ESERCIZIO W14D4

L’esercizio di oggi ha un duplice scopo:

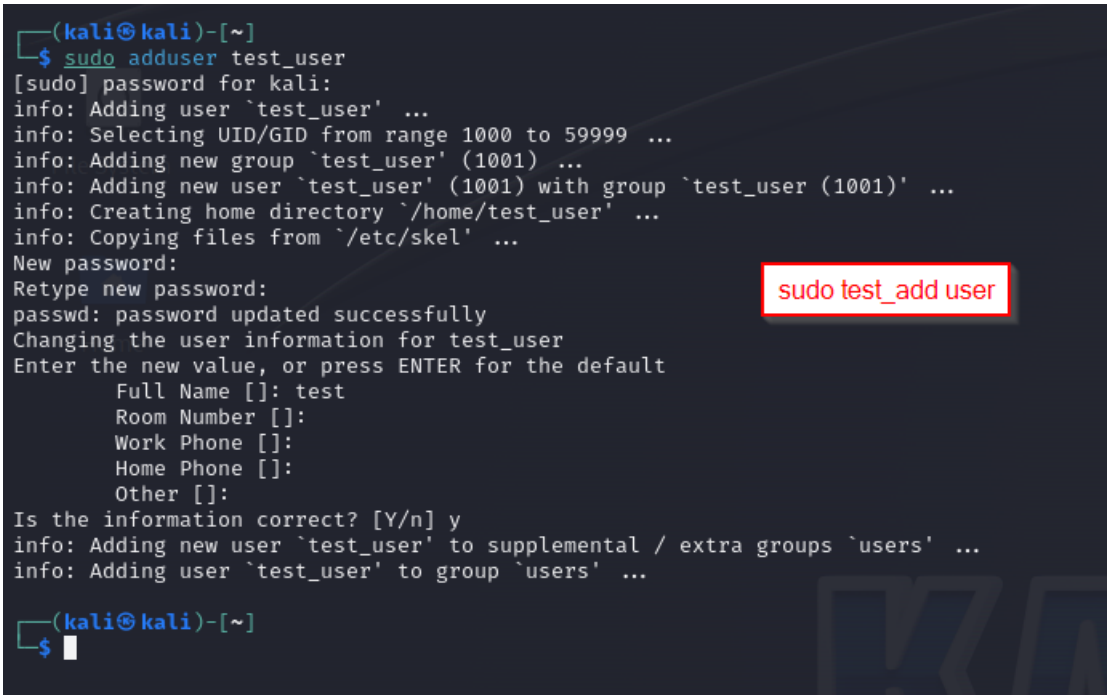
- Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

L’esercizio si svilupperà in due fasi:

- Una prima fase dove si vedrà l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Creazione Test_user

Per cominciare creiamo un user al quale assegniamo una password.

