

ESERCIZIO FACOLTATIVO W5D1 TULLI ROBERTO

Dopo aver aperto un terminale, per leggere il manuale dei comandi kill e ps basta semplicemente scrivere man <<comando>>

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

una volta dato invio si aprirà il manuale del comando da noi inserito (es. kill) presentando a schermo la seguente schermata dove poter leggere tutto il funzionamento del comando.

```
kali@kali: ~  
File Actions Edit View Help  
KILL(1) User Commands KILL(1)  
NAME  
kill - send a signal to a process  
SYNOPSIS  
kill [options] <pid> [...]  
DESCRIPTION  
The default signal for kill is TERM. Use -l or -L to list available signals.  
Particularly useful signals include HUP, INT, KILL, STOP, CONT, and 0. Alternate  
signals may be specified in three ways: -9, -SIGKILL or -KILL. Negative PID val-  
ues may be used to choose whole process groups; see the PGID column in ps command  
output. A PID of -1 is special; it indicates all processes except the kill  
process itself and init.  
OPTIONS  
<pid> [...]  
Send signal to every <pid> listed.  
-<signal>  
-s <signal>  
--signal <signal>  
Specify the signal to be sent. The signal can be specified by using name  
or number. The behavior of signals is explained in signal(7) manual page.  
-q, --queue value  
Use sigqueue(3) rather than kill(2) and the value argument is used to  
specify an integer to be sent with the signal. If the receiving process  
has installed a handler for this signal using the SA_SIGINFO flag to  
sigaction(2), then it can obtain this data via the si_value field of the  
siginfo_t structure.  
-l, --list [signal]  
List signal names. This option has optional argument, which will convert  
signal number to signal name, or other way round.  
Manual page kill(1) line 1 (press h for help or q to quit)
```

Successivamente l'esercizio richiede di lanciare il comando <<vi pippo>>, aprire un terminale e di visualizzare tutti i propri processi:

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ kali@kali: ~  
(kali@kali)-[~]  
$ ps aux  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.2  0.7 24108 14184 ?        Ss   11:08   0:02 /sbin/init splash  
root         2  0.0  0.0      0     0 ?        S    11:08   0:00 [kthreadd]  
root         3  0.0  0.0      0     0 ?        S    11:08   0:00 [pool_workqueue_release  
root         4  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-kvfree_rcu_r  
root         5  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-rcu_gp]  
root         6  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-sync_wq]  
root         7  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-slub_flushwq  
root         8  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-netns]  
root         9  0.1  0.0      0     0 ?        I    11:08   0:02 [kworker/0:0-events]  
root        12  0.0  0.0      0     0 ?        I    11:08   0:00 [kworker/u8:0-ipv6_addr  
root        13  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-mm_percpu_wq  
root        14  0.0  0.0      0     0 ?        I    11:08   0:00 [rcu_tasks_kthread]  
root        15  0.0  0.0      0     0 ?        I    11:08   0:00 [rcu_tasks_rude_kthread  
root        16  0.0  0.0      0     0 ?        I    11:08   0:00 [rcu_tasks_trace_kthrea  
root        17  0.0  0.0      0     0 ?        S    11:08   0:00 [ksoftirqd/0]  
root        18  0.2  0.0      0     0 ?        I    11:08   0:03 [rcu_preempt]  
root        19  0.0  0.0      0     0 ?        S    11:08   0:00 [rcu_exp_par_gp_kthread  
root        20  0.0  0.0      0     0 ?        S    11:08   0:00 [rcu_exp_gp_kthread_wor  
root        21  0.0  0.0      0     0 ?        S    11:08   0:00 [migration/0]  
root        22  0.0  0.0      0     0 ?        S    11:08   0:00 [idle_inject/0]  
root        23  0.0  0.0      0     0 ?        S    11:08   0:00 [cpuhp/0]  
root        24  0.0  0.0      0     0 ?        S    11:08   0:00 [cpuhp/1]  
root        25  0.0  0.0      0     0 ?        S    11:08   0:00 [idle_inject/1]  
root        26  0.0  0.0      0     0 ?        S    11:08   0:00 [migration/1]  
root        27  0.0  0.0      0     0 ?        S    11:08   0:00 [ksoftirqd/1]  
root        28  0.0  0.0      0     0 ?        I    11:08   0:00 [kworker/1:0-events]  
root        30  0.1  0.0      0     0 ?        I    11:08   0:01 [kworker/u9:0-kvfree_rc  
root        33  0.0  0.0      0     0 ?        I    11:08   0:00 [kworker/u10:1-events_u  
root        34  0.0  0.0      0     0 ?        S    11:08   0:00 [kdevtmpfs]  
root        35  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-inet_frag_wq  
root        36  0.0  0.0      0     0 ?        S    11:08   0:00 [kauditd]  
root        37  0.0  0.0      0     0 ?        S    11:08   0:00 [khungtaskd]  
root        39  0.0  0.0      0     0 ?        S    11:08   0:00 [oom_reaper]  
root        40  0.0  0.0      0     0 ?        I    11:08   0:00 [kworker/u9:2-events_un  
root        41  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-writeback]  
root        42  0.0  0.0      0     0 ?        S    11:08   0:00 [kcompactd0]  
root        43  0.0  0.0      0     0 ?        SN   11:08   0:00 [ksmd]  
root        44  0.2  0.0      0     0 ?        SN   11:08   0:03 [khugepaged]  
root        45  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-kintegrityd]  
root        46  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-kblockd]  
root        47  0.0  0.0      0     0 ?        I<   11:08   0:00 [kworker/R-blkcg_punt_b
```

