HYDRA ATTACK

HYDRA è un software per eseguire diversi attacchi Dizionario/Bruteforce su diversi protocolli di rete per scoprire l'USER e la Password.

Esso può essere eseguito da riga di comando oppure da GUI (interfaccia grafica)

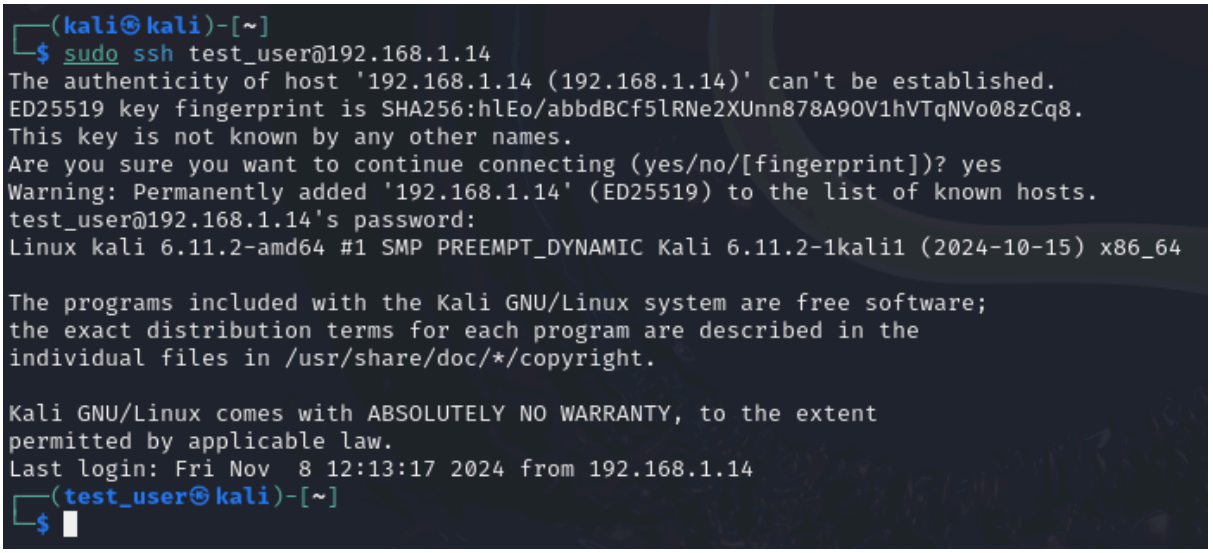
Oggi proveremo, tramite riga di comando, di trovare i dati di accesso alla porta SSH (22)

Tutte le porte utilizzano un sistema di autenticazione per potervi accedere .
La porta SSH (22) è utilizzata per far comunicare diversi dispositivi criptando il trasferimento dei dati rendendoli sicuri.

Per prima cosa andiamo a creare un nuovo user sulla macchina Kali:

USER: test_user
Password: testpass
Adesso accendiamo la porta ssh con il seguente comando:
SERVICE SSH START
SERVICE SSH STATUS → per capire se è aperta

Proviamo un piccolo test usando test_user



Con questo comando facciamo collegare l'user ad un server tramite il protocollo SSH

Facciamo partire i hydra e scriviamo su riga di comando la seguente istruzione:

