LABORATORIO EPICODE

S6_L4

Traccia: Esercizio 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.

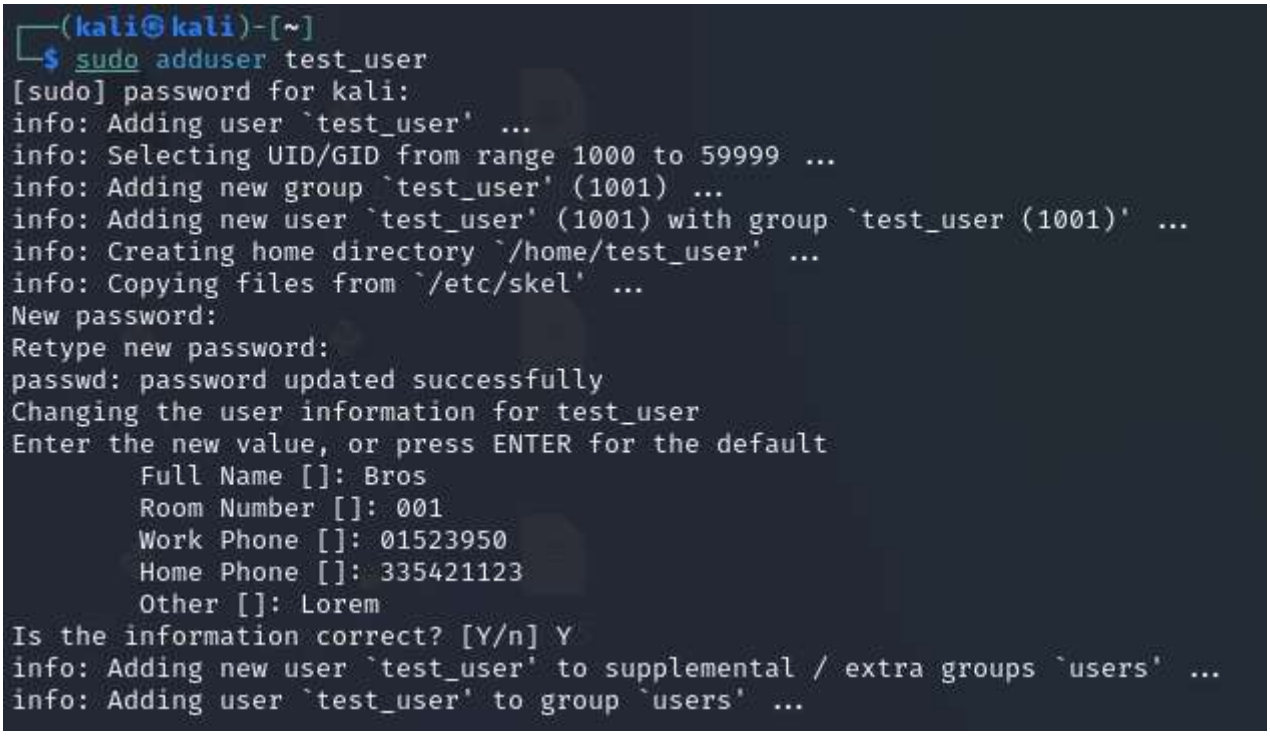
L'esercizio si svilupperà in due fasi:

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

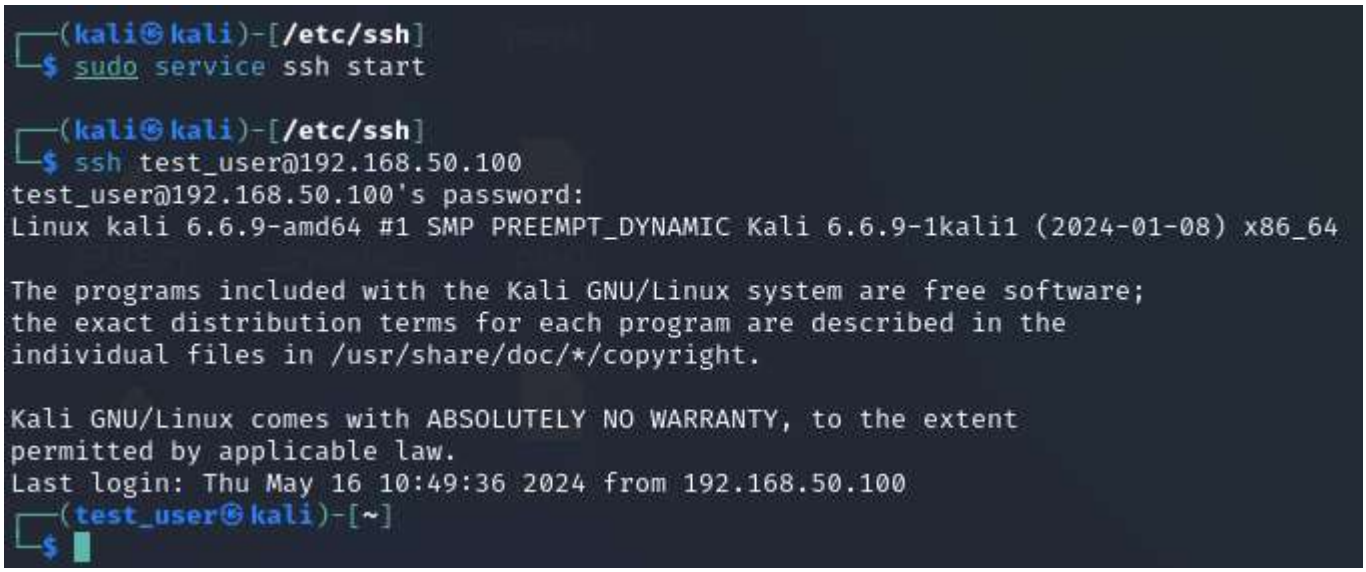
● Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

