

## 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-firmware'
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:muTsTgVnMrz68XcjYus0wA4Lrh312j5Iwptwunz5f0Q.
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;

```
(test_user@kali)-[~]
$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-11-08 03:23:58 EST; 1h 14min ago
     Invocation: a70662e44b914b538f08ba16b624d69e
       Docs: man:sshd(8)
             man:sshd_config(5)
   Process: 9821 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 9823 (sshd)
       Tasks: 1 (limit: 9437)
      Memory: 4.9M (peak: 21.8M)
         CPU: 232ms
        CGroup: /system.slice/ssh.service
                └─9823 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
```

Ci assicuriamo che il servizio sia attivo;

```
# sudo su
(root@kali)-[/home/kali]
# sudo apt-get install seclists
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 1728 not upgraded.
Need to get 508 MB of archives.
After this operation, 2,045 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.3-0kali1 [508 MB]
Fetched 508 MB in 1min 1s (8,295 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 413747 files and directories currently installed.)
Preparing to unpack .../seclists_2024.3-0kali1_all.deb ...
Unpacking seclists (2024.3-0kali1) ...
Setting up seclists (2024.3-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...

(root@kali)-[/home/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 192.168.1.51 -t 4 ssh
```

Aggiorniamo le librerie seclists;

```
(test_user@kali)-[~]
$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
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 04:59:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prev
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 ssh://192.168.178.51:22/

[STATUS] 37.00 tries/min, 37 tries in 00:01h, 999963 to do in 450:27h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 999916 to do in 595:12h, 4 active

[STATUS] 26.29 tries/min, 184 tries in 00:07h, 999816 to do in 633:57h, 4 active
[STATUS] 25.87 tries/min, 388 tries in 00:15h, 999612 to do in 644:05h, 4 active

[STATUS] 25.94 tries/min, 804 tries in 00:31h, 999196 to do in 642:07h, 4 active
[STATUS] 26.00 tries/min, 1222 tries in 00:47h, 998778 to do in 640:15h, 4 active
[STATUS] 25.97 tries/min, 1636 tries in 01:03h, 998364 to do in 640:46h, 4 active
[STATUS] 25.87 tries/min, 2044 tries in 01:19h, 997956 to do in 642:51h, 4 active
[STATUS] 25.94 tries/min, 2464 tries in 01:35h, 997536 to do in 641:01h, 4 active
```

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.

```

(test_user@kali)-[~]
$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.178.51 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 04:59:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
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 ssh://192.168.178.51:22/

[STATUS] 37.00 tries/min, 37 tries in 00:01h, 999963 to do in 450:27h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 999916 to do in 595:12h, 4 active

[STATUS] 26.29 tries/min, 184 tries in 00:07h, 999816 to do in 633:57h, 4 active
[STATUS] 25.87 tries/min, 388 tries in 00:15h, 999612 to do in 644:05h, 4 active

[STATUS] 25.94 tries/min, 804 tries in 00:31h, 999196 to do in 642:07h, 4 active
[STATUS] 26.00 tries/min, 1222 tries in 00:47h, 998778 to do in 640:15h, 4 active
[STATUS] 25.97 tries/min, 1636 tries in 01:03h, 998364 to do in 640:46h, 4 active
[STATUS] 25.87 tries/min, 2044 tries in 01:19h, 997956 to do in 642:51h, 4 active
[STATUS] 25.94 tries/min, 2464 tries in 01:35h, 997536 to do in 641:01h, 4 active
[STATUS] 25.93 tries/min, 2878 tries in 01:51h, 997122 to do in 640:58h, 4 active
[STATUS] 25.90 tries/min, 3289 tries in 02:07h, 996711 to do in 641:27h, 4 active
[STATUS] 25.90 tries/min, 3704 tries in 02:23h, 996296 to do in 641:04h, 4 active
[STATUS] 25.92 tries/min, 4121 tries in 02:39h, 995879 to do in 640:24h, 4 active
[STATUS] 25.91 tries/min, 4535 tries in 02:55h, 995465 to do in 640:14h, 4 active
[STATUS] 25.88 tries/min, 4944 tries in 03:11h, 995056 to do in 640:42h, 4 active
[22][ssh] host: 192.168.178.51 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 08:20:55

(test_user@kali)-[~]

```

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;

```

[sudo] password for kali:
(root@kali)-[/home/kali]
# sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1728 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 13s (11.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 420089 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vs
ftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...

(root@kali)-[/home/kali]
# sudo nano /etc/vsftpd.conf

(root@kali)-[/home/kali]
# sudo systemctl restart vsftpd

(root@kali)-[/home/kali]
# sudo useradd testuser
sudo passwd testuser
New password:
Retype new password:

```

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

```
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:$y$j9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr35.oFZR4:20035:0:99999:7:::
```

e che quindi la pass cryptata è questa :

```
$y$j9T$EbPT7gr2PNleokasPhwqb/$y/VQT2exgBCGKwc6MMsx/hWsK3Fq4Ffr/Wr35.oFZR4
```

nel formato bcrypt.

Ho utilizzato John The Ripper per decifrarla, ma non ci ho messo 5/10 secondi.

Ho anche installato una versione “jumbo” di John The Ripper.

Altra alternativa che mi viene in mente è che, in quanto amministratore del sistema posso andare direttamente a modificare la password e quindi impostarne una che conosco.

Mi dispiace, ma non sono un hacker. 😊