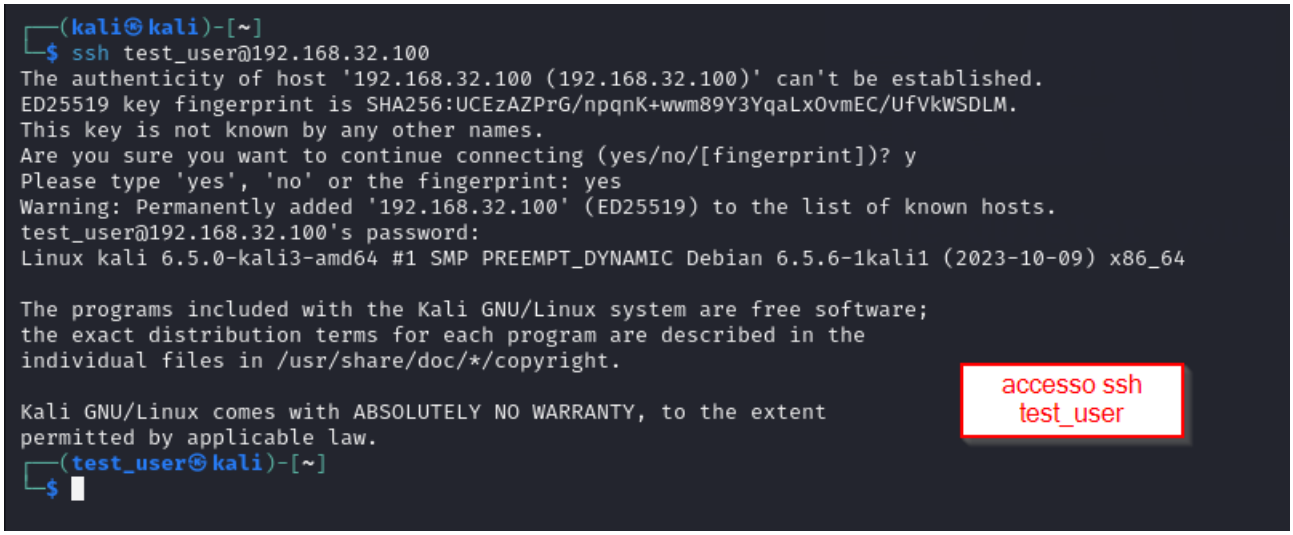


Controllo configurazioni

Controlliamo i settaggi inseriti nelle configurazioni. Possiamo cambiare porta, indirizzo e altre modalità.

Attivazione servizio e testing ssh

Come da titolo, dopo aver avviato il servizio ssh con *sudo service ssh start,* proviamo ad accedere all'utente test_user con le credenziali inserite prima.




```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.32.100
The authenticity of host '192.168.32.100 (192.168.32.100)' can't be established.
ED25519 key fingerprint is SHA256:UCEzAZPrG/npqnK+wwm89Y3YqaLxOvmEC/UfVkWSDLM.
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 '192.168.32.100' (ED25519) to the list of known hosts.
test_user@192.168.32.100's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
└─$
```

