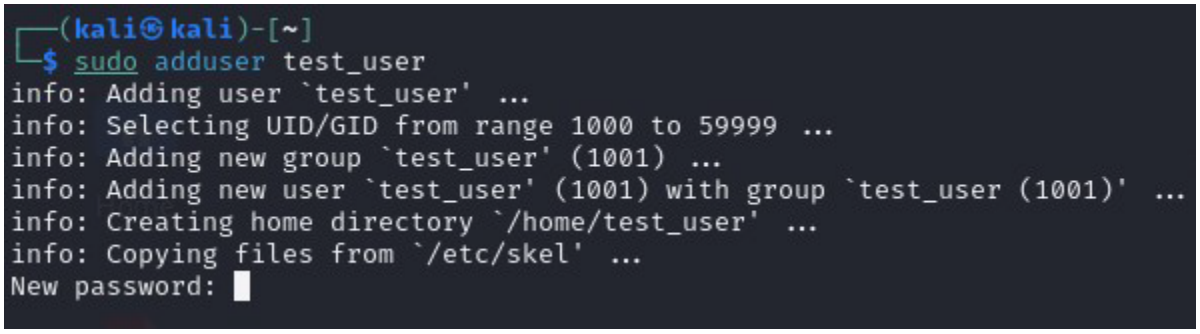
PRATICA S6L5

Il progetto di questa settimana ha un duplice scopo:
• Fare pratica con Hydra per crackare l'autenticazione dei servizi di rete.
• Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

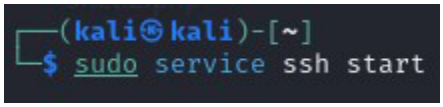
L'esercizio si svolgerà in 2 fasi:
• Nella prima, vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
• Nella seconda, saremo liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rcp, telnet, autenticazione HTTP.

1. ABILITAZIONE SSH E CRACKING

Avviamo Kali Linux e inviamo il comando sudo adduser test_user per creare un nuovo utente chiamato test_user. Poi impostiamo come password test_password.



Ora avviamo il servizio ssh con sudo service ssh start:



Ora testiamo la connessione ssh del nuovo utente appena creato, eseguendo il comando ssh test_user@192.168.5.5, dove 192.168.5.5 è l'IP della macchina Kali:

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.5.5
The authenticity of host '192.168.5.5 (192.168.5.5)' can't be established.
ED25519 key fingerprint is SHA256:WlK3PFlLPs44oRNcVty7PU3EIg3KXkq3XwCq1d+fuF0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.5' (ED25519) to the list of known hosts.
test_user@192.168.5.5's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.
┌──(test_user㉿kali)-[~]
└─$
```

A questo punto possiamo configurare Hydra per una sessione di cracking.

Ipotizzando di non conoscere username e password l'unica opzione è un attacco a dizionario. Usiamo gli switch -L, -P, che ci permettono di selezionare i file.txt contenenti milioni di username e password. Il comando sarà **hydra -L username_list -P password_list IP_KALI -t 4 ssh**.

Prima di lanciare il comando scarichiamo una collezione di username e password di seclists. Queste cartelle contengono milioni di file da poter testare in un attacco a dizionario.

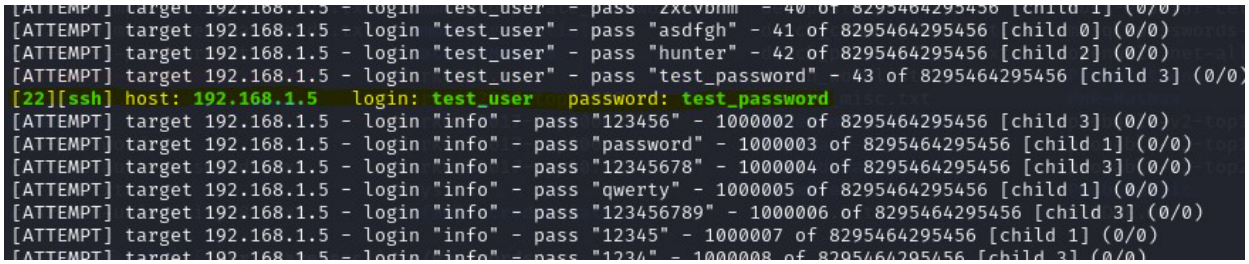
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1880 not upgraded.
Need to get 526 MB of archives.
After this operation, 2,082 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 6s (86.6 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 401828 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...
```

Ora possiamo inviare il comando Hydra selezionando i path delle liste.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.5 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 04:39:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.5:22/
```

La stima di tempo per provare tutte le combinazioni è di 18 ore, quindi ho manipolato la lista degli username inserendo in cima alla lista l'username di mio interesse e la lista delle password inserendo non troppo in basso la password test_password, in modo che venisse impiegato meno tempo, poi ho di nuovo mandato il comando e questo è il risultato.

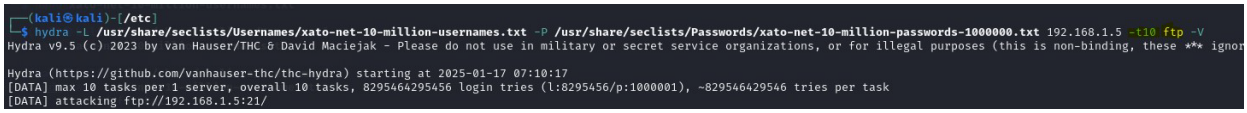


Il programma ha quindi trovato la giusta combinazione.

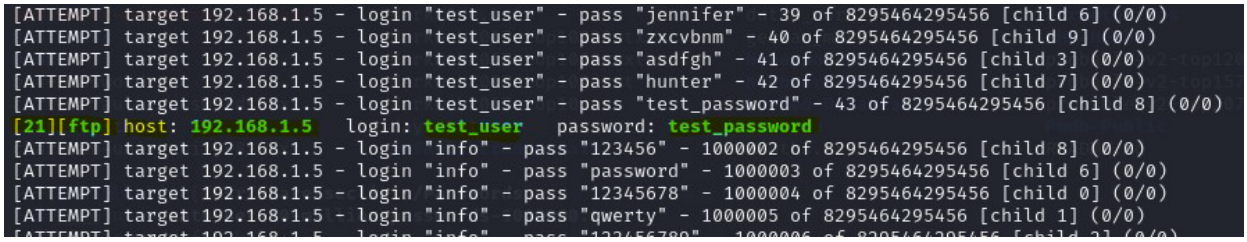
2. ABILITAZIONE FTP E CRACKING

Prima di tutto installiamo il servizio FTP con il comando **sudo app Install vsftpd**.

Avviamo il servizio e inviamo il comando hydra modificando il parametro da -t4 a -t10 e modificando il servizio da ssh a ftp.



La -t definisce il numero di task, ovvero quante combinazioni può provare per volta, un numero molto basso di task può rendere il processo troppo lungo mentre un numero troppo alto potrebbe creare problemi al programma. Hydra mi ha dato questo risultato.



Possiamo notare che questa volta viene specificata la porta 21 dato che il servizio ftp lavora su quest’ultima.