AUTHENTICATION CRACKING
ESERCITAZIONE W14D4

INTRODUZIONE

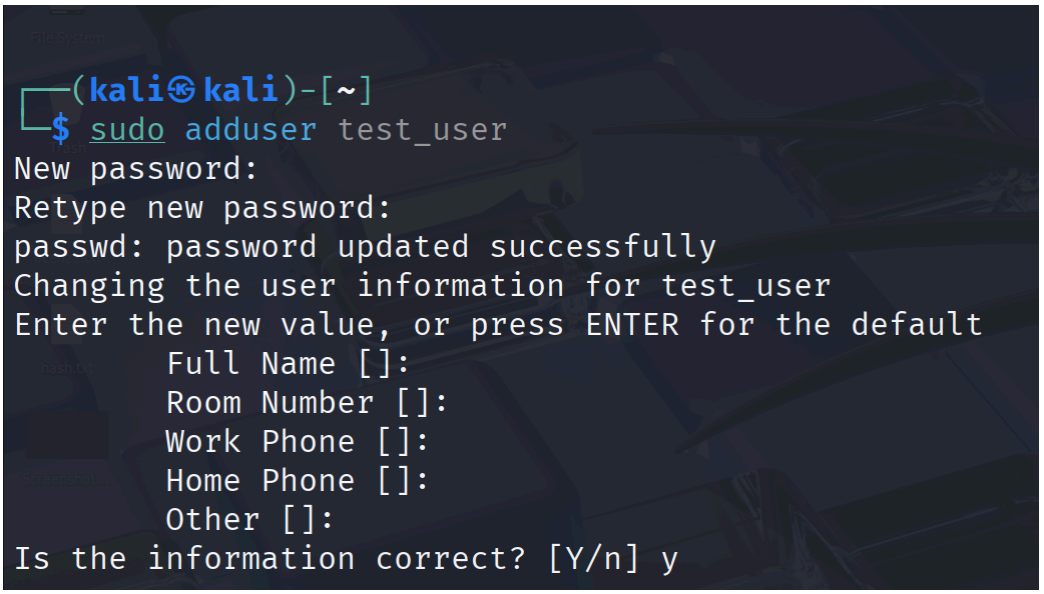
- L'obiettivo dell'esercitazione è creare un semplice ambiente di test (utente, servizi SSH/FTP) e mostrare come Hydra possa usare wordlist per provare combinazioni utente/password fino a individuare credenziali valide

PREPARAZIONE DELL'AMBIENTE E TEST ACCESSO SSH

- Per la creazione di un account di prova andiamo a utilizzare il comando

sudo adduser test_user

- Come secondo punto andiamo a inserire una password in questo caso useremo **testpass**



una volta configurato l'account possiamo abilitare il demone SSH:

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

- Prima di procedere andiamo a verificare che il servizio risponda andando a effettuare un login di prova, utilizzando il seguente comando

ssh test_user@192.168.50.100

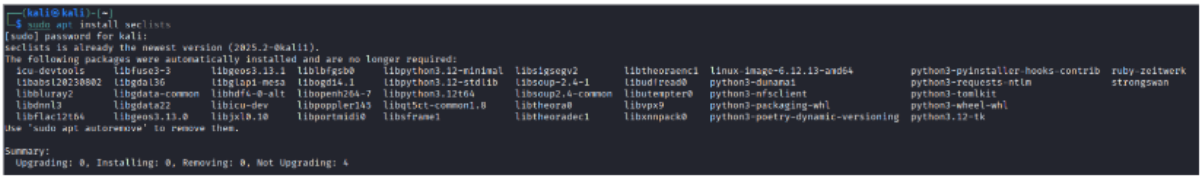
```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

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.
```

Questa fase serve a confermare che l'utente esiste e che SSH è correttamente in ascolto sull'IP indicato.

PREPARAZIONE DELLA WORDLIST

- Hydra richiede liste di nomi utente e password da provare per questo andiamo a scaricare una ***seclists*** con il comando

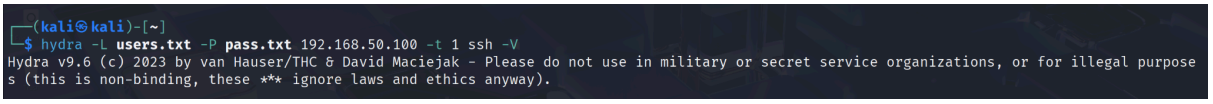
sudo apt install seclists



ESECUZIONE DELL'ATTACCO

Per lanciare l'attacco andiamo a utilizzare il seguente comando

hydra -L users.txt -P pass.txt 192.168.50.100 -t 1 ssh -V



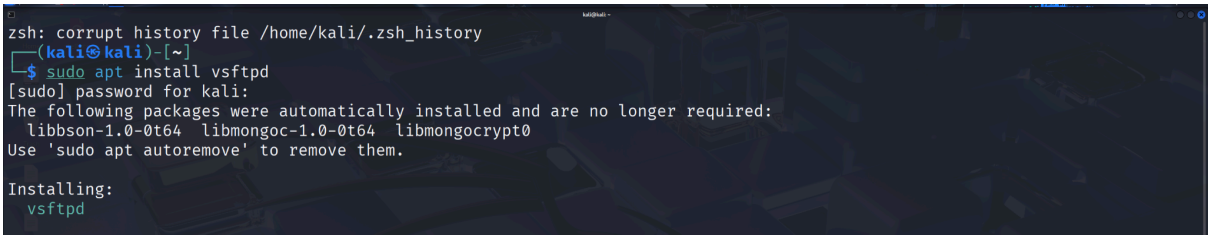
Spiegazione tecnica del comando:

- ***-L users.txt*** → file con gli username da provare.
- ***-P pass.txt*** → file con le password.
- ***192.168.50.100*** → indirizzo del target.
- ***-t 1*** → numero di thread concorrenti.
- ***ssh*** → modulo da attaccare.
- ***-V*** → output verboso per tracciare i tentativi.

INSTALLAZIONE E AVVIO DEL SERVIZIO FTP

Per ripetere l'esercizio su FTP si installa un server leggero e sicuro come **`vsftpd`** con il comando

sudo apt install vsftpd



per lanciare il servizio utilizziamo un comando simile a quello per ssh ovvero

ydra -L users.txt -P pass.txt 192.168.50.100 -t 4 ftp