Sistema

Información sobre la distribución

- **cat /etc/issue**
- **lsb_release -a**
- **cat /etc/*-release**

```
kali@kali:~$ cat /etc/issue
Kali GNU/Linux Rolling \n \l
kali@kali:~$ lsb_release -a
No LSB modules are available.
Distributor ID:   Kali
Description:      Kali GNU/Linux Rolling
Release:    2023.3
Codename:   kali-rolling
kali@kali:~$ cat /etc/*-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

Información sobre el kernel

- **uname -a**
- **cat /proc/version**

```
kali@kali:~$ uname -a
Linux kali 6.5.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03)
x86_64 GNU/Linux

kali@kali:~$ cat /proc/version
Linux version 6.5.0-kali2-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-4) 13.2.0, GNU
ld (GNU Binutils for Debian) 2.41) #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-
03)
```

Hora, zona horaria y tiempo funcionamiento

- **date**
- **timedatectl**
- **uptime**

```
kali@kali:~$ date
lun 13 nov 2023 10:10:22 CET

kali@kali:~$ timedatectl
               Local time: lun 2023-11-13 10:10:35 CET
           Universal time: lun 2023-11-13 09:10:35 UTC
                 RTC time: lun 2023-11-13 09:06:50
                Time zone: Europe/Madrid (CET, +0100)
System clock synchronized: no
```

```
              NTP service: n/a
          RTC in local TZ: no

kali@kali:~$ uptime
10:10:39 up 8 min,  2 users,  load average: 0,15, 0,18, 0,13
```

- **`last reboot`** → últimos reinicios

```
kali@kali:~$ last reboot
reboot   system boot  6.5.0-kali2-amd6 Mon Nov 13 10:01   still running
reboot   system boot  6.5.0-kali2-amd6 Tue Oct 17 16:55 - 17:04  (00:08)
reboot   system boot  6.1.0-kali9-amd6 Tue Oct 17 16:34 - 16:56  (00:22)
reboot   system boot  6.1.0-kali7-amd6 Sun Jun  4 19:45 - 21:06  (01:21)
reboot   system boot  6.1.0-kali7-amd6 Tue May 30 12:44 - 12:53  (00:09)
...
```

Software instalado

- **`dpkg -l`** → listado paquetes instalados (sistemas debian/ubuntu)
- **`rpm --query --all`** → listado paquetes instalados (sistemas red hat)

```
kali@kali:~$ dpkg -l | head
Deseado=desconocido(U)/Instalar/eliminaR/Purgar/retener(H)
| Estado=No/Inst/ficheros-Conf/desempaqUetado/medio-conF/medio-inst(H)/espera-
disparo(W)/pendienTe-disparo
|/ Err?=(ninguno)/requiere-Reinst (Estado,Err: mayúsc.=malo)
||/ Nombre                                           Versión
Arquitectura Descripción
+++-==============================================-==================================-
============-
================================================================================
ii  accountsservice                                  23.13.9-4
amd64        query and manipulate user account information
ii  acl                                              2.3.1-3
amd64        access control list - utilities
ii  adduser                                          3.137
all          add and remove users and groups
ii  adwaita-icon-theme                               45.0-1
all          default icon theme of GNOME
ii  aircrack-ng                                      1:1.7-5
amd64        wireless WEP/WPA cracking utilities
...
```

Tareas programadas

- **`cat /etc/crontab`**
- **`ls -lhF /etc/cron*`**

```
kali@kali:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
```

```
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *  * * * root  cd / && run-parts --report /etc/cron.hourly
25 6  * * * root  test -x /usr/sbin/anacron || { cd / && run-parts --report
/etc/cron.daily; }
47 6  * * 7 root  test -x /usr/sbin/anacron || { cd / && run-parts --report
/etc/cron.weekly; }
52 6  1 * * root  test -x /usr/sbin/anacron || { cd / && run-parts --report
/etc/cron.monthly; }
```

Hardware

cpu

- **lscpu**
- **cat /proc/cpuinfo**

