

I PROCESSI ATTIVI

Il comando top

ps produce un'immagine statica dei processi in corso, in pratica fotografa lo stato del sistema al momento in cui viene lanciata l'istruzione di monitoraggio delle esecuzioni.

In questa schermata possiamo osservare alcuni delle seguenti voci importanti:

- Il pid serve a indicare l'identificativo del processo.
- Lo user è colui che esegue il processo.
- Il Command è il comando eseguito dal processo.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
top - 16:56:26 up 2:39, 1 user, load average: 0,07, 0,04, 0,00  
Tasks: 151 total, 3 running, 148 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0,3 us, 0,4 sy, 0,0 ni, 99,3 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st  
MiB Mem : 3920,9 total, 2583,7 free, 613,7 used, 723,5 buff/cache  
MiB Swap: 976,0 total, 976,0 free, 0,0 used. 3145,2 avail Mem  
  
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND  
  616 root        20   0   927196 133968 56904 S   1,3   3,3   1:34.77 Xorg  
42528 kali        20   0   411288  94088  75408 S   0,7   2,3   0:00.22 qterminal  
  627 root        20   0         0         0         0 S   0,3   0,0   0:02.52 usb-storage  
  897 kali        20   0   287080  27520  19712 S   0,3   0,7   0:44.14 panel-15-genmon  
42550 kali        20   0   10424    3424    2784 R   0,3   0,1   0:00.05 top  
    1 root        20   0   165808  10648  7792 S   0,0   0,3   0:01.29 systemd  
    2 root        20   0         0         0         0 S   0,0   0,0   0:00.01 kthreadd  
    3 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 rcu_gp  
    4 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 rcu_par_gp  
    6 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 kworker/0:0H-events_highpri  
    8 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 mm_percpu_wq  
    9 root        20   0         0         0         0 S   0,0   0,0   0:00.00 rcu_tasks_rude_  
   10 root        20   0         0         0         0 S   0,0   0,0   0:00.00 rcu_tasks_trace  
   11 root        20   0         0         0         0 R   0,0   0,0   0:00.23 ksoftirqd/0  
   12 root        20   0         0         0         0 I   0,0   0,0   0:04.41 rcu_sched  
   13 root        rt    0         0         0         0 S   0,0   0,0   0:00.12 migration/0  
   15 root        20   0         0         0         0 S   0,0   0,0   0:00.00 cpuhp/0  
   16 root        20   0         0         0         0 S   0,0   0,0   0:00.00 cpuhp/1  
   17 root        rt    0         0         0         0 S   0,0   0,0   0:00.11 migration/1  
   18 root        20   0         0         0         0 S   0,0   0,0   0:00.03 ksoftirqd/1  
   20 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 kworker/1:0H-events_highpri  
   21 root        20   0         0         0         0 S   0,0   0,0   0:00.00 cpuhp/2  
   22 root        rt    0         0         0         0 S   0,0   0,0   0:00.11 migration/2  
   23 root        20   0         0         0         0 S   0,0   0,0   0:00.09 ksoftirqd/2  
   25 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 kworker/2:0H-events_highpri  
   26 root        20   0         0         0         0 S   0,0   0,0   0:00.00 cpuhp/3  
   27 root        rt    0         0         0         0 S   0,0   0,0   0:00.11 migration/3  
   28 root        20   0         0         0         0 S   0,0   0,0   0:00.05 ksoftirqd/3  
   30 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 kworker/3:0H-events_highpri  
