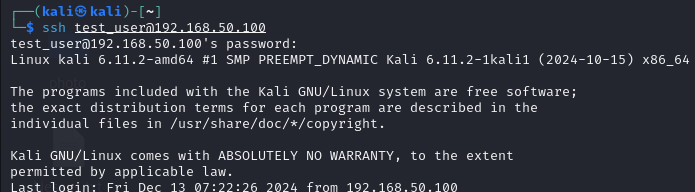
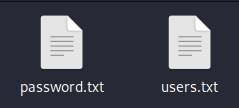
Brute forcing sevizi ssh e ftp

Per prima cosa ho creato un user di prova chiamato test\_user:



E ho impostato la password come: testpass

Il prossimo step sarebbe quello di lanciare hydra con le liste di test e password che le slide ci hanno proposto. Questo procedimento però richiederebbe tempistiche estese, quindi al fine del test ho personalmente creato una lista di user e di password personalizzata, prestando attenzione a inserire test\_user negli User e testpass nelle password.

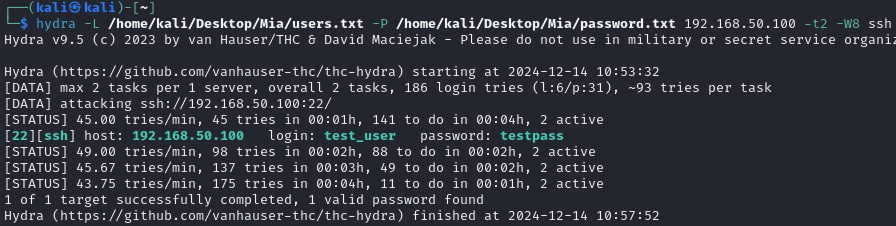
Fatto questo, ho tentato di lanciare hydra con

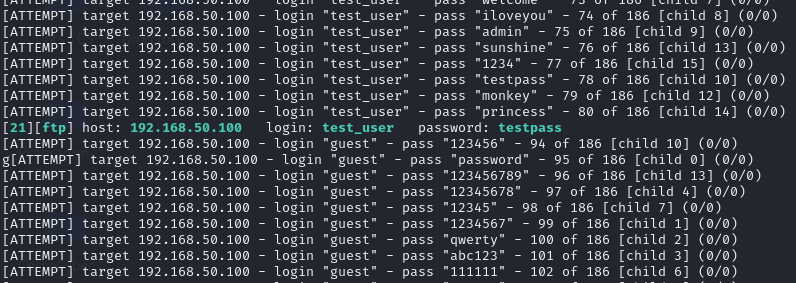
Il comando:

Il comando è così composto

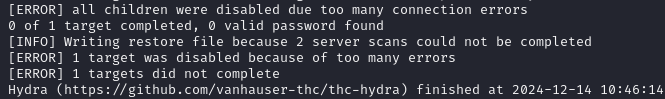
* Hydra: richiama il programma Hydra
* -L: starebbe per “login” dice a hydra di utilizzare il file che indicheremo nella directory a seguire come nomi per possibili users. La L maiuscola indica di reiterare i tentativi per ogni username in users.txt
* /home/kali/Desktop/Mia/users.txt: Directory del file users.txt
* -P: starebbe per “password”, dice a hydra di utilizzare i file che indicheremo nella directory a seguire come password. La P maiuscola indica di reiterare i tentativi per ogni password presente in password.txt
* /home/kali/Desktop/Mia/users.txt: Directory del file password.txt
* 192.168.50.100: IP della mia macchina Kali
* -t16: numero di Threads per indicare quanti tentativi eseguire contemporaneamente, un numero più alto aumenta il rischio di essere bloccati
* -W3: indica quanti secondi aspettare, diminuisce il rischi di essere bloccati
* Ssh: servizio da attaccare
* -V: modalità verbosa, printa in chiaro ogni tentativo

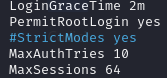
Hydra comincia a fare i sui tentativi e dopo poco tempo notiamo questo:

Ciò ci indica che hydra ha trovato un positivo: username – test\_user e password – testpass. Sappiamo essere corretto

Eseguiamo ora lo stesso comando, ma specificando di voler attaccare il servizio ftp, poco dopo abbiamo un risultato simile:

Abbiamo testato le potenzialità di hydra con successo.

C’è da specificare che lanciando il primo comando, ssh dopo poco tempo ci impedisce di proseguire, terminando il nostro tentativo. Per evitare questo ho provato varie cose, la principale e più ovvia sarebbe abbassare il numero di Threads e alzare quello di Wait, come -t3 e -W10. Ho comunque deciso di controllare se potessi trovare il modo di lanciare hydra con un alto numero di threads, che ci avrebbe permesso di utilizzare pools di passwords e users più grandi, similmente a come accadrebbe in un real-life-scenario.

Attraverso le mie ricerche ho capito di dover modificare il config di ssh per fare questo tentativo, l’ho dunque così editato:

-Sono andato dunque a aumentare il login grace time, i tentativi di autenticazione, le sessioni contemporanee permesse e i numeri di startups.

Purtroppo, nessuna di queste modifiche ha aiutato in maniera significativa hydra, motivo per cui il comando che alla fine ha avuto successo utilizza 2 threads e un wait a 8 secondi.