```
kali@kali:~$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         48 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  2
  On-line CPU(s) list:   0,1
Vendor ID:               AuthenticAMD
  Model name:            AMD Ryzen 7 5700U with Radeon Graphics
    CPU family:          23
    Model:               104
    Thread(s) per core:  1
    Core(s) per socket:  2
    Socket(s):           1
    Stepping:            1
    BogoMIPS:            3593,24
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush mmx fxsr sse
                          sse2 ht syscall nx mmxext fxsr_opt rdtscp lm constant_tsc
rep_good nopl nonstop_tsc cpuid e
                         xtd_apicid tsc_known_freq pni pclmulqdq ssse3 cx16 sse4_1
sse4_2 x2apic movbe popcnt aes xsa
                         ve avx rdrand hypervisor lahf_lm cmp_legacy cr8_legacy abm
sse4a misalignsse 3dnowprefetch s
                         sbd vmmcall fsgsbase avx2 rdseed clflushopt arat
Virtualization features:
  Hypervisor vendor:     KVM
  Virtualization type:   full
...
```

discos, particiones, sistema de ficheros

- **lsblk**
- **fdisk -l** → particiones
- **cat /etc/fstab** → particiones y opciones de montaje
- **df -h** → espacio usado

```
kali@kali:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
```

```
sda      8:0    0   50G  0 disk
├─sda1   8:1    0 44,7G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  5,3G  0 part [SWAP]
sr0     11:0    1 1024M  0 rom

kali@kali:~$ sudo fdisk -l
[sudo] contraseña para kali:
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x873880d9

Device     Boot    Start       End  Sectors  Size Id Type
/dev/sda1  *        2048  93749247 93747200 44,7G 83 Linux
/dev/sda2       93751294 104855551 11104258  5,3G  5 Extended
/dev/sda5       93751296 104855551 11104256  5,3G 82 Linux swap / Solaris

kali@kali:~$ cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=683485be-1136-4ba7-9a1d-35d758e08ab7 /               ext4    errors=remount-ro 0
1
# swap was on /dev/sda5 during installation
UUID=9372271c-09b4-4217-b179-84df4b9b84d6 none            swap    sw              0
0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

kali@kali:~$ df -h
S.ficheros     Tamaño Usados  Disp Uso% Montado en
udev             1,9G      0  1,9G   0% /dev
tmpfs            392M   1,1M  391M   1% /run
/dev/sda1         44G    26G   17G  62% /
tmpfs            2,0G      0  2,0G   0% /dev/shm
tmpfs            5,0M      0  5,0M   0% /run/lock
Descargas        468G   215G  254G  46% /media/sf_Descargas
tmpfs            392M   124K  392M   1% /run/user/1000
```

La gran mayoría de los sistemas Linux se amoldan al el estándar de jerarquía de archivos (FHS o *Filesystem Hierarchy Standard*), siendo los directorios más importantes son:

Directorio	Usos
/bin	contiene comandos básicos (cp, mv, ls, rm. mkdir, cat, …)
/sbin	contiene comandos de administración del sistema que generalmente los usa el administrador (fdisk, iptables, sysctl)
/etc	contiene archivos de configuración global que determinan el comportamiento del sistema para todos los usuarios
/usr/bin	contiene aplicaciones como apt, nmap, ncat, ...
/usr/share	contiene el man y ficheros de apoyo para aplicaciones
/root	Directorio personal del superusuario root

Directorio	Usos
/home	Contiene los directorios personales de los usuarios
/media	Usado como punto de montaje para discos duros y dispositivos removibles como USB, Cds, …
/mnt	Usado como punto de montaje para sistemas de archivos en red

memoria

- **free -h** o **free -m**