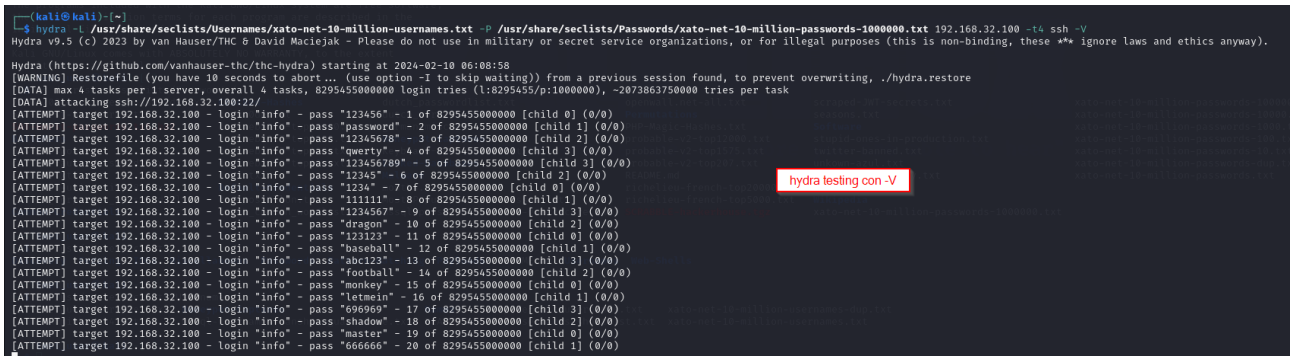
Seclist installate

Nel caso vogliamo andare a testare password e username multiple, possiamo installare le seclists. Qui sotto mostro la presenza di quest'ultime nella macchina.


```
┌──(test_user㉿kali)-[~]
└─$ ls /usr/share/seclists/Passwords/
2020-200_most_used_passwords.txt  Cracked-Hashes             dutch_passwordlist.txt                 openwall.net-all.txt          scraped-JWT-secrets.txt                xato-net-10-million-passwords-100000.txt
500-worst-passwords.txt           darkc0de.txt               dutch_wordlist                         Permutations                  seasons.txt                            xato-net-10-million-passwords-10000.txt
500-worst-passwords.txt.bz2       darkweb2017-top10000.txt   german_misc.txt                        PHP-Magic-Hashes.txt          Software                               xato-net-10-million-passwords-1000.txt
BiblePass                         darkweb2017-top1000.txt    Honeypot-Captures                      probable-v2-top12000.txt      stupid-ones-in-production.txt          xato-net-10-million-passwords-100.txt
bt4-password.txt                  darkweb2017-top100.txt     Keyboard-Combinations.txt              probable-v2-top1575.txt       twitter-banned.txt                     xato-net-10-million-passwords-10.txt
cirt-default-passwords.txt        darkweb2017-top10.txt      Leaked-Databases                       probable-v2-top207.txt        unkown-azul.txt                        xato-net-10-million-passwords-dup.txt
citrix.txt                        days.txt                   Malware                                README.md                     UserPassCombo-Jay.txt                  xato-net-10-million-passwords.txt
clarkson-university-82.txt        Default-Credentials        months.txt                             richelieu-french-top20000.txt WiFi-WPA
common_corporate_passwords.lst    der-postillon.txt          Most-Popular-Letter-Passes.txt         richelieu-french-top5000.txt  Wikipedia
Common-Credentials                dutch_common_wordlist.txt  mssql-passwords-nansh0u-guardicore.txt SCRABBLE-hackerhouse.tgz      xato-net-10-million-passwords-1000000.txt
```

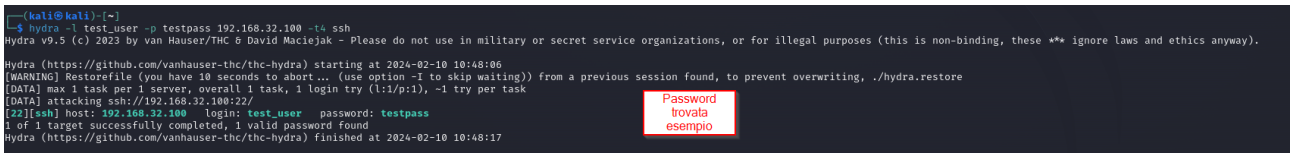
Testing 10 millions

Per testare le liste inseriamo il loro percorso ed mettiamo i flag maiuscoli. Hydra controllerà gli username e le password fino a che non segnerà di verde un match, per confermare il successo della combinazione.



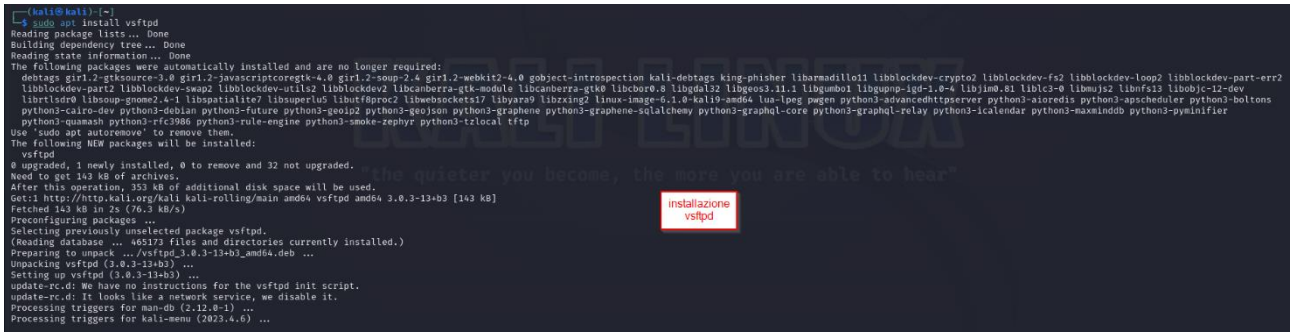
Testing singolo

Se invece vogliamo trovare una password o degli username specifici, lasciamo le lettere minuscole e indichiamo le credenziali.



