S6L5
Authentication cracking con Hydra

Esercizio del giorno

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.

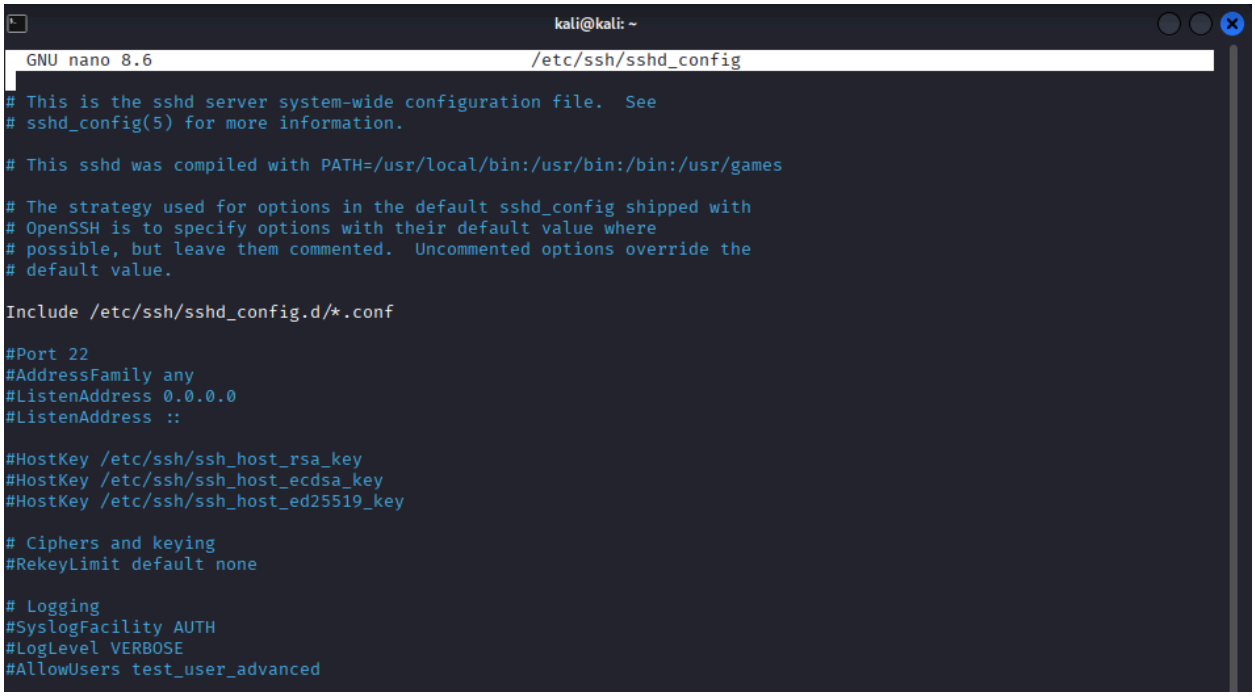
Fase 1: Esercizio guidato SSH

La prima parte dell'esercitazione dimostra il processo completo di attacco a un servizio SSH configurato.

Creiamo un utente chiamato “test_user_advanced” e inseriamo una password, in questo caso “**Ep1c0d3_2024!Secure#**”

Facciamo partire il servizio SSH con il comando:

sudo service ssh start



Viene verificata la connettività SSH iniziale attraverso il comando:

ssh test_user_advanced@192.168.50.10

Questa verifica preliminare assicura il corretto funzionamento del servizio prima di procedere con l'attacco vero e proprio.

Configurazione di Hydra

Una volta verificato l'accesso, non ci resta che configurare Hydra, per attaccare la configurazione SSH con il seguente comando:

hydra -L user_txt -P password_txt 192.168.50.10 -t1 ssh

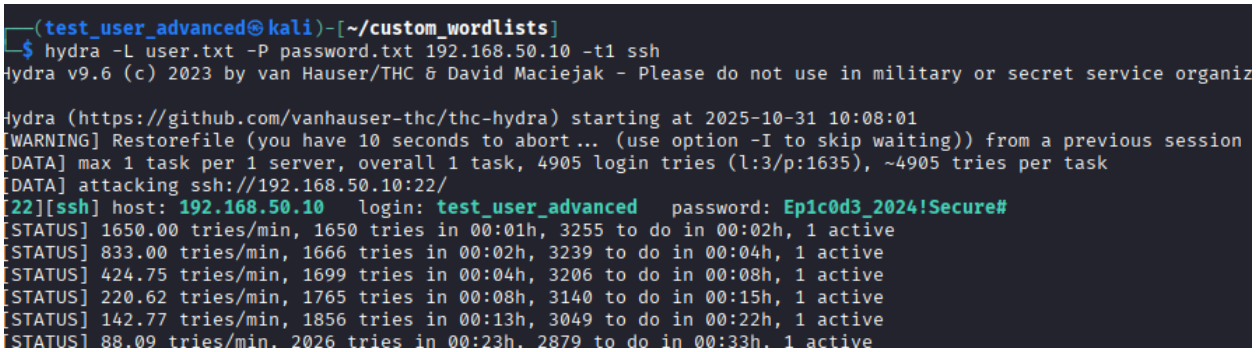
dove -L e -P sono usati per inserire le wordlist contenenti username e password e il parametro -t1 definisce il numero di task paralleli.