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.14 -t 4 -W 1 -vV ssh

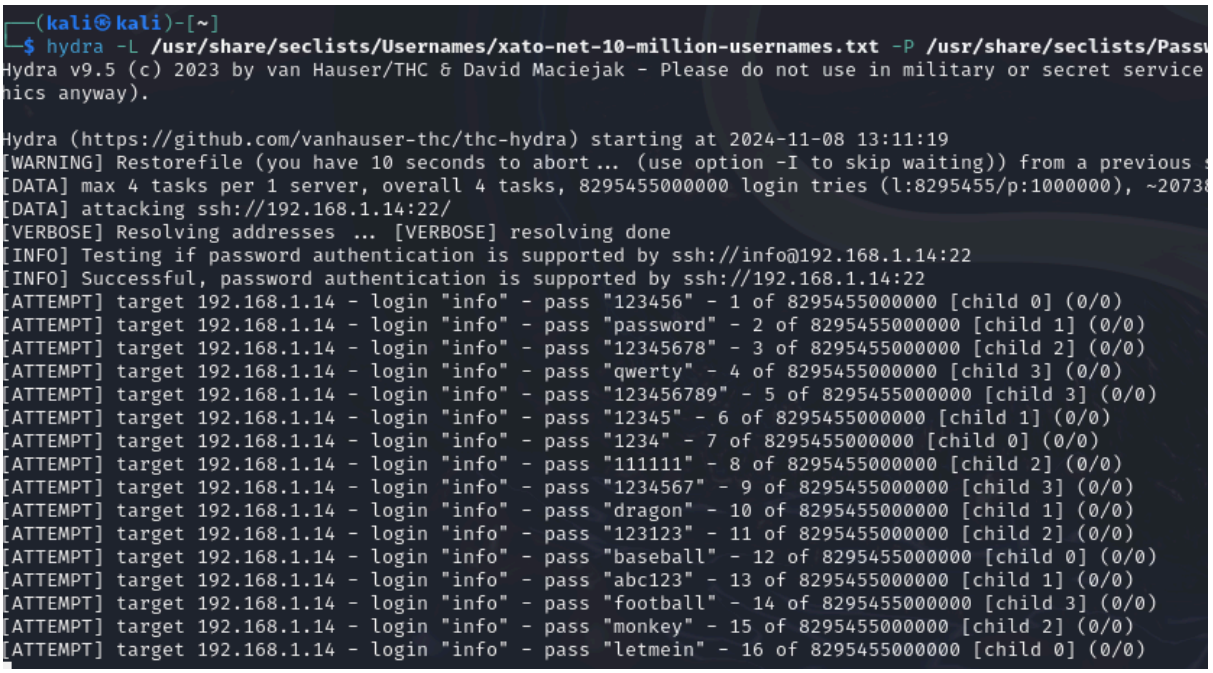
-L va a prendere i possibili user da un dizionario precedentemente installato su kali (seclist)

-P Va a prendere le possibili password da un dizionario seclist

-t 4 Numero di tentativi per combinazione

-W1 Delay per ogni combinazione

-vV Vedo i tentativi



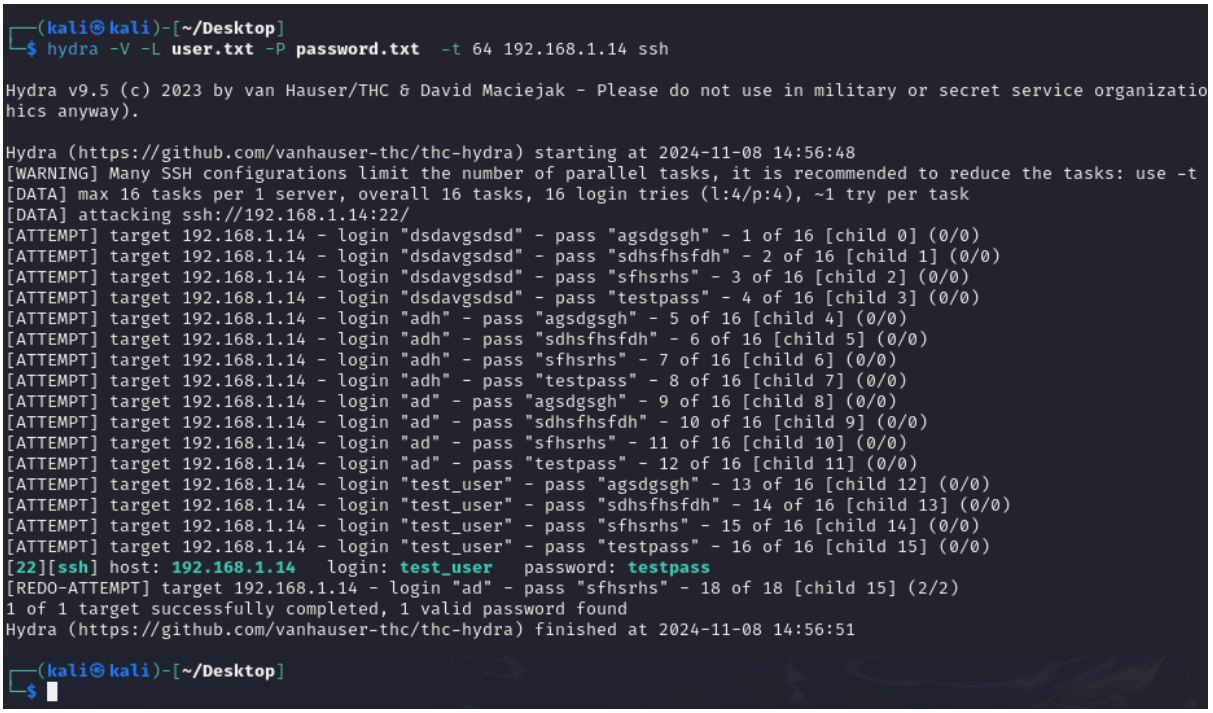
Si è stimato che per trovare la password ed user il software ci metta un tempo esorbitante.
Quindi dobbiamo trovare una soluzione al problema:

