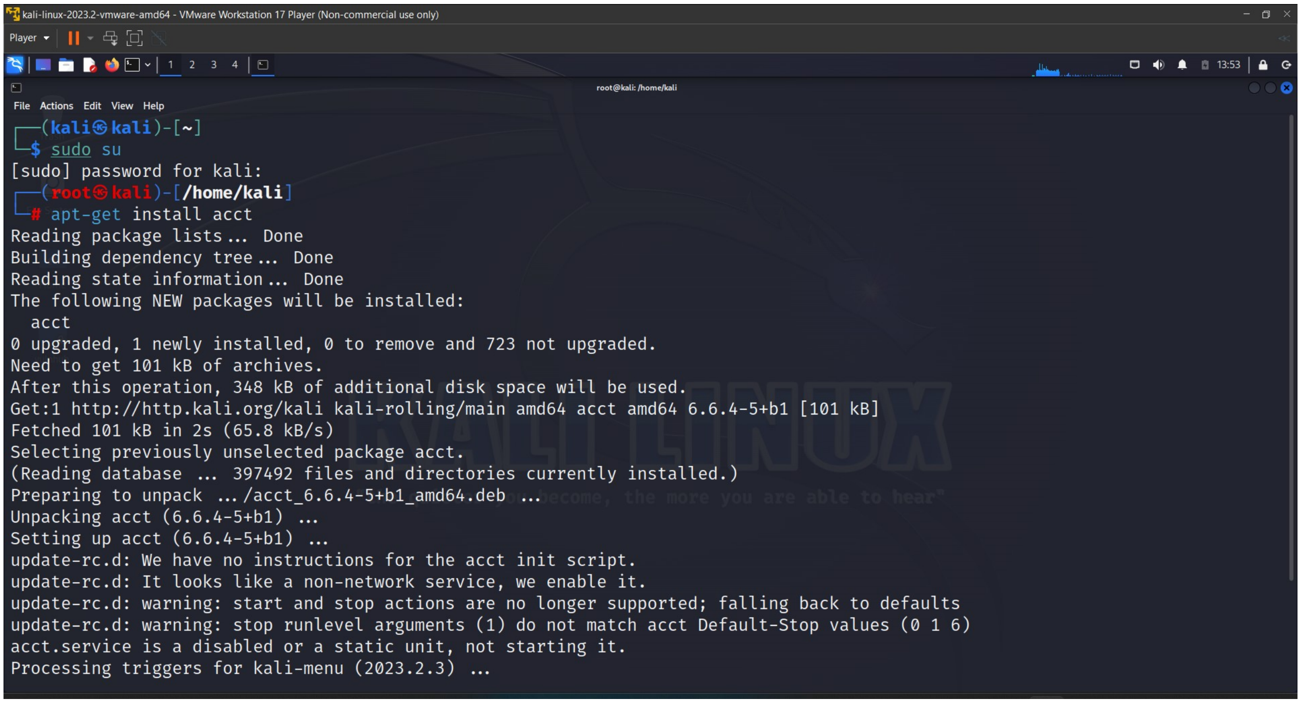
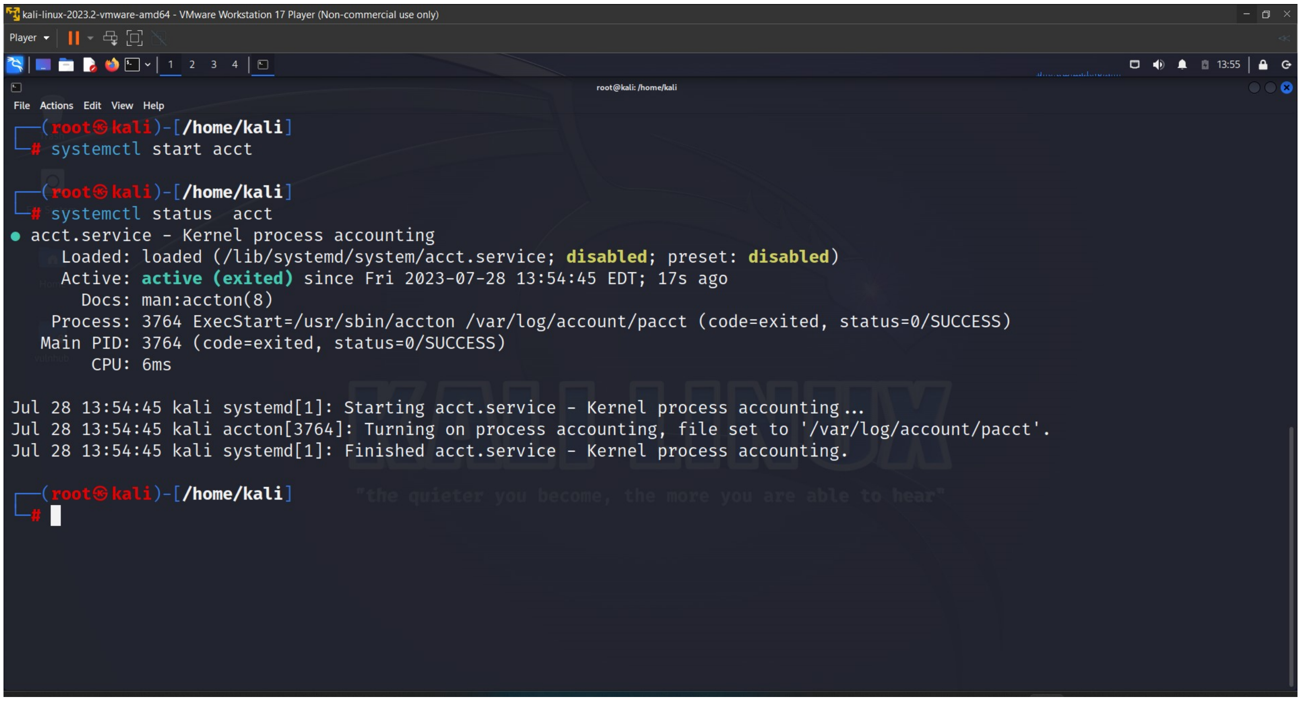
instalacion de la herramienta


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
13:53
root@kali: /home/kali
File Actions Edit View Help