Importanza delle wordlist

Viene sottolineata l'importanza cruciale delle wordlist di qualità. Il documento raccomanda l'installazione di seclists, una collezione completa di username e password, attraverso il comando:

sudo apt install seclists

Tuttavia, il report evidenzia un problema significativo: l'utilizzo di wordlist troppo estese (come evidenziato dalla dimensione di 8.295.473.599.916 combinazioni) risulta impraticabile per tempistiche realistiche, perciò ne utilizzerò una più piccola composta da "solo" 4905 combinazioni.



Fase 2: Esercizio autonomo FTP

La seconda parte dell'esercitazione incoraggia l'applicazione autonoma delle tecniche apprese ad altri servizi di rete.

Viene suggerito in particolare il servizio FTP, con indicazioni per l'installazione e configurazione:

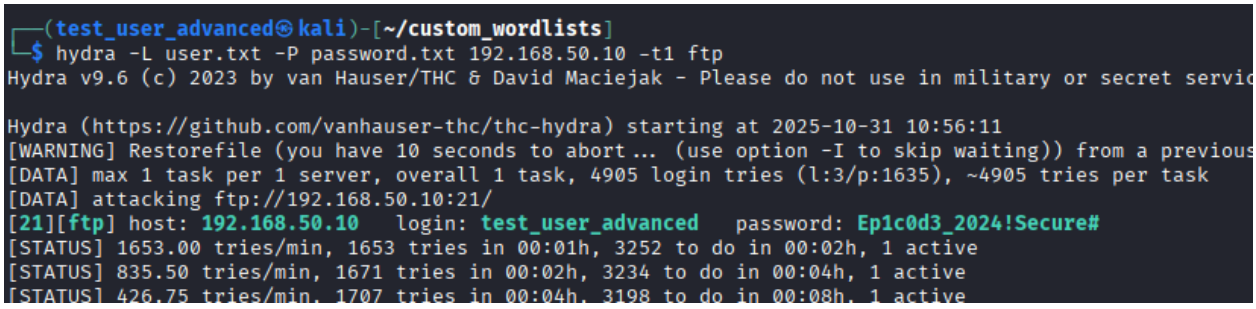
sudo apt install vsftpd

sudo service vsftpd start

Stavolta inseriamo il codice:

hydra -L user_txt -P password_txt 192.168.50.10 -t1 ftp

Così facendo tenteremo l'attacco dalla porta 21 (FTP).



Conclusioni:

Alla fine di questa esercitazione con Hydra, diventa chiaro che gli attacchi brute force puri, dove si provano tutte le combinazioni possibili di caratteri, sono nella pratica poco efficienti e richiedono tempi enormi. Come abbiamo visto dall'esempio nel report, quando si utilizzano wordlist troppo grandi come quelle di seclists, il numero di tentativi diventa astronomico e i tempi di attacco si dilatano in modo impraticabile.

La vera efficacia nel cracking delle password non sta nella forza bruta, ma nell'intelligenza con cui si scelgono le password da testare. Un attacco a dizionario ben costruito, anche se più piccolo, può essere molto più efficace di un brute force completo. Questo perché la maggior parte degli utenti tende a creare password che seguono pattern prevedibili o che contengono parole comuni, riferimenti personali, o variazioni semplici di password note.

L'approccio migliore è quindi quello di creare wordlist personalizzate e mirate al contesto specifico che stiamo attaccando. Per esempio, se stiamo testando un sistema chiamato "Epicode", ha senso includere password che contengono questo nome, con variazioni comuni come "Ep1c0d3", "epicode2024", o combinazioni con caratteri speciali. Queste password hanno una probabilità molto più alta di successo rispetto a password completamente casuali.

Inoltre, è importante ricordare che i servizi moderni hanno meccanismi di protezione contro gli attacchi brute force. Troppi tentativi in poco tempo possono far bloccare l'IP o attivare sistemi di rate limiting. Per questo, oltre a usare dizionari più piccoli e mirati, è fondamentale regolare i parametri di Hydra come il numero di connessioni parallele e i tempi di attesa tra un tentativo e l'altro.

In definitiva, il cracking delle password è più un'arte che una scienza esatta: richiede pazienza, una buona comprensione della psicologia degli utenti nella scelta delle password, e la capacità di creare dizionari intelligenti che massimizzino le probabilità di successo minimizzando i tempi di attacco.