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.

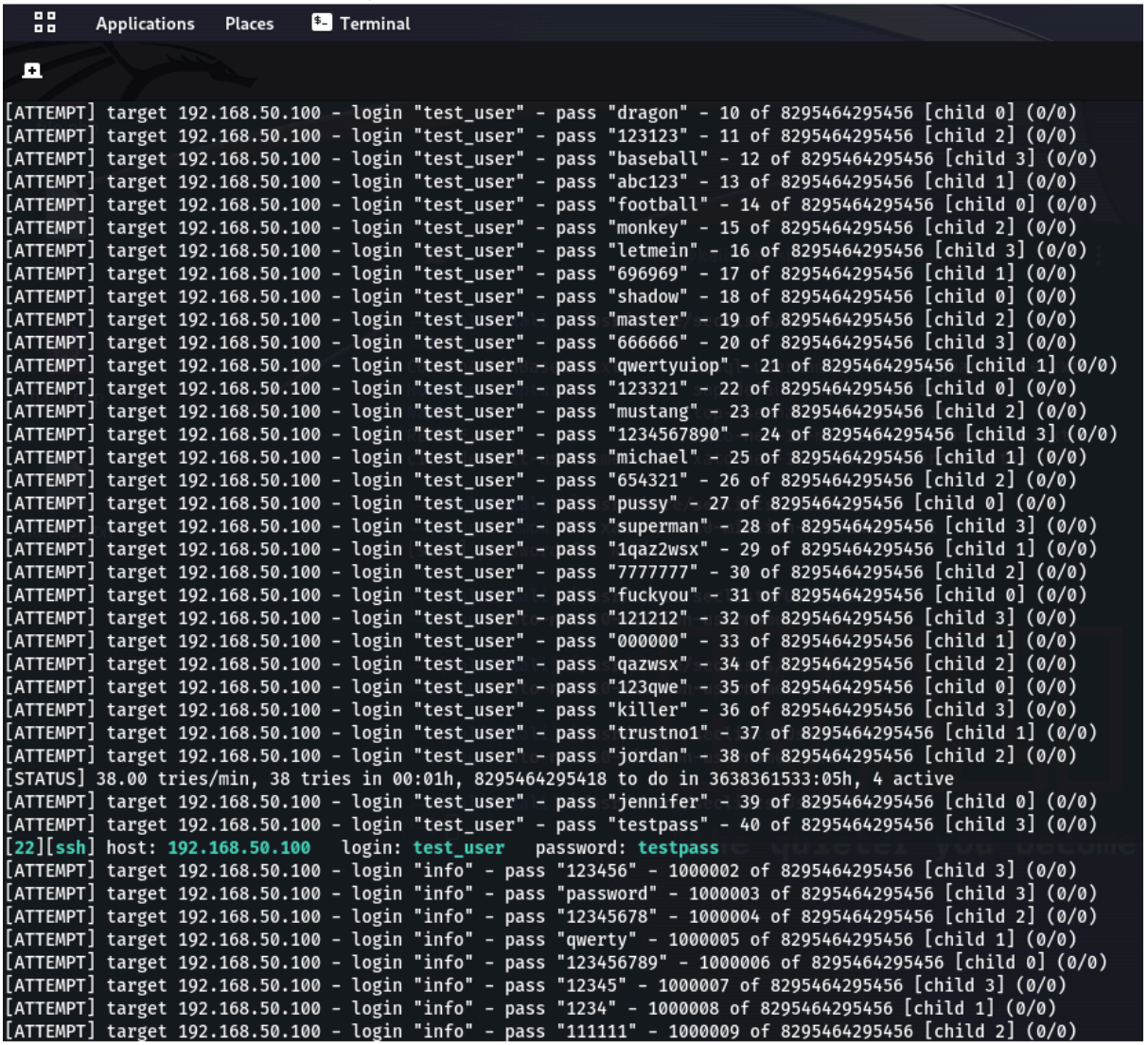
Ovviamente abbiamo scaricato i dizionari da utilizzare sia per trovare il nome utente sia per trovare la password.
Fra i vari dizionari troviamo quelli utili agli attacchi brute force su reti Wi-Fi, e molti altri dizionari, ognuno utile ad un suo scopo.
Per i nostri scopi abbiamo bisogno di altri tipi 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
```

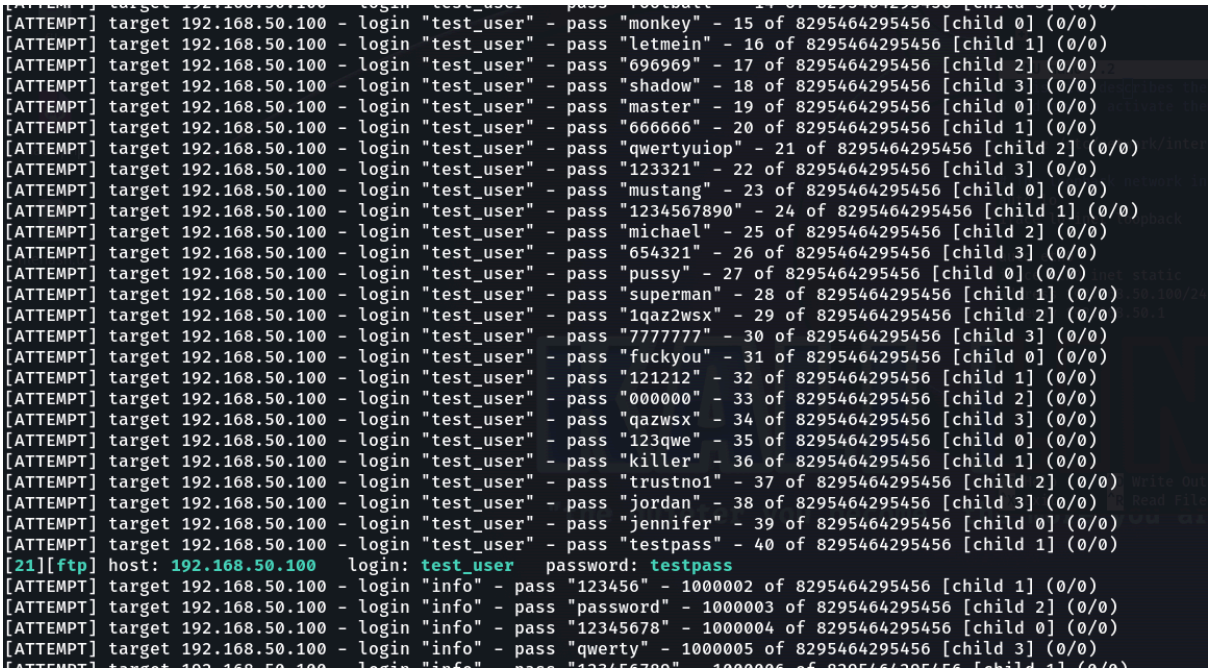


Il secondo punto/obiettivo della traccia è eseguire lo stesso attacco brute force a dizionario, ma questa volta utilizzeremo il protocollo FTP.

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

Questo è il codice che utilizzeremo:

**hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt \ -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt **
-V 192.168.50.100 -t4 ftp



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