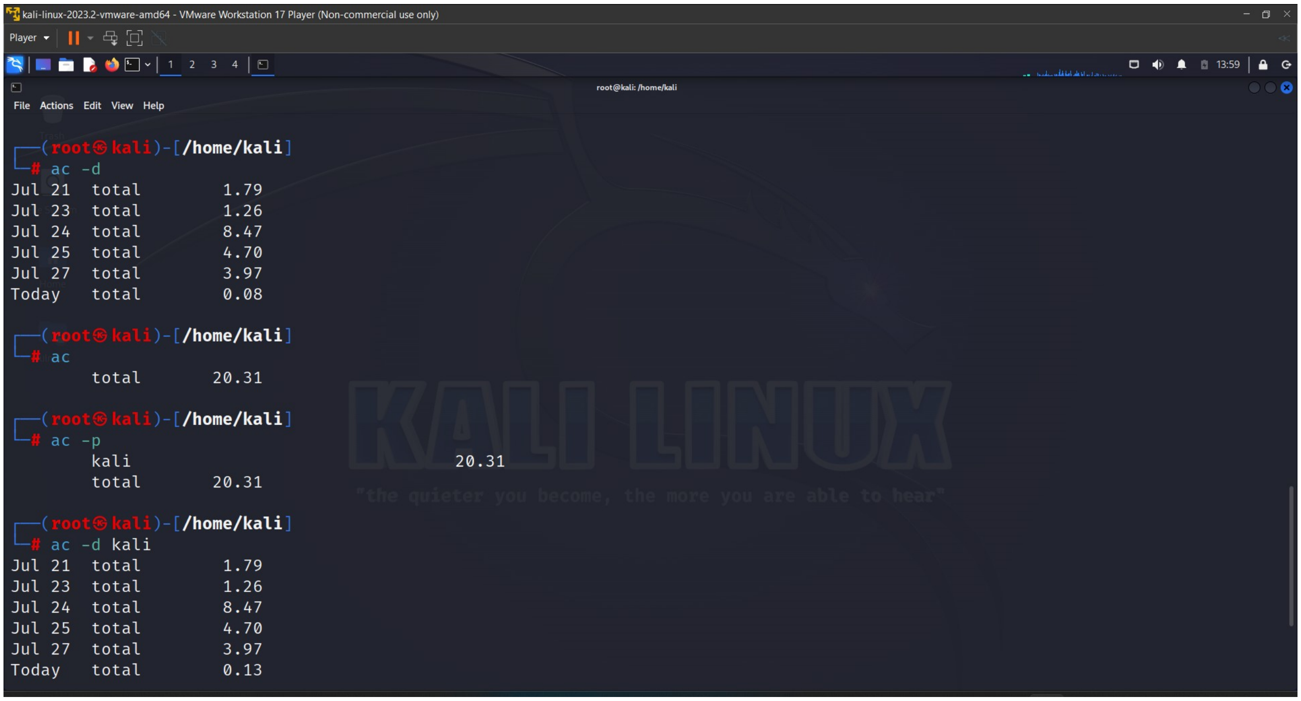
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# apt-get install acct
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  acct
0 upgraded, 1 newly installed, 0 to remove and 723 not upgraded.
