AUTHENTICATION CRACKING CON HYDRA

Traccia: 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.

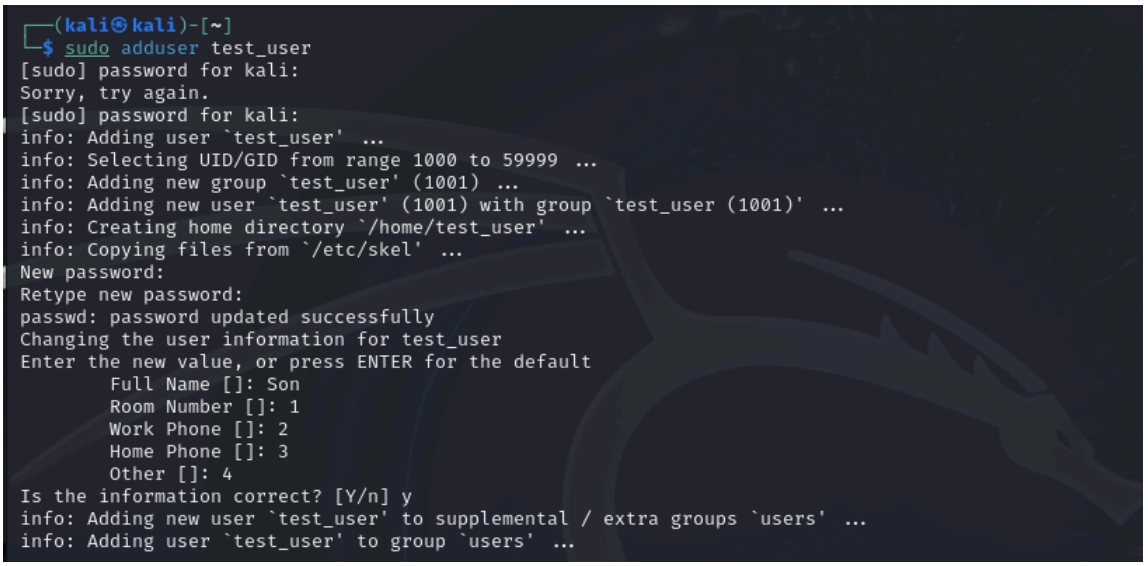
L'esercizio si svilupperà in due fasi:

- 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.

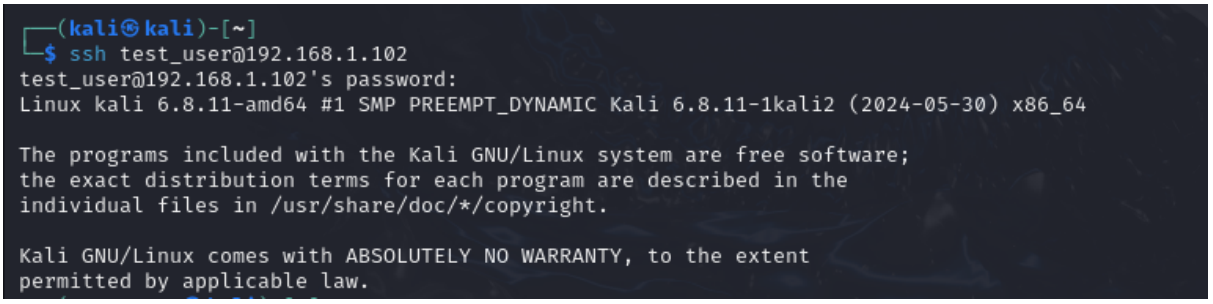
Svolgimento:

Introduzione

In questo esercizio si chiede di creare un account sulla macchina Kali Linux da utilizzare per effettuare un test di cracking tramite lo strumento Hydra.
Prima di intraprendere qualsiasi azione, sarà una buona norma scaricare una wordlist che possa facilitare il compito ad Hydra, in quanto un attacco Brute Force sarebbe efficace, ma troppo dispendioso in termini di tempo.
La lista consigliata è la lista *seclists*.
Dopodichè, il secondo step consiste nel creare l'account fittizio che verrà utilizzato per questo password cracking.



Il passaggio successivo consiste nell'istallazione ed attivazione del servizio SSH (Secure Shell), un protocollo di rete crittografato che serve a stabilire la connessione tra due dispositivi su una rete non sicura.



Hydra

Adesso siamo pronti per avviare il programma Hydra per andare ad attivare la ricerca della password.

