Authentication cracking con Hydra

Introduzione

L'obiettivo di questa esercitazione è simulare un attacco per craccare l'autenticazione di servizi di rete utilizzando Hydra , uno degli strumenti più diffusi per questo tipo di operazioni. L'esercizio si concentra sui servizi **SSH** e **FTP** , valutando quanto sia facile compromettere un sistema configurato in modo insicuro.

Configurazione user

Tramite terminale di **kali linux,** abbiamo creato un nuovo utente chiamato **test_user** e inserito una password semplice (**testpass**).

```
└─$ sudo adduser test_user
[sudo] password for kali:
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 []: testuser
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Successivamente attiviamo il servizio ssh con il comando **sudo service ssh start** e testiamo la connessione, nel nostro caso le credenziali inserite sono corrette in quanto riceviamo il prompt dei comandi dell'utente **test_user** sulla nostra kali.

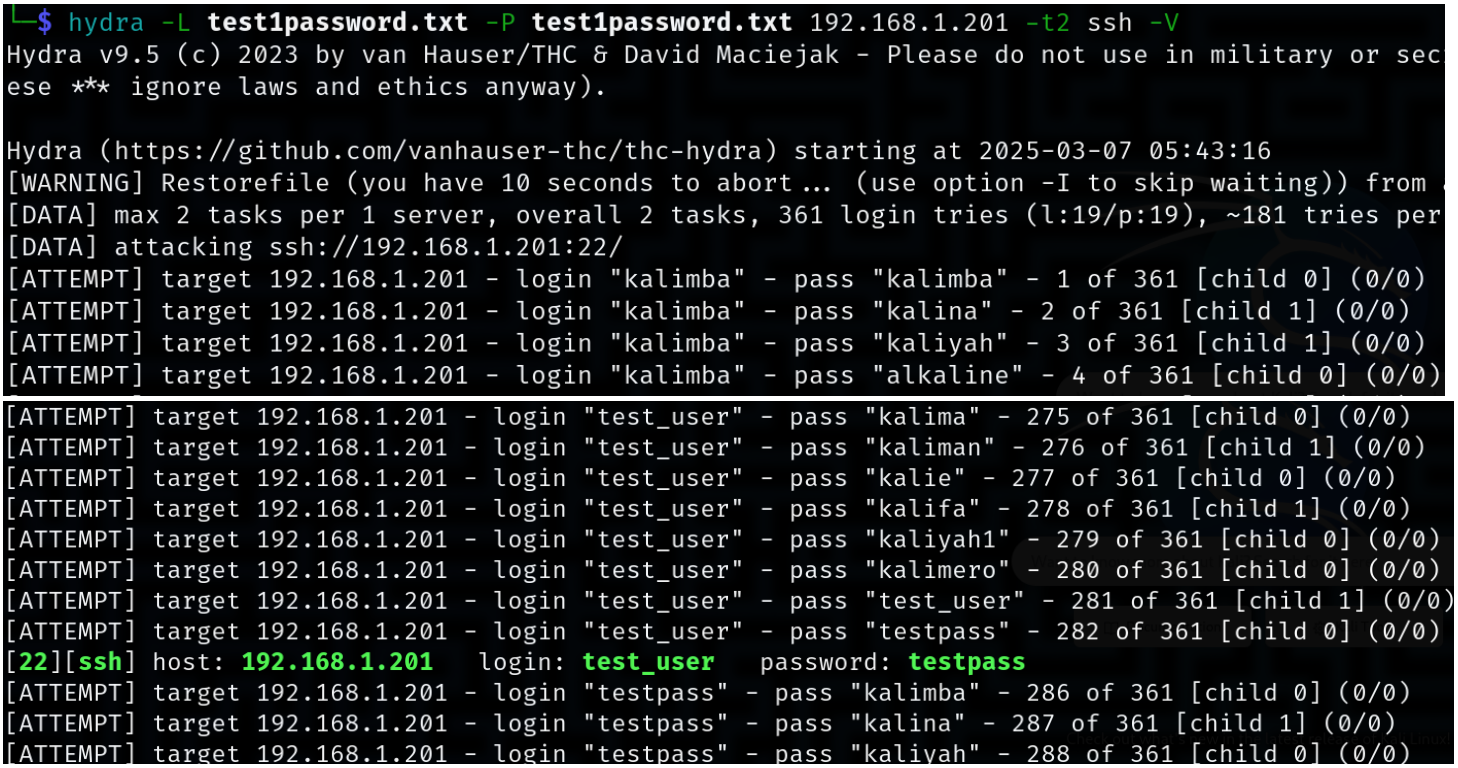
```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.201
test_user@192.168.1.201's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