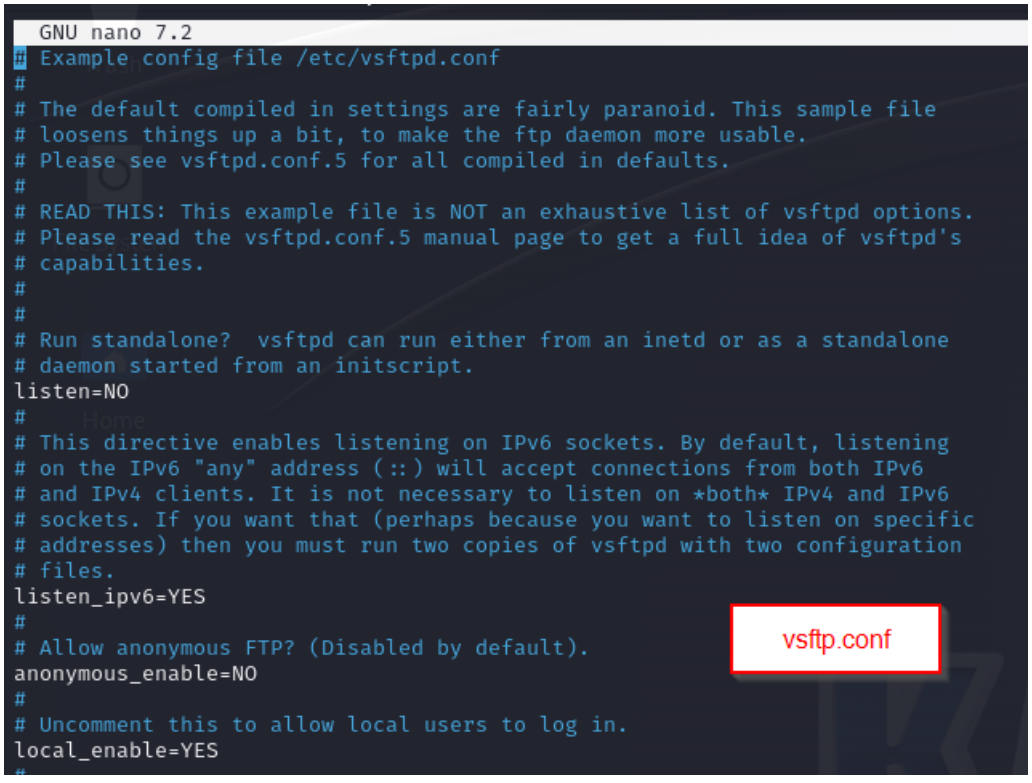
Installazione servizio vsftpd

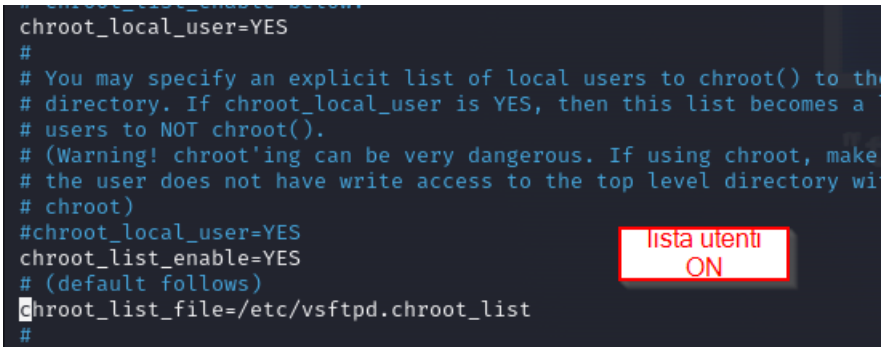
L'ultima parte della consegna prevede il cracking di un servizio ftp. Installo dunque i pacchetti sulla macchina.

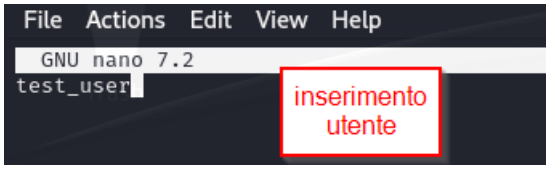


Configurazione servizio vsftpd

Prima di procedere oltre, togliamo le spunte da ciò che ciò che ci interessa. Permettiamo i diritti di scrittura agli gli utenti ftp, inoltre attiviamo la funzione che permette di racchiudere gli utenti dentro un file, che chiameremo vsftpd.chroot_list.







Testing ftp password

Per fare prima, indichiamo come sempre l'utente test_user e la password.