 è il target

-t2 sono i tentativi che dovrà fare **hydra**
-f finisce la ricerca una volta trovati i risultati giusti



Nell'immagine viene esposto il risultato: **22 ssh host:192.168.2.100 login: test_user password: testpass**

2. Esecuzione: parte seconda

Similmente da quanto fatto prima **installo vsftpd** dal **Terminale Kali Linux** con: **sudo apt install vsftpd**

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
vsftpd is already the newest version (3.0.5-0.4).
The following packages were automatically installed and are no longer required:
  curlftpfs     libavformat61          libfuse2t64    libpocketsphinx3  libradare2-5.0.0t64  libsphinxbase3t64  libvdpau-va-gl1              pocketsphinx-en-us
  libavfilter10  libconfig-inifiles-perl  libgpgme11t64  libpostproc58     libsimdutf27         libswscale8        linux-image-6.12.38+kali-amd64  python3-xlrd
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 358
```

Lo avvio sempre da Terminale:
sudo service vsftpd start

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

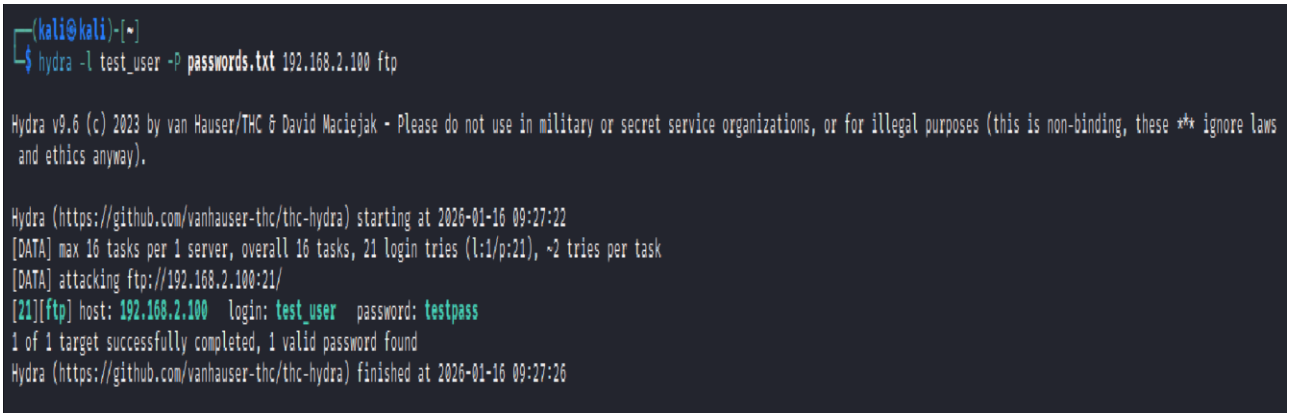
Controllo se sia attivo:
sudo service vsftpd status

```
┌──(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 2026-01-16 09:24:45 EST; 13s ago
 Invocation: ad52c0dbd5a6494aa30b122d220e79bf
    Process: 71542 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 71543 (vsftpd)
      Tasks: 1 (limit: 10209)
     Memory: 948K (peak: 2.2M)
        CPU: 11ms
     CGroup: /system.slice/vsftpd.service
             └─71543 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 16 09:24:45 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 16 09:24:45 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

Lo connetto con l'ip **192.168.2.100** e chiudo:

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.2.100
Connected to 192.168.2.100.
220 (vsFTPd 3.0.5)
Name (192.168.2.100:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
```

Utilizzo **HYDRA** per ricavare le credenziali:
hydra -l test_user -P passwords.txt 192.168.2.100 ftp



Nell'immagine viene rappresentato il risultato:
21 ftp host:192.168.2.100 login: test_user password: testpass