Need to get 101 kB of archives.
After this operation, 348 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 acct amd64 6.6.4-5+b1 [101 kB]
Fetched 101 kB in 2s (65.8 kB/s)
Selecting previously unselected package acct.
(Reading database ... 397492 files and directories currently installed.)
Preparing to unpack .../acct_6.6.4-5+b1_amd64.deb ...
Unpacking acct (6.6.4-5+b1) ...
Setting up acct (6.6.4-5+b1) ...
update-rc.d: We have no instructions for the acct init script.
update-rc.d: It looks like a non-network service, we enable it.
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
update-rc.d: warning: stop runlevel arguments (1) do not match acct Default-Stop values (0 1 6)
acct.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2023.2.3) ...
```

la activamos y vemos el status


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
13:55
root@kali: /home/kali
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

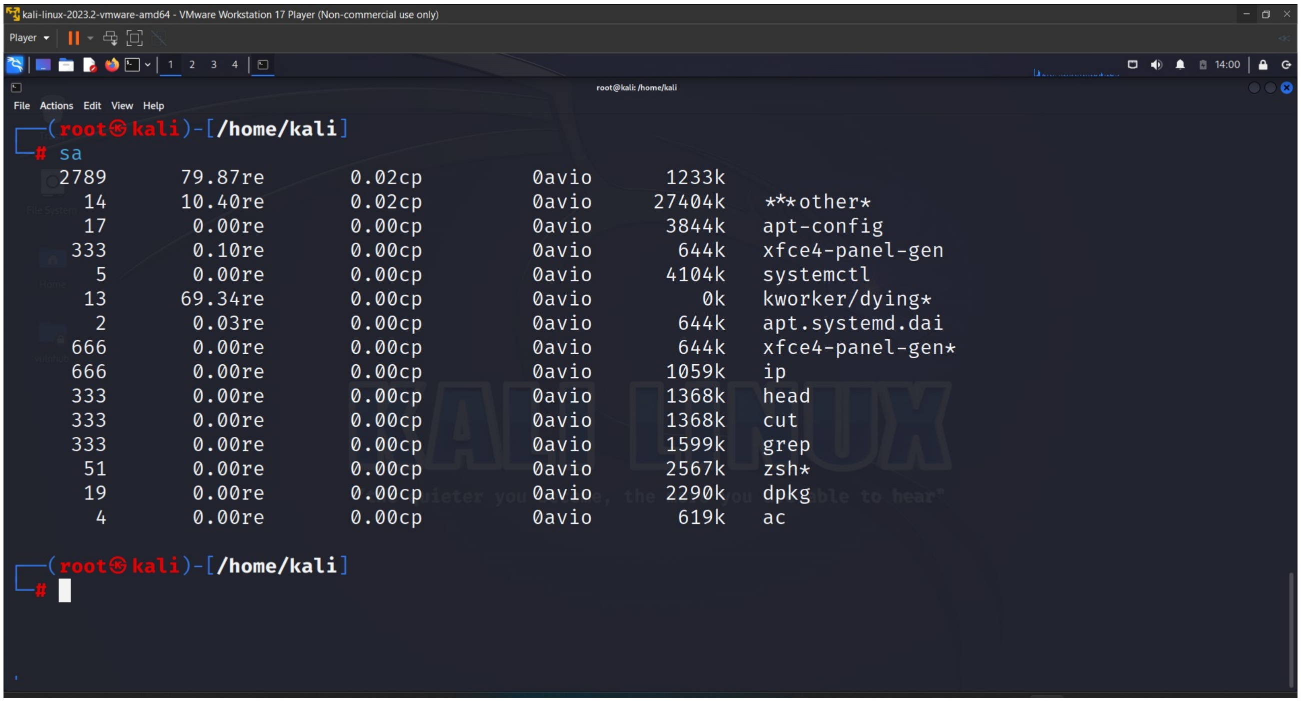
```
┌──(root㉿kali)-[/home/kali]
└─# systemctl start acct

┌──(root㉿kali)-[/home/kali]
└─# systemctl status  acct
● acct.service - Kernel process accounting
     Loaded: loaded (/lib/systemd/system/acct.service; disabled; preset: disabled)
     Active: active (exited) since Fri 2023-07-28 13:54:45 EDT; 17s ago
       Docs: man:accton(8)
    Process: 3764 ExecStart=/usr/sbin/accton /var/log/account/pacct (code=exited, status=0/SUCCESS)