   32 root        20   0         0         0         0 S   0,0   0,0   0:00.00 kdevtmpfs  
   33 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 netns  
   34 root         0 -20         0         0         0 I   0,0   0,0   0:00.00 inet_frag_wq
```

Per monitorare più nello specifico i processi attivi sul nostro Kali Linux sia per il root sia per utente Kali, occorre digitare i seguenti comandi:

“ps aux | grep root” “ps aux | grep kali”

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
$ ps aux | grep root  
root    1  0.0  0.2 165808 10648 ?        Ss   14:16   0:00 /sbin/init splash  
root    2  0.0  0.0 0          0  0 ?        S    14:16   0:00 [kthreadd]  
root    3  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [rcu_gp]  
root    4  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [rcu_par_gp]  
root    6  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kworker/0:0H-events_highpri]  
root    8  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [mm_percpu_wq]  
root    9  0.0  0.0 0          0  0 ?        S    14:16   0:00 [rcu_tasks_rude_]  
root   10  0.0  0.0 0          0  0 ?        S    14:16   0:00 [rcu_tasks_trace]  
root   11  0.0  0.0 0          0  0 ?        S    14:16   0:00 [ksoftirqd/0]  
root   12  0.0  0.0 0          0  0 ?        I    14:16   0:02 [rcu_sched]  
root   13  0.0  0.0 0          0  0 ?        S    14:16   0:00 [migration/0]  
root   15  0.0  0.0 0          0  0 ?        S    14:16   0:00 [cpuhp/0]  
root   16  0.0  0.0 0          0  0 ?        S    14:16   0:00 [cpuhp/1]  
root   17  0.0  0.0 0          0  0 ?        S    14:16   0:00 [migration/1]  
root   18  0.0  0.0 0          0  0 ?        S    14:16   0:00 [ksoftirqd/1]  
root   20  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kworker/1:0H-events_highpri]  
root   21  0.0  0.0 0          0  0 ?        S    14:16   0:00 [cpuhp/2]  
root   22  0.0  0.0 0          0  0 ?        S    14:16   0:00 [migration/2]  
root   23  0.0  0.0 0          0  0 ?        S    14:16   0:00 [ksoftirqd/2]  
root   25  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kworker/2:0H-events_highpri]  
root   26  0.0  0.0 0          0  0 ?        S    14:16   0:00 [cpuhp/3]  
root   27  0.0  0.0 0          0  0 ?        S    14:16   0:00 [migration/3]  
root   28  0.0  0.0 0          0  0 ?        S    14:16   0:00 [ksoftirqd/3]  
root   30  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kworker/3:0H-events_highpri]  
root   32  0.0  0.0 0          0  0 ?        S    14:16   0:00 [kdevtmpfs]  
root   33  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [netns]  
root   34  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [inet_frag_wq]  
root   37  0.0  0.0 0          0  0 ?        I    14:16   0:00 [kworker/2:1-events]  
root   38  0.0  0.0 0          0  0 ?        S    14:16   0:00 [kauditd]  
root   39  0.0  0.0 0          0  0 ?        S    14:16   0:00 [khungtaskd]  
root   40  0.0  0.0 0          0  0 ?        S    14:16   0:00 [oom_reaper]  
root   41  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [writeback]  
root   42  0.0  0.0 0          0  0 ?        S    14:16   0:00 [kcompactd0]  
root   43  0.0  0.0 0          0  0 ?        SN   14:16   0:00 [ksmd]  
root   44  0.0  0.0 0          0  0 ?        SN   14:16   0:00 [khugepaged]  
root   45  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kintegrityd]  
root   46  0.0  0.0 0          0  0 ?        I<   14:16   0:00 [kblockd]
```