```
(kali㉿kali)-[~]
└─$ ps aux | grep pippo
kali    17355  0.0  0.5  16196 10680 pts/0    Sl+  11:44   0:00 vim pippo
kali    19335  0.0  0.1   6528  2304 pts/1    S+   11:48   0:00 grep --color=auto pippo
```

```
(kali@kali)-[~]  
$ kill -9 17355
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
zsh: killed vim pippo  
~  
  
(kali@kali)-[~]  
$ 65;15;7M65;15;7M64;15;7M65;21;10M65;21;10M64;38;4M65;43;11M65;43;11M64;43;11M6  
4;43;11M64;43;11M64;43;11M64;43;11M64;43;11M64;43;11M65;43;11M65;43;11M65;43;11M65;43;11M6  
5;43;11M65;43;11M65;43;11M65;24;14M65;24;14M65;24;14M65;24;14M65;24;14M65;24;14M6  
4;24;14M64;24;14M64;24;14M64;24;14M64;24;14M64;24;14M
```

The image is a composite of two screenshots related to Kali Linux. The left screenshot shows a terminal window with the following content:

```
error: list of process IDs must follow p

Usage:
ps [options]

Try 'ps --help <module>|list|output|threads|misc|all'
or 'ps --help <sl|lo|t|m|a>'
for additional help text.

For more details see ps(1).
pipgo: command not found

(kali@kali)-[~]
$ ps aux | grep pipgo
kali   17355  0.0  0.5 16196 10680 pts/0    Sl+  11:44   0:00 vim pipgo
kali   19335  0.0  0.1  6528  2304 pts/1    S+   11:48   0:00 grep --color=auto pi

(kali@kali)-[~]
$ kill -9 17355

(kali@kali)-[~]
$ firefox &
[1] 30843

(kali@kali)-[~]
$ [GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt

[1] + done      firefox
(kali@kali)-[~]
$ firefox &
[1] 31345

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

The right screenshot shows a Kali Linux desktop environment. It features a blue and white Kali Linux logo (a dragon head) on a black background with a blue maze pattern. Below the logo is a search bar with the text "Want to know more about Kali? Search for it here!". At the bottom, there are two buttons: "Documentation" and "Kali Tools". The top of the desktop shows a browser window with the address bar displaying "file:///usr/share/kali-defaults/web/homepage.html". The browser's address bar also shows several bookmarks: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking DB".