   Main PID: 3764 (code=exited, status=0/SUCCESS)
        CPU: 6ms

Jul 28 13:54:45 kali systemd[1]: Starting acct.service - Kernel process accounting...
Jul 28 13:54:45 kali accton[3764]: Turning on process accounting, file set to '/var/log/account/pacct'.
Jul 28 13:54:45 kali systemd[1]: Finished acct.service - Kernel process accounting.

┌──(root㉿kali)-[/home/kali]
└─# 
```

vemos el tiempo de logueo de los users


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
13:59
root@kali: /home/kali
File Actions Edit View Help

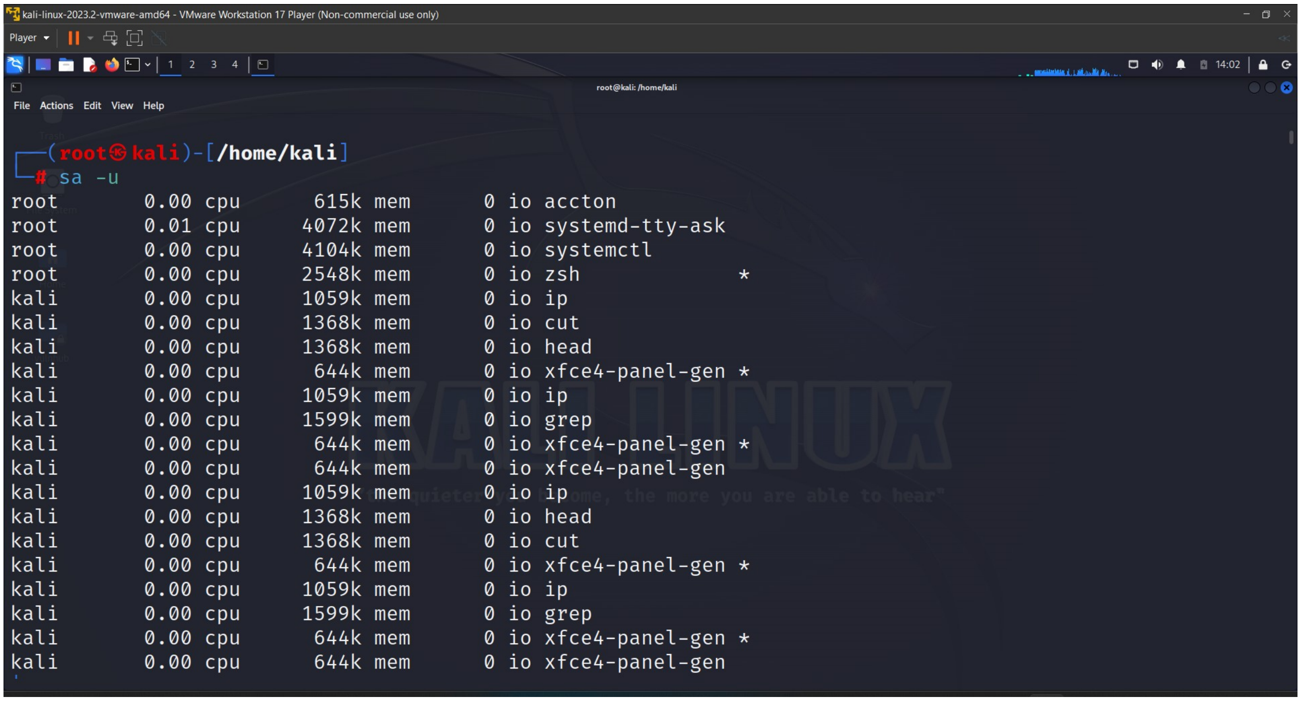
```
┌──(root㉿kali)-[/home/kali]
└─# ac -d
Jul 21  total        1.79
Jul 23  total        1.26
Jul 24  total        8.47
Jul 25  total        4.70
Jul 27  total        3.97
Today   total        0.08

┌──(root㉿kali)-[/home/kali]
└─# ac
        total       20.31

┌──(root㉿kali)-[/home/kali]
└─# ac -p
        kali                         20.31
        total       20.31

┌──(root㉿kali)-[/home/kali]
└─# ac -d kali
Jul 21  total        1.79
Jul 23  total        1.26
Jul 24  total        8.47
Jul 25  total        4.70
Jul 27  total        3.97
Today   total        0.13
```

comandos ejecutados por otros users


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
14:00
root@kali: /home/kali
File Actions Edit View Help

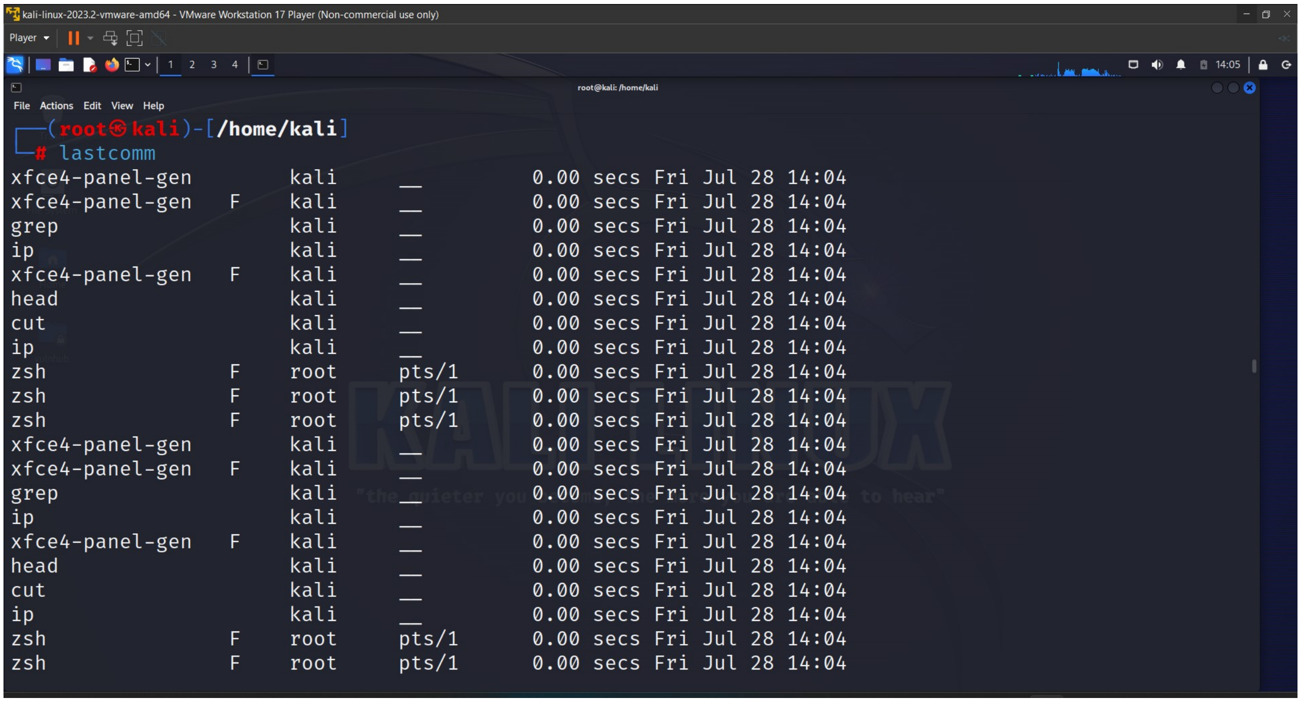
```
┌──(root㉿kali)-[/home/kali]
└─# sa
  2789      79.87re      0.02cp        0avio      1233k