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
$ ps aux | grep kali  
kali    733  0.0  0.2 17236  9536 ?        Ss   14:16   0:00 /lib/systemd/systemd --user  
kali    734  0.0  0.1 169820  4748 ?        S    14:16   0:00 (sd-pam)  
kali    749  0.0  0.3 51492 12948 ?        S<sl 14:16   0:00 /usr/bin/pipewire  
kali    750  0.0  0.6 148368 25800 ?        Ssl  14:16   0:01 /usr/bin/pipewire-media-session  
kali    751  0.0  0.7 622916 31108 ?        S<sl 14:16   0:00 /usr/bin/pulseaudio --daemonize=no --log-target=jo  
urnal  
kali    752  0.0  1.0 286836 41780 ?        Ssl  14:16   0:00 xfce4-session  
kali    756  0.0  0.1  9764  4876 ?        Ss   14:16   0:02 /usr/bin/dbus-daemon --session --address=systemd:  
--nofork --nopidfile --systemd-activation --syslog-only  
kali    802  0.0  0.0  5824  460 ?        Ss   14:16   0:00 /usr/bin/ssh-agent x-session-manager  
kali    812  0.0  0.2 310788  9512 ?        Ssl  14:16   0:00 /usr/libexec/at-spi-bus-launcher  
kali    818  0.0  0.1  9580  4296 ?        S    14:16   0:00 /usr/bin/dbus-daemon --config-file=/usr/share/defa  
ults/at-spi2/accessibility.conf --nofork --print-address 11  
kali    822  0.0  0.1 231788  5440 ?        SL   14:16   0:00 /usr/lib/aarch64-linux-gnu/xfce4/xfconf/xfconfd  
kali    828  0.0  0.1 164196  7400 ?        SL   14:16   0:00 /usr/libexec/at-spi2-registrd --use-gnome-session  
kali    838  0.0  0.0  81028  1392 ?        SLs  14:16   0:00 /usr/bin/gpg-agent --supervised  
kali    840  0.1  2.6 1156428 105816 ?       SL   14:16   0:08 xfwm4 --display :0.0 --sm-client-id 20d409fd5-e307  
-4b00-bad5-38f36b3952ff  
kali    843  0.0  0.2 239208  9344 ?        Ssl  14:16   0:00 /usr/libexec/gvfsd  
kali    848  0.0  0.1 381960  7440 ?        SL   14:16   0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f  
kali    870  0.0  0.6 233328 26456 ?        SL   14:16   0:00 xfsettingsd --display :0.0 --sm-client-id 29265e92  
e-af57-4ed9-8984-455f19908d32  
kali    881  0.0  1.5 494316 61520 ?        SL   14:16   0:03 xfce4-panel --display :0.0 --sm-client-id 274095d3  
0-fc84-42cc-a30a-25d360b8b72c  
kali    885  0.0  0.6 344088 26164 ?        SL   14:16   0:00 Thunar --sm-client-id 2c735fa89-ed6e-4ef0-8692-aef  
cd2ee5877 --daemon  
kali    890  0.0  1.7 493284 68820 ?        SL   14:16   0:02 xfdesktop --display :0.0 --sm-client-id 2a8f66b78-  
e4e4-438e-b03b-da8855a97dc7  
kali    893  0.0  1.0 467144 43224 ?        SL   14:16   0:00 /usr/lib/aarch64-linux-gnu/xfce4/panel/wrapper-2.0  
/usr/lib/aarch64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 16777223 whiskermenu Menu Whisker Mostra un menu  
per accedere facilmente alle applicazioni installate  
kali    896  0.0  0.6 343068 26588 ?        SL   14:16   0:00 /usr/lib/aarch64-linux-gnu/xfce4/panel/wrapper-2.0  
/usr/lib/aarch64-linux-gnu/xfce4/panel/plugins/libsystray.so 14 16777225 systray Componente aggiuntivo del vassoio d  
elle notifiche Fornisce gli elementi di notifica dello stato (gli indicatori dell'applicazione) e gli elementi del va  
ssodio di sistema classico  
kali    897  0.4  0.6 287080 27336 ?        SL   14:16   0:27 /usr/lib/aarch64-linux-gnu/xfce4/panel/wrapper-2.0  
/usr/lib/aarch64-linux-gnu/xfce4/panel/plugins/libgenmon.so 15 16777226 genmon Monitor generico Mostra l'output di u
```

Ora procediamo alla creazione della cartella “epicode_lab” e file di testo “esercizio.txt”.
Innanzitutto collegarsi al desktop tramite comando “cd desktop” e una volta fatto ciò digitare comando “touch esercito.txt”