FASE 1

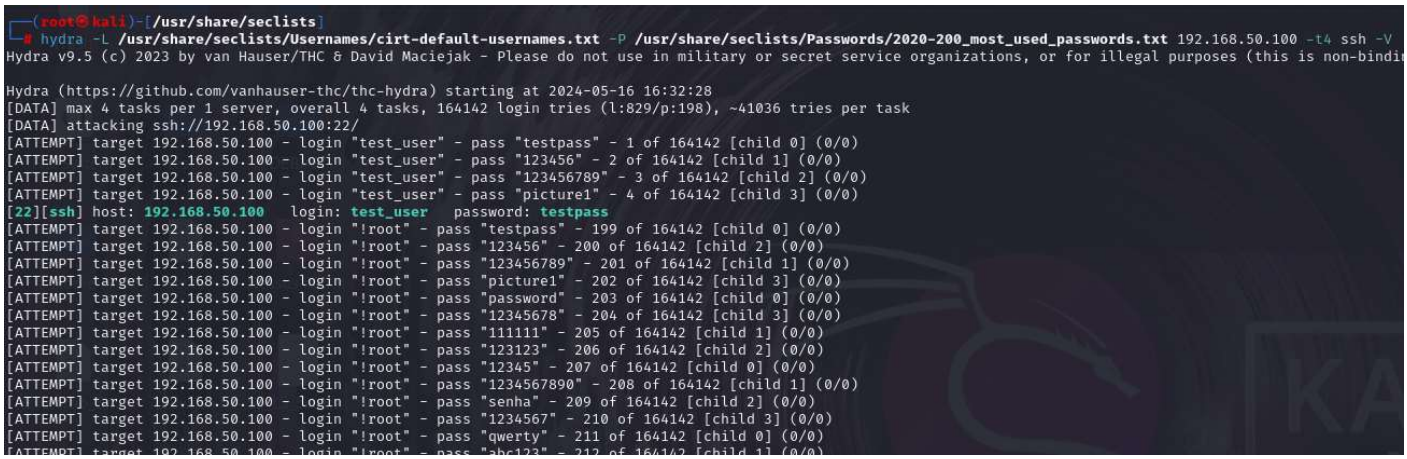
1. Procediamo con la creazione di un nuovo user con nome test_user e la password testpass inserendo alcuni dati identificativi



2. Attiviamo il servizio ssh con il seguente comando in figura



3. Una volta verificato il collegamento, utilizziamo Hydra per fare la ricerca dello Username e della Password in liste dedicate in file di testo nella sezione **seclists** che kali propone per svolgere l'esercitazione



FASE 2

Per creare la FASE 2 abbiamo optato di creare un nuovo servizio ftp

1. Procediamo con la creazione di un nuovo user con nome test_user2 e la password testpass2 inserendo alcuni dati identificativi

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user2
[sudo] password for kali:
info: Adding user `test_user2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user2' (1002) ...
info: Adding new user `test_user2' (1002) with group `test_user2 (1002)' ...
info: Creating home directory `/home/test_user2' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user2' to supplemental / extra groups `users' ...
info: Adding user `test_user2' to group `users' ...
```

2. Attiviamo il servizio ftp con il seguente comando in figura

```
┌──(kali㉿kali)-[~]
└─$ service vsftpd start
```

3. A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking

```
┌──(kali㉿kali)-[~]
└─$ ftp test_user2@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4. Eseguiamo la ricerca dello Username e della Password in liste dedicate in file di testo nella sezione **seclists** che kali propone per svolgere l'esercitazione