Hydra

Traccia:

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

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.

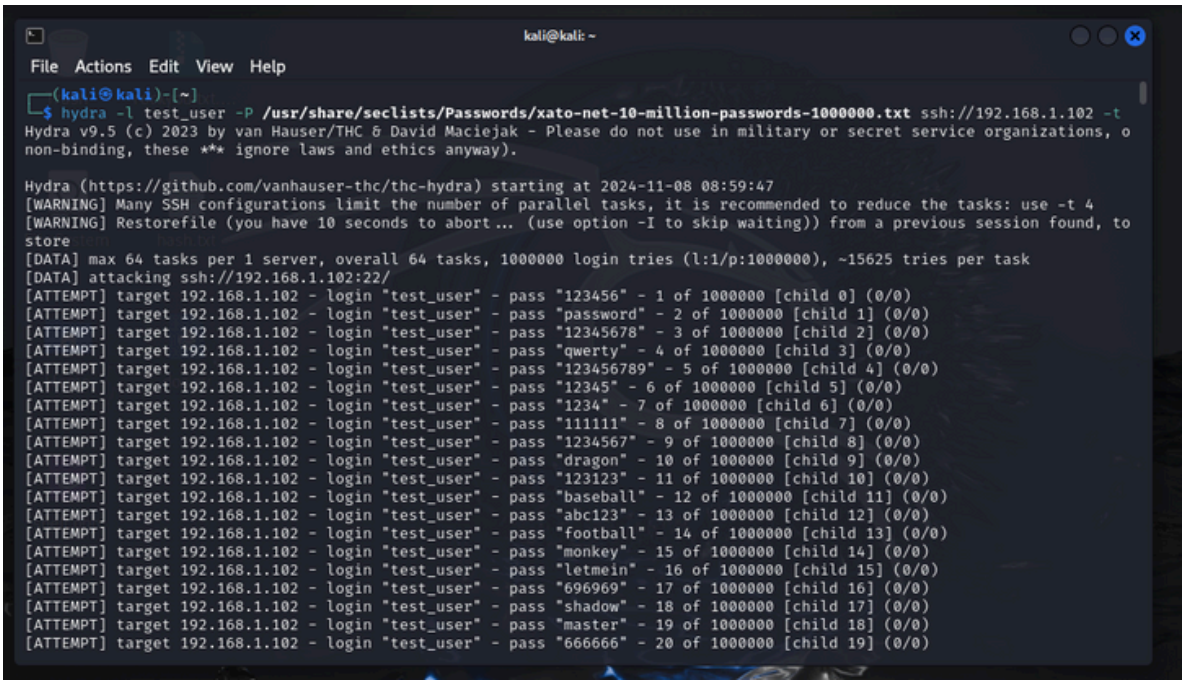
L'esercizio si svilupperà in due fasi:

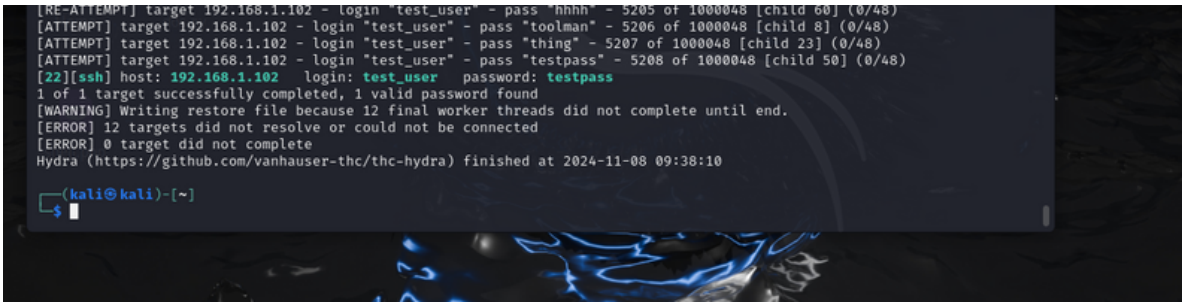
- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.

- 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.

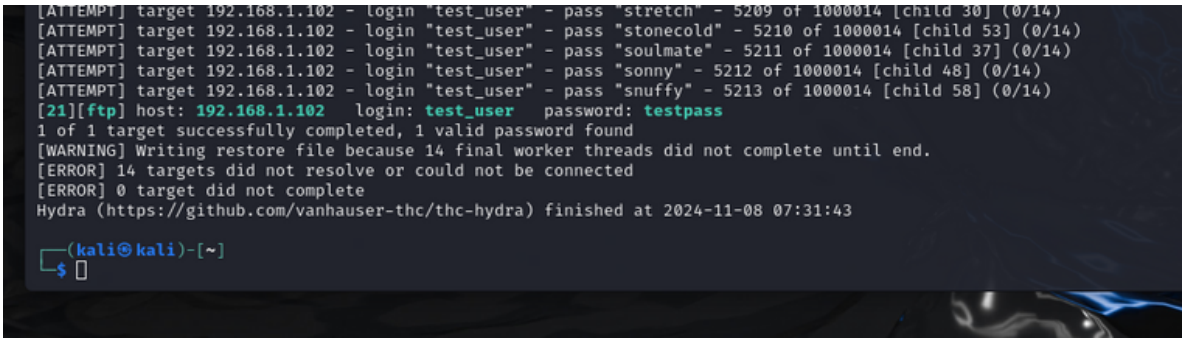
Creazione User e ssh

Attacco e risultato ssh





Attacco e risultato ftp



Relazione

L'esercizio di oggi ha lo scopo di mettere in pratica l'uso di Hydra per craccare l'autenticazione dei servizi di rete e approfondire la configurazione di tali servizi.

Prima fase dell'esercizio:

- Ho creato un nuovo utente su Kali, chiamato "test_user" con la password "testpass".
- Successivamente, su Kali, ho attivato il servizio SSH con il comando sudo service ssh start.
- Ho testato la connessione SSH con l'utente test_user utilizzando il comando ssh test_user@192.168.1.102.
- Ho poi utilizzato Hydra per effettuare un attacco di cracking sull'autenticazione SSH. In questa fase, ho impiegato una lista di username e password per eseguire un attacco a dizionario, sfruttando i comandi -L e -P per specificare le wordlist da utilizzare e l'indirizzo IP della macchina Kali. In questo caso, ho usato Seclists, che fornisce una vasta collezione di username e password utili per questo tipo di attacco.

Seconda fase dell'esercizio:

- Ho scelto un altro servizio di rete da configurare, come FTP, e ho testato l'autenticazione con Hydra.
- Per FTP, ho dovuto installare e avviare il servizio vsftpd tramite i comandi forniti nelle slide.

Questo esercizio consente di consolidare le conoscenze e le tecniche di cracking tramite l'uso di Hydra.

Daniel_Gabriel_Costeanu