```
kali@Kali: ~/desktop/epicode_lab
File Azioni Modifica Visualizza Aiuto
(kali@Kali)-[~]
$ cd desktop/
(kali@Kali)-[~/desktop]
$ mkdir epicode_lab
mkdir: impossibile creare la directory "epicode_lab": File già esistente
(kali@Kali)-[~/desktop]
$ /home/kali/desktop
(kali@Kali)-[~/desktop]
$ epicode_lab
(kali@Kali)-[~/desktop/epicode_lab]
$ touch esercizio.txt
(kali@Kali)-[~/desktop/epicode_lab]
$ touch esercizio.txt
(kali@Kali)-[~/desktop/epicode_lab]
$
```

Per apportare modifiche all'interno digitare comando "nano"

```
kali@Kali: ~/desktop/epicode_lab
File Azioni Modifica Visualizza Aiuto
GNU nano 6.2 /desktop/epicode_lab *
esercizio.txt

Save modified buffer?
S Si
N No      C Annulla
```

Fatto ciò possiamo controllare che il file sia presente su Kali.

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
$ cat esercizio.txt  
epicode_lab  
~  
$ ls  
cartella Documenti esercizio.txt Immagini Modelli nano.43192.save Scaricati Video  
desktop epicode_lab esercizio.txt IP.pcapng Musica Pubblici Scrivania Wireshark.pcapng  
~  
$ la  
.bash_logout Documenti .gnupg Musica Wireshark.pcapng  
.bashrc epicode_lab .ICEauthority nano.43192.save .Xauthority  
.bashrc.original esercizio.txt Immagini .profile .xsession-errors  
.cache .esercizio.txt.swp IP.pcapng Pubblici .xsession-errors.old  
cartella esercizio.txt .java Scaricati .zsh_history  
.config .esercizio.txt.swp .local Scrivania .zshrc  
desktop .face Modelli sudo_as_admin_successful  
.dmrc .face.icon .mozilla Video  
~  
$
```

Ora procediamo alla creazione di un nuovo user tramite comando “useradd” e nome utente.

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
$ sudo useradd  
[sudo] password di kali:  
Usage: useradd [options] LOGIN  
useradd -D  
useradd -D [options]  
  
Options:  
--badnames do not check for bad names  
-b, --base-dir BASE_DIR base directory for the home directory of the new account  
--btrfs-subvolume-home use BTRFS subvolume for home directory  
-c, --comment COMMENT GECOS field of the new account  
-d, --home-dir HOME_DIR home directory of the new account  
-D, --defaults print or change default useradd configuration  
-e, --expiredate EXPIRE_DATE expiration date of the new account  
-f, --inactive INACTIVE password inactivity period of the new account  
-g, --gid GROUP name or ID of the primary group of the new account  
-G, --groups GROUPS list of supplementary groups of the new account  
-h, --help display this help message and exit  
-k, --skel SKEL_DIR use this alternative skeleton directory  
-K, --key KEY=VALUE override /etc/login.defs defaults  
-l, --no-log-init do not add the user to the lastlog and faillog databases  
-m, --create-home create the user's home directory  
-M, --no-create-home do not create the user's home directory  
-N, --no-user-group do not create a group with the same name as the user  
-o, --non-unique allow to create users with duplicate (non-unique) UID  
-p, --password PASSWORD encrypted password of the new account  
-r, --system create a system account  
-R, --root CHROOT_DIR directory to chroot into  
-P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files  
-s, --shell SHELL login shell of the new account  
-u, --uid UID user ID of the new account  
-U, --user-group create a group with the same name as the user
```

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
esercizio.txt  
(kali@Kali)~  
$ sudo useradd fabio  
[sudo] password di kali:  
  
(kali@Kali)~  
$ whoami  
kali  
  
(kali@Kali)~  
$ sudo useradd fabio  
useradd: user 'fabio' already exists  
  
(kali@Kali)~  
$
```

```
kali@Kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@Kali)~  
$ whoami  
kali  
  
(kali@Kali)~  
$ su fabio  
Password:  
$ whoami  
fabio  
$
```

```
(kali@Kali)~  
$ top -u fabio  
top - 17:27:24 up 3:10, 1 user, load average: 0,08, 0,02, 0,01  
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0,8 us, 0,5 sy, 0,0 ni, 98,7 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st  
MiB Mem : 3920,9 total, 2529,5 free, 656,3 used, 735,0 buff/cache  
MiB Swap: 976,0 total, 976,0 free, 0,0 used. 3097,6 avail Mem  


| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|-----|------|----|----|------|-----|-----|---|------|------|-------|---------|
|-----|------|----|----|------|-----|-----|---|------|------|-------|---------|