1. trovare una lista più piccola ed aggiornata da poter testare
2. creare una lista utilizzando il comando grep per filtrare le liste di SECLIST
   grep -E "^[a-z]{8}$" xato-net-10-million-passwords-1000000.txt | grep "pass" >
   ElencoPassTest.txt

prendi in considerazione soltanto gli user nella lista con 8 caratteri ed nel campo

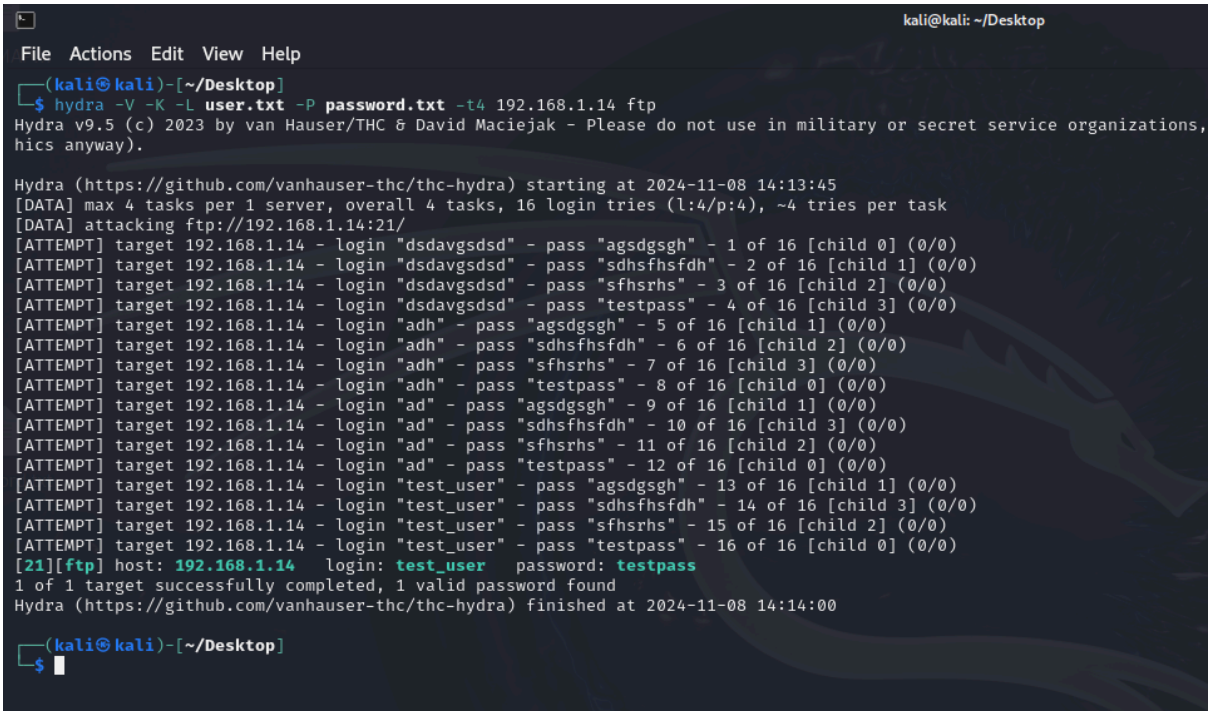
password solo ed esclusivamente le parole contenti pass

Creando questa lista (esempio da me creata) possiamo riavviare HYDRA e scoprire le credenziali:



Quello scritto in verde sono le credenziali che stiamo cercando

Ho provato nello stesso modo non il protocollo FTP



SOLUZIONI PER DIFESA

1. Per difendersi a questo attacco possiamo utilizzare password più lunghe e complesse

2. Utilizzare parole meno comuni

3. Usare la doppia autenticazione

SOLUZIONI PER ATTACCO

1. Utilizzare Dizionari più corti e aggiornati sulle nuove parole

2. Utilizzare metodi utilizzando l'ingegneria sociale esempio PHISHING

3. Provare con protocolli che non utilizzano la criptazione dei dati (FTP)