```
kali@kali:~$ free -h
               total        usado        libre  compartido   búf/caché   disponible
Mem:           3,8Gi       816Mi       2,8Gi       1,8Mi       464Mi       3,0Gi
Inter:         5,3Gi          0B       5,3Gi
```

Procesos

- **ps**
- **ps -ef** o **ps aux** → listar todos los procesos
- **ps -ejH** o **ps axjf** o **pstree** → listar todos los procesos en forma de árbol

```
kali@kali:~$ ps
    PID TTY          TIME CMD
   1974 pts/1    00:00:05 zsh
   2703 pts/1    00:00:00 ps

kali@kali:~$ ps -ef
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 10:01 ?        00:00:09 /sbin/init splash
root           2       0  0 10:01 ?        00:00:00 [kthreadd]
root           3       2  0 10:01 ?        00:00:00 [rcu_gp]
root           4       2  0 10:01 ?        00:00:00 [rcu_par_gp]
root           5       2  0 10:01 ?        00:00:00 [slub_flushwq]
root           6       2  0 10:01 ?        00:00:00 [netns]
root          11       2  0 10:01 ?        00:00:00 [mm_percpu_wq]
root          12       2  0 10:01 ?        00:00:00 [rcu_tasks_kthread]
...

kali@kali:~$ ps axjf
   PPID     PID    PGID     SID TTY        TPGID STAT   UID   TIME COMMAND
...
      1    1942    1942    1942 ?             -1 Ss       0   0:00 sshd: /usr/sbin/sshd
-D [listener] 0 of 10-100 sta
   1942    1955    1955    1955 ?             -1 Ss       0   0:00  \_ sshd: kali [priv]
   1955    1967    1955    1955 ?             -1 S     1000   0:00      \_ sshd:
kali@pts/1
   1967    1974    1974    1974 pts/1       2727 Ss    1000   0:06          \_ -zsh
```

- **top** o **htop** → visualización de procesos en tiempo real

```
top - 10:34:10 up 32 min,  2 users,  load average: 0,04, 0,05, 0,06
Tareas: 151 total,   1 running, 150 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,2 us,  0,2 sy,  0,0 ni, 99,5 id,  0,0 wa,  0,0 hi,  0,2 si,  0,0 st
MiB Mem :   3913,1 total,   2841,4 free,    820,9 used,    469,8 buff/cache
MiB Intercambio:   5422,0 total,   5422,0 free,      0,0 used.   3092,2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    182 root      20   0       0      0      0 I   0,3   0,0   0:00.24 kworker/1:3-events
   1275 kali      20   0  303380  28700  21404 S   0,3   0,7   0:00.41 xfsettingsd
   2775 kali      20   0   11828   5632   3456 R   0,3   0,1   0:00.13 top
      1 root      20   0   21224  12884   9556 S   0,0   0,3   0:09.18 systemd
      2 root      20   0       0      0      0 S   0,0   0,0   0:00.00 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
      5 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 netns
     11 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 mm_percpu_wq
     12 root      20   0       0      0      0 I   0,0   0,0   0:00.00 rcu_tasks_kthread
     13 root      20   0       0      0      0 I   0,0   0,0   0:00.00 rcu_tasks_rude_kthread
     14 root      20   0       0      0      0 I   0,0   0,0   0:00.00 rcu_tasks_trace_kthread
     15 root      20   0       0      0      0 S   0,0   0,0   0:00.17 ksoftirqd/0
     16 root      20   0       0      0      0 I   0,0   0,0   0:00.28 rcu_preempt
     17 root      rt   0       0      0      0 S   0,0   0,0   0:00.01 migration/0
     18 root     -51   0       0      0      0 S   0,0   0,0   0:00.00 idle_inject/0
     19 root      20   0       0      0      0 S   0,0   0,0   0:00.00 cpuhp/0
     20 root      20   0       0      0      0 S   0,0   0,0   0:00.00 cpuhp/1
     21 root     -51   0       0      0      0 S   0,0   0,0   0:00.00 idle_inject/1
     22 root      rt   0       0      0      0 S   0,0   0,0   0:00.22 migration/1
     23 root      20   0       0      0      0 S   0,0   0,0   0:00.13 ksoftirqd/1
     24 root      20   0       0      0      0 I   0,0   0,0   0:00.00 kworker/1:0-cgroup_destroy
     25 root       0 -20       0      0      0 I   0,0   0,0   0:00.00 kworker/1:0H-events_highpri
```

- gestión de procesos:
  - **`&`** → lanzar a segundo plano
  - **`CTRL+Z`** + **`bg`** → lanzar a segundo plano
  - **`fg`** → traer a primer plano
  - **`jobs`** → listar procesos en segundo plano
  - **`kill`** → matar/reiniciar procesos

Red

Interfaces/ips

- **`ip addr`**
- **`ifconfig`**
- **`cat /etc/network/interface`**s
- **`/etc/netplan/`** → ubicación archivo configuración en sistemas Ubuntu modernos