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.
Last login: Fri Mar  7 04:05:25 2025 from 192.168.1.201
┌──(test_user㉿kali)-[~]
└─$
```

Attacco al servizio SSH

Per testare la sicurezza del servizio SSH, abbiamo utilizzato **Hydra** con una wordlist contenente oltre **1 milione di password** , presa direttamente da **Seclists** .

Dopo alcuni minuti di attesa decidiamo di interrompere il processo perchè avrebbe richiesto molto tempo.

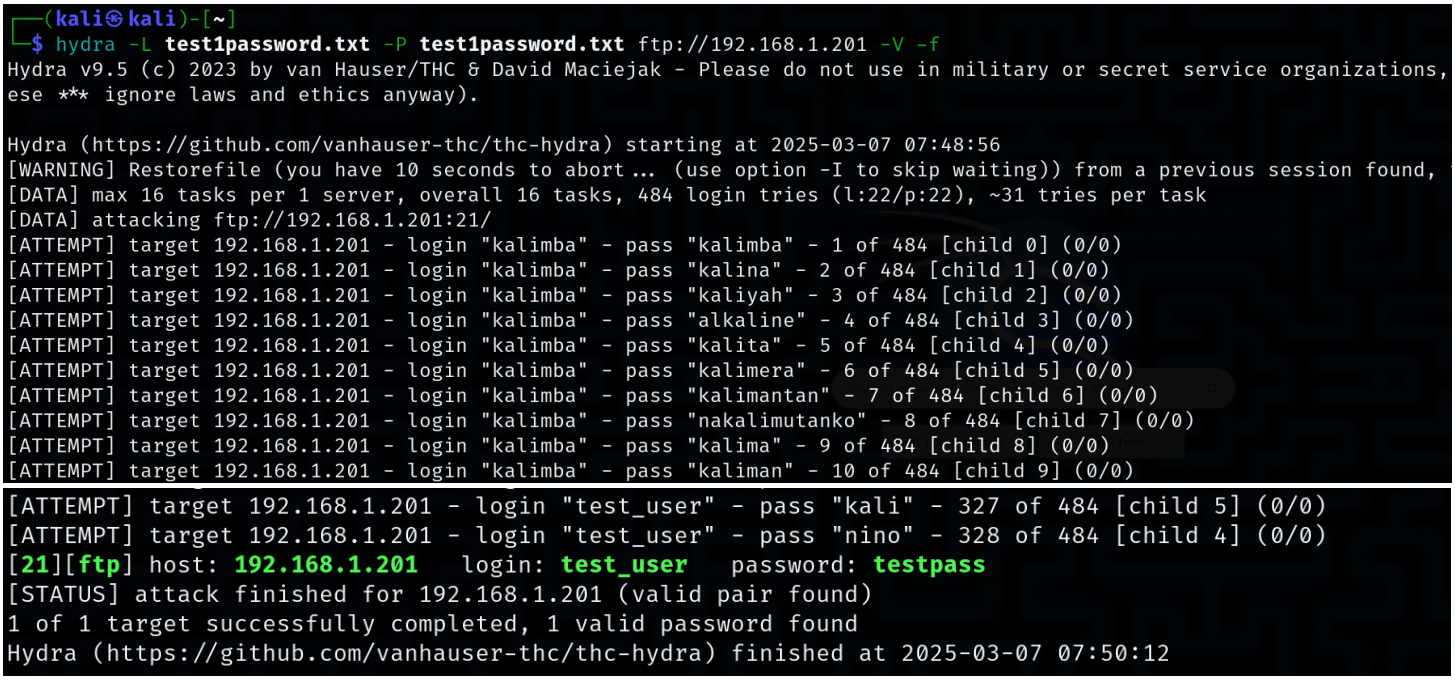
Andiamo quindi a creare una wordlist che include password comuni estratte da Seclists e aggiunto manualmente la password **testpass**, che so essere quella dell'utente **test_user**.
Data la dimensione ridotta della wordlist riusciamo ad ottenere le credenziali in breve tempo.



Attacco al servizio FTP

Successivamente, abbiamo configurato e avviato il servizio FTP utilizzando **vsftpd** con il comando
sudo service vsftpd start.

Una volta avviato il servizio, abbiamo ripetuto l'attacco con Hydra, questa volta mirando al servizio FTP sulla porta 21. Per monitorare lo stato dell'attacco e interrompere il processo non appena le credenziali corrette fossero state trovate, abbiamo aggiunto i parametri **-V** (verbose mode) e **-f** (ferma l'esecuzione dopo il primo successo).



Anche in questo caso, Hydra ha individuato rapidamente la password **testpass.**

Conclusioni

Questa simulazione ci dimostra quanto sia facile compromettere servizi di rete come SSH e FTP quando vengono utilizzate credenziali deboli. Anche un **attacco a dizionario** con strumenti basilari come Hydra può avere successo se le password sono semplici o prevedibili.