    14      10.40re      0.02cp        0avio     27404k   ***other*
    17       0.00re      0.00cp        0avio      3844k   apt-config
   333       0.10re      0.00cp        0avio       644k   xfce4-panel-gen
     5       0.00re      0.00cp        0avio      4104k   systemctl
    13      69.34re      0.00cp        0avio         0k   kworker/dying*
     2       0.03re      0.00cp        0avio       644k   apt.systemd.dai
   666       0.00re      0.00cp        0avio       644k   xfce4-panel-gen*
   666       0.00re      0.00cp        0avio      1059k   ip
   333       0.00re      0.00cp        0avio      1368k   head
   333       0.00re      0.00cp        0avio      1368k   cut
   333       0.00re      0.00cp        0avio      1599k   grep
    51       0.00re      0.00cp        0avio      2567k   zsh*
    19       0.00re      0.00cp        0avio      2290k   dpkg
     4       0.00re      0.00cp        0avio       619k   ac

┌──(root㉿kali)-[/home/kali]
└─# 
```

todos lo comandos ejecutados por cualquier user del sistema


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
14:02
root@kali: /home/kali
File Actions Edit View Help

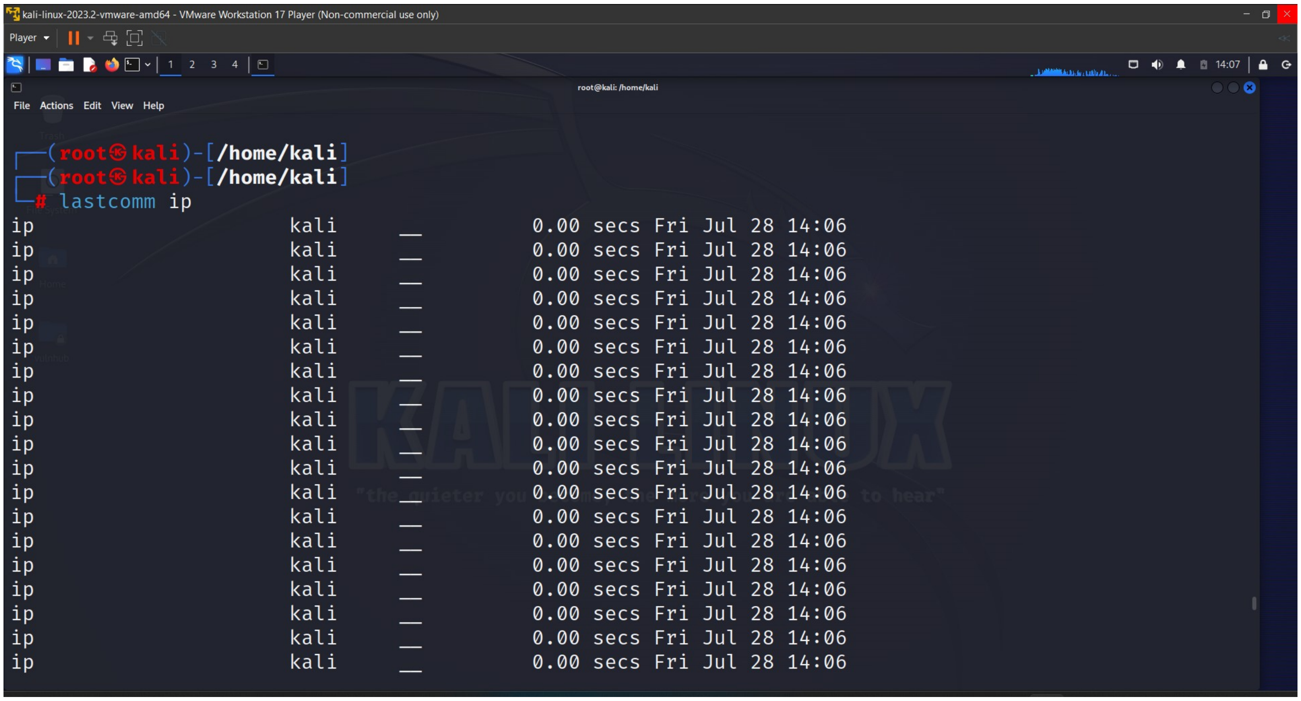
```
┌──(root㉿kali)-[/home/kali]
└─# sa -u
root       0.00 cpu     615k mem     0 io accton
root       0.01 cpu    4072k mem     0 io systemd-tty-ask
root       0.00 cpu    4104k mem     0 io systemctl
root       0.00 cpu    2548k mem     0 io zsh             *