per la risoluzione del punto 7 invece inseriamo il comando <firefox> per aprire il browser poi i tasti “ctrl+Z” per sospenderlo e successivamente <bg> per continuare mandarlo in background.

```
kali 17355 0.0 0.5 16196 10680 pts/0 Sl+ 11:44 0:00 vim pippo
kali 19335 0.0 0.1 6528 2304 pts/1 S+ 11:48 0:00 grep --color=auto pippo

(kali@kali)-[~]
$ kill -9 17355

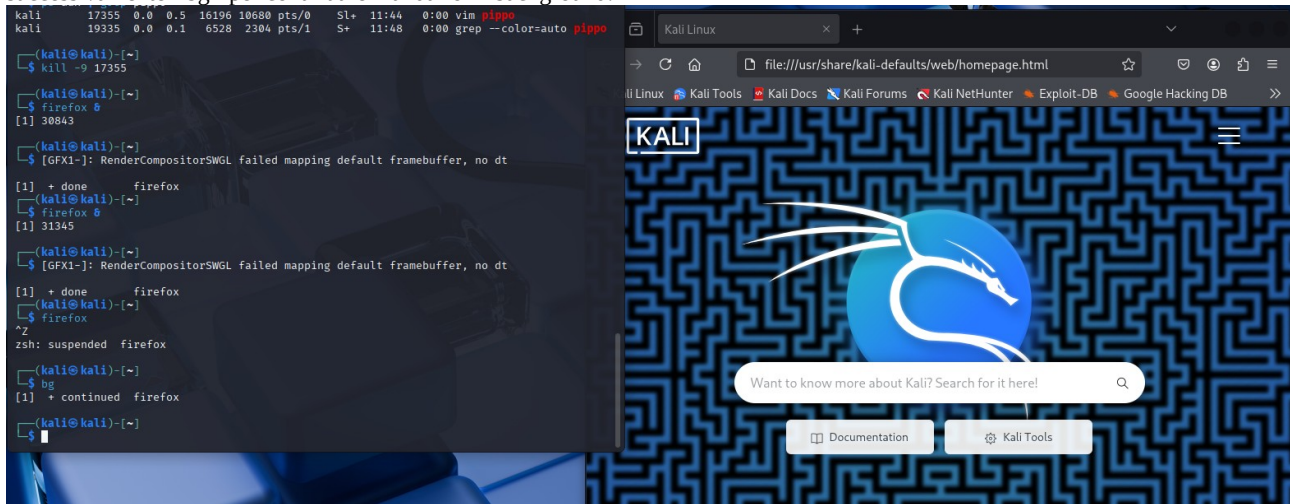
(kali@kali)-[~]
$ firefox &
[1] 30843

(kali@kali)-[~]
$ [GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt

[1] + done firefox
(kali@kali)-[~]
$ firefox &
[1] 31345

(kali@kali)-[~]
$ [GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt

[1] + done firefox
(kali@kali)-[~]
$ firefox
^Z
zsh: suspended firefox
(kali@kali)-[~]
$ bg
[1] + continued firefox
(kali@kali)-[~]
$
```



Se vogliamo invece uccidere firefox basterà inserire il comando <<kill %(n. processo da killare)>> e premendo invio questo cesserà.

```
(kali@kali)-[~]
$ firefox &
[1] 37832

(kali@kali)-[~]
$ kill %1

(kali@kali)-[~]
$
[1] + terminated firefox
(kali@kali)-[~]
$
```

Per risolvere l'ultimo punto dell'esercizio (vedere spazio sta occupando sul disco) dovremo inserire il comando <<df -h>>

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

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	921M	0	921M	0%	/dev
tmpfs	198M	972K	197M	1%	/run
/dev/sda1	79G	16G	59G	21%	/
tmpfs	987M	4.0K	987M	1%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	1.0M	0	1.0M	0%	/run/credentials/systemd-journald.service
tmpfs	987M	296K	987M	1%	/tmp
tmpfs	1.0M	0	1.0M	0%	/run/credentials/getty@tty1.service
tmpfs	198M	124K	198M	1%	/run/user/1000