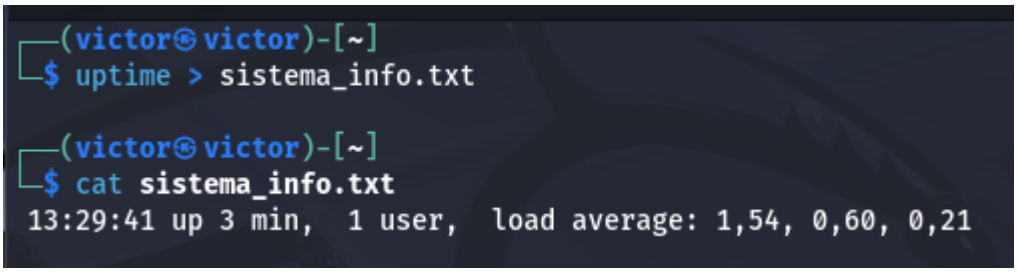