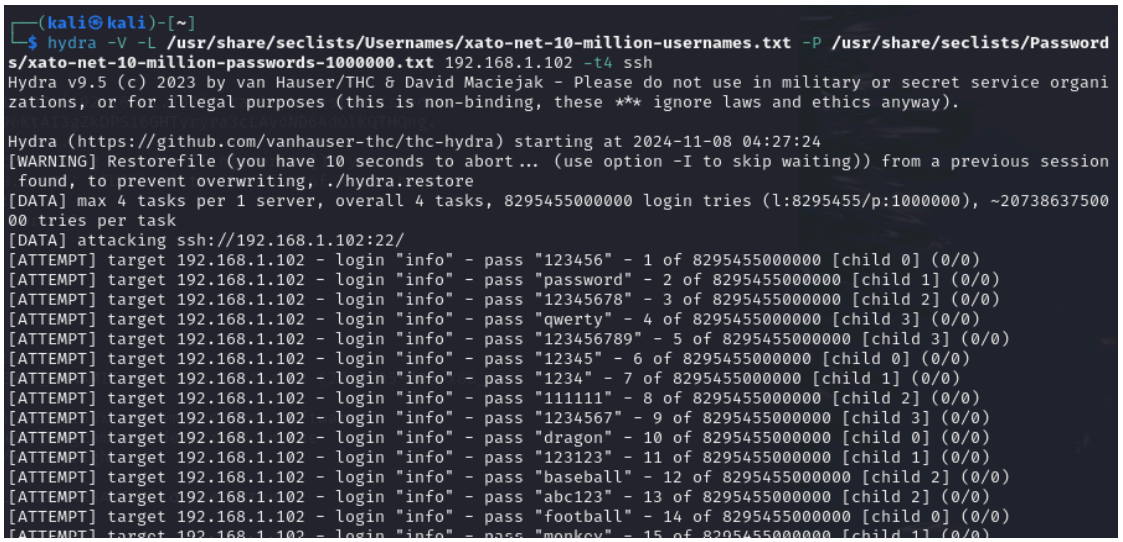
Il comando che andremo ad avviare sara:

hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.1.102 -t4 ssh

In cui:

- -V (verbose mode) ci farà visualizzare la lista di tutti i tentativi effettuati;
- -L serve per specificare la wordlist degli username a cui attingeremo;
- -P specifica la wordlist delle password;
- -t4 il numero di thread che andrà ad analizzare (determina la velocità);
- ssh è il protocollo utilizzato.

Il risultato che otterremo al suo avvio sarà il seguente:



Il programma è stato avviato e sta procedendo con successo, ma, essendo la lista molto lunga, ci metterà molto ad ottenere il risultato sperato, quindi sono andata a cercare delle soluzioni alternative per facilitare il programma.

Possibili soluzioni per velocizzare il programma

La prima soluzione a cui ho pensato è quella di accorciare le liste.
In questo caso si presuppone di conoscere già username e password, per aiutare il programma la prima cosa che ho fatto è stata consultare le liste disponibili.
La prima scrematura effettuata è stata quella di attingere alla lista delle Password, anzichè utilizzare quella da 100000 password, ho sostituito il file con la lista contenente 10000 elementi.
La lista però è ancora molto lunga, il passaggio successivo che ho pensato di cominciare ad attuare è stato quello di realizzare una lista contenente solo password che iniziano con la T ed una contenente solo username con la T, ma anche questa soluzione ha prodotto troppi risultati per essere analizzati in poco tempo.
La soluzione più efficace che ho trovato è stata quella di ridurre le liste limitandomi a poche righe tra quelle utili con il comando:

sed -n '5200,5220p' /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt > pass_5200_5220.txt

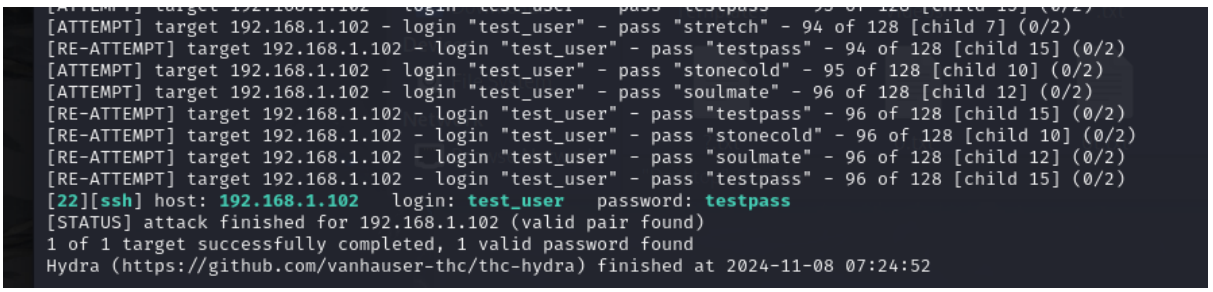
Questo comando ha prodotto un file contenente le righe dalla 5200 alla 5220, in una delle quali è presente la password che ci serve, la stessa cosa è stata eseguita con il file degli user.
Nel comando di Hydra ho inserito anche:

- -t16 che velocizza l'analisi dei thread;
- -f che farà fermare la ricerca non appena avrà trovato username e password corretti.