kali       0.00 cpu    1059k mem     0 io ip
kali       0.00 cpu    1368k mem     0 io cut
kali       0.00 cpu    1368k mem     0 io head
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen *
kali       0.00 cpu    1059k mem     0 io ip
kali       0.00 cpu    1599k mem     0 io grep
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen *
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen
kali       0.00 cpu    1059k mem     0 io ip
kali       0.00 cpu    1368k mem     0 io head
kali       0.00 cpu    1368k mem     0 io cut
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen *
kali       0.00 cpu    1059k mem     0 io ip
kali       0.00 cpu    1599k mem     0 io grep
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen *
kali       0.00 cpu     644k mem     0 io xfce4-panel-gen
```

nos muestra los ultimos comandos ejecutados por cada user


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
14:05
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
└─# lastcomm
xfce4-panel-gen        kali     __          0.00 secs Fri Jul 28 14:04
xfce4-panel-gen    F   kali     __          0.00 secs Fri Jul 28 14:04
grep                   kali     __          0.00 secs Fri Jul 28 14:04
ip                     kali     __          0.00 secs Fri Jul 28 14:04
xfce4-panel-gen    F   kali     __          0.00 secs Fri Jul 28 14:04
head                   kali     __          0.00 secs Fri Jul 28 14:04
cut                    kali     __          0.00 secs Fri Jul 28 14:04
ip                     kali     __          0.00 secs Fri Jul 28 14:04
zsh                F   root     pts/1       0.00 secs Fri Jul 28 14:04
zsh                F   root     pts/1       0.00 secs Fri Jul 28 14:04
zsh                F   root     pts/1       0.00 secs Fri Jul 28 14:04
xfce4-panel-gen        kali     __          0.00 secs Fri Jul 28 14:04
xfce4-panel-gen    F   kali     __          0.00 secs Fri Jul 28 14:04
grep                   kali     __          0.00 secs Fri Jul 28 14:04
ip                     kali     __          0.00 secs Fri Jul 28 14:04
xfce4-panel-gen    F   kali     __          0.00 secs Fri Jul 28 14:04
head                   kali     __          0.00 secs Fri Jul 28 14:04
cut                    kali     __          0.00 secs Fri Jul 28 14:04
ip                     kali     __          0.00 secs Fri Jul 28 14:04
zsh                F   root     pts/1       0.00 secs Fri Jul 28 14:04
zsh                F   root     pts/1       0.00 secs Fri Jul 28 14:04
```

por ejemplo el user que uso un determinado comando en este caso ip



kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
14:07
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
┌──(root㉿kali)-[/home/kali]
└─# lastcomm ip
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
ip                     kali     __         0.00 secs Fri Jul 28 14:06
```