```

Con comando `ls -la` è possibile vedere tutti i permessi che gli utenti possiedono.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
(kali@kali)-[~]  
$ ls -la  
totale 692  
drwxr-xr-x 19 kali kali 4096 2 nov 17.28 .  
drwxr-xr-x 3 root root 4096 24 ott 18.00 ..  
-rw-r--r-- 1 kali kali 220 24 ott 18.00 .bash_logout  
-rw-r--r-- 1 kali kali 5551 24 ott 18.00 .bashrc  
-rw-r--r-- 1 kali kali 3526 24 ott 18.00 .bashrc.original  
drwxr-xr-x 11 kali kali 4096 27 ott 17.47 .cache  
drwxr-xr-x 2 kali kali 4096 2 nov 16.08 cartella  
drwxr-xr-x 14 kali kali 4096 2 nov 16.12 .config  
drwxr-xr-x 4 kali kali 4096 2 nov 16.45 desktop  
-rw-r--r-- 1 kali kali 35 24 ott 18.13 .dmrc  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Documenti  
drwxr-xr-x 2 kali kali 4096 2 nov 15.36 epicode_lab  
-rw-r--r-- 1 kali kali 12 2 nov 17.00 esercizio.txt  
-rw-r--r-- 1 kali kali 1024 2 nov 17.00 .esercizio.txt.swp  
-rw-r--r-- 1 kali kali 12 2 nov 17.04 esercizio.txt  
-rw-r--r-- 1 kali kali 1024 2 nov 17.04 .esercizio.txt.swp  
-rw-r--r-- 1 kali kali 11759 24 ott 18.00 .face  
lrwxrwxrwx 1 kali kali 5 24 ott 18.00 .face.icon -> .face  
drwx----- 3 kali kali 4096 24 ott 18.13 .gnupg  
-rw----- 1 kali kali 0 24 ott 18.13 .ICEauthority  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Immagini  
-rw----- 1 kali kali 450088 28 ott 17.45 IP.pcapng  
drwxr-xr-x 3 kali kali 4096 24 ott 18.00 .java  
drwxr-xr-x 4 kali kali 4096 24 ott 18.13 .local  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Modelli  
drwx----- 5 kali kali 4096 27 ott 15.31 .mozilla  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Musica  
-rw----- 1 kali kali 14 2 nov 16.59 nano.43192.save  
-rw-r--r-- 1 kali kali 807 24 ott 18.00 .profile  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Pubblici  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Scaricati  
-rw-r--r-- 1 kali kali 0 27 ott 15.59 .sudo_as_admin_successful  
drwxr-xr-x 2 kali kali 4096 24 ott 18.13 Video  
-rw----- 1 kali kali 0 2 nov 17.13 .viminfo  
-rw----- 1 kali kali 72764 27 ott 17.47 Wireshark.pcapng
```

Per procedere all'eliminazione dell'utente creato inserire comando "sudo userdel e nome user"

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
(kali@kali)-[~]  
$ sudo userdel fabio  
[sudo] password di kali:  
(kali@kali)-[~]  
$ su fabio  
su: user fabio does not exist or the user entry does not contain all the required fields  
(kali@kali)-[~]  
$
```

FINE