```
kali@kali:~$ ip addr
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 08:00:27:51:e0:04 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 83597sec preferred_lft 83597sec
    inet6 fe80::fb75:3897:7844:2012/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 08:00:27:c1:df:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
       valid_lft 497sec preferred_lft 497sec
    inet6 fe80::a00:27ff:fec1:dfbd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::fb75:3897:7844:2012  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:51:e0:04  txqueuelen 1000  (Ethernet)
        RX packets 34  bytes 3712 (3.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60  bytes 6394 (6.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fec1:dfbd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c1:df:bd  txqueuelen 1000  (Ethernet)
        RX packets 2808  bytes 219364 (214.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2204  bytes 842120 (822.3 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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Tabla de rutas

- **ip route**
- **route**

```
kali@kali:~$ ip route
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
192.168.56.0/24 dev eth1 proto kernel scope link src 192.168.56.102 metric 101

kali@kali:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.56.0    0.0.0.0         255.255.255.0   U     101    0        0 eth1
```

Caché ARP

- **ip neigh**
- **arp -a**

```
kali@kali:~$ ip neigh
10.0.2.3 dev eth0 lladdr 52:54:00:12:35:03 STALE
192.168.56.100 dev eth1 lladdr 08:00:27:6b:5b:37 STALE
10.0.2.2 dev eth0 lladdr 52:54:00:12:35:02 STALE
192.168.56.1 dev eth1 lladdr 0a:00:27:00:00:00 REACHABLE
kali@kali:~$ arp -a
? (10.0.2.3) at 52:54:00:12:35:03 [ether] on eth0
? (192.168.56.100) at 08:00:27:6b:5b:37 [ether] on eth1
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
ideapad5 (192.168.56.1) at 0a:00:27:00:00:00 [ether] on eth1
```

Resolución DNS

- servidores DNS:
  - **cat /etc/resolv.conf**
  - **resolvectl status**

```
kali@kali:~$ cat /etc/resolv.conf
# Generated by NetworkManager
search sanclemente.local
nameserver 10.0.2.3
```

- resolución DNS con **/etc/hosts**

```
kali@kali:~$ cat /etc/hosts
127.0.0.1   localhost
127.0.1.1   kali.kali   kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Conexiones de red

- **ss -putan**
- **netstat -putan**
- para ver los procesos (`-p`) hay que tener permisos de administrador