Il comando finale inviato a Hydra risulterà il seguente:

hydra -V -L users_241935_241940.txt -P pass_5200_5220.txt 192.168.1.102 -t16 -f ssh

Il seguente sarà il risultato finale:

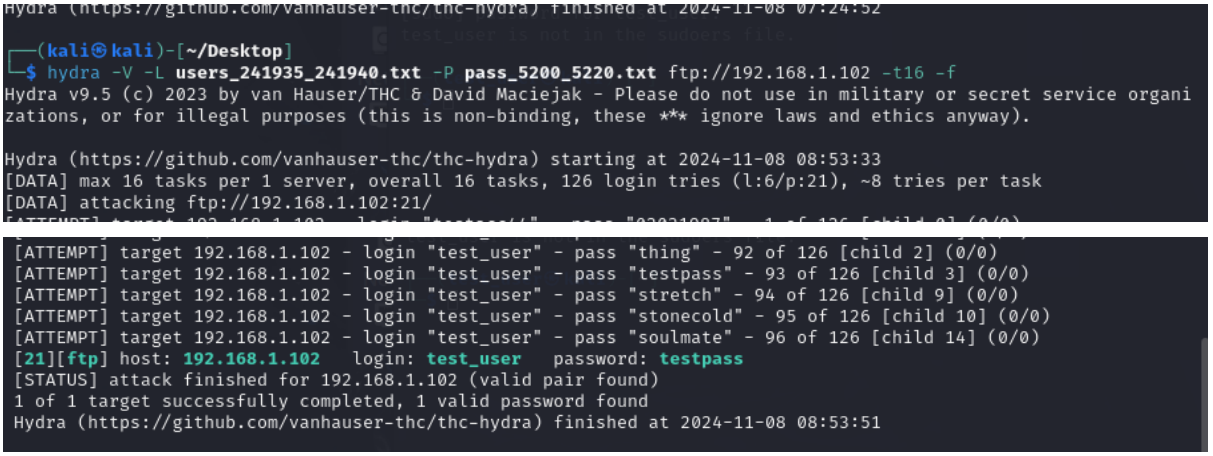


FTP
Il tentativo è stato eseguito anche tramite protocollo FTP.
Andiamo a rivedere di cosa si occupa: il protocollo FTP (File Transfer Protocol) è il protocollo standard che regola il trasferimento dei file tra un client ed un server su una rete TCP/IP, utile per trasferire anche grandi volumi di dati.
Il primo passaggio che sono andata ad eseguire è stata l'attivazione del protocollo sulla macchina Kali e verificarne il funzionamento.

Il passo successivo è stato provare il comando di Hydra, io l'ho eseguito utilizzando le liste accorciate realizzate precedentemente.
Il comando che ho eseguito per avviare Hydra utilizzando il protocollo FTP sarà il seguente:

hydra -V -L users_241935_241940.txt -P pass_5200_5220.txt ftp://192.168.1.102 -t16 -f

Da notare come ho mantenuto le stesse caratteristiche utilizzate, ciò che è cambiato è il protocollo, dettato dal comando con <<ftp://>> al posto dell'ssh finale presente nel comando precedente.
Il risultato sarà il seguente:



Conclusioni
Hydra è un potente programma open source utilizzato per eseguire attacchi Brute Force anche in rete, in ambito di Cyber Security si utilizza per testare la robustezza delle credenziali sui vari protocolli, i protocolli utilizzati in questo progetto sono stati: SSH e FTP.
Sfruttando una wordlist, ovvero un dizionario, è possibile effettuare attacchi a dizionario, ovvero attacchi che attingono ad una lista già pronta delle credenziali più frequenti, ciò consente al programma di ridurre considerevolmente le tempistiche di ricerca delle credenziali, se esse sono presenti sulla lista.

Per ridurre le tempistiche di ricerca si possono usare diversi accorgimenti tra cui:

- accorciare la lista;
- velocizzare l'analisi dei thread;
- interrompere la ricerca una volta ottenuto il risultato sperato;
- cambiare protocollo su cui effettuare la ricerca (FTP risulta più veloce, SSH tra i più lenti).

Con questi accorgimenti è possibile ottenere un risultato efficace in minor tempo.

Progetto presentato da:
Sonia Laterza