```
kali@kali:~$ ss -putan
Netid     State      Recv-Q     Send-Q               Local Address:Port           Peer
Address:Port      Process
udp       ESTAB      0          0              192.168.56.102%eth1:68
192.168.56.100:67
udp       ESTAB      0          0                   10.0.2.15%eth0:68
10.0.2.2:67
tcp       LISTEN     0          128                       0.0.0.0:22
0.0.0.0:*
tcp       ESTAB      0          0                   192.168.56.102:22
192.168.56.1:47922
tcp       LISTEN     0          128                          [::]:22
[::]:*

kali@kali:~$ sudo netstat -putan
Active Internet connections (servers and established)
```

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1942/sshd: /usr/sbi
tcp        0      0 192.168.56.102:22       192.168.56.1:47922      ESTABLISHED
1955/sshd: kali [pr
tcp6       0      0 :::22                   :::*                    LISTEN
1942/sshd: /usr/sbi
udp        0      0 192.168.56.102:68       192.168.56.100:67       ESTABLISHED
536/NetworkManager
udp        0      0 10.0.2.15:68            10.0.2.2:67             ESTABLISHED
536/NetworkManager
```

Usuarios

Usuario actual

- **Whoami** → usuario
- **id** → usuario y grupos

```
kali@kali:~$ whoami
kali

kali@kali:~$ id
uid=1000(kali) gid=1000(kali)
grupos=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(
video),46(plugdev),109(netdev),117(bluetooth),120(wireshark),134(scanner),142(vboxsf),14
3(kaboxer)
```

ficheros de usuarios y grupos:

- **/etc/passwd**
- **/etc/shadow**
- **/etc/group**

```
kali@kali:~$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
...
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
...

kali@kali:~$ sudo cat /etc/shadow
root:!:18931:0:99999:7:::
daemon:*:18931:0:99999:7:::
...
kali:$y$j9T$f71HpfR9pwAE3V5iGndLZB.$X2fBN44qoCt0kumA/
wGPQUfdql0Dv.TWPRIR98yXZ7C:18931:0:99999:7:::
...

kali@kali:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali,root
tty:x:5:
...
man:x:12:
```

```
proxy:x:13:
kmem:x:15:
dialout:x:20:kali,root
...
```

- **groups <nombre usuario>** → grupos a los que pertenece un usuario

```
kali@kali:~$ groups kali
kali : kali adm dialout cdrom floppy sudo audio dip video plugdev netdev bluetooth
wireshark scanner vboxsf kaboxer
```

Sesiones

- **w** → ver usuarios con sesión
- **who**
- **last** → usuarios *logueados* desde último reinicio

```
kali@kali:~$ w
 11:05:50 up  1:04,  2 users,  load average: 0,07, 0,07, 0,07
USER     TTY      DESDE            LOGIN@   IDLE   JCPU   PCPU WHAT
kali     tty7     :0               10:03    1:03m  7.80s  0.77s xfce4-session
kali     pts/1    192.168.56.1     10:05    2.00s 13.65s  0.02s w

kali@kali:~$ who
kali     tty7         2023-11-13 10:03 (:0)
kali     pts/1        2023-11-13 10:05 (192.168.56.1)

kali@kali:~$ last
kali     pts/1        192.168.56.1     Mon Nov 13 10:05   still logged in
kali     tty7         :0               Mon Nov 13 10:03   still logged in
reboot   system boot  6.5.0-kali2-amd6 Mon Nov 13 10:01   still running
...
```

sudo

- **sudo -l** → ver comandos que el usuario puede ejecutar con `sudo`

```
kali@kali:~$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on kali:
    (ALL : ALL) ALL
```

- **/etc/sudoers** → ver configuración de `sudo`

```
kali@kali:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults    use_pty
```

```
# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"
...
root  ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

Operaciones de búsqueda

- **grep**
  - **grep password documento.txt** → buscar la palabra password en el archivo documento.txt
  - **grep -rn "password" .** → búsqueda recursiva a partir del directorio actual de ficheros con la palabra password
- **find**
  - **find . -name flag1.txt** → buscar flag1.txt en directorio actual y subdirectorios
  - **find /home -name flag1.txt** → buscar flag1.txt en directorio /home y subdirectorios
  - **find / -type f -perm 0777** → buscar ficheros con permisos 777
  - **find / -type f -perm 0777 2> /dev/null** → buscar ficheros con permisos 777 redirigiendo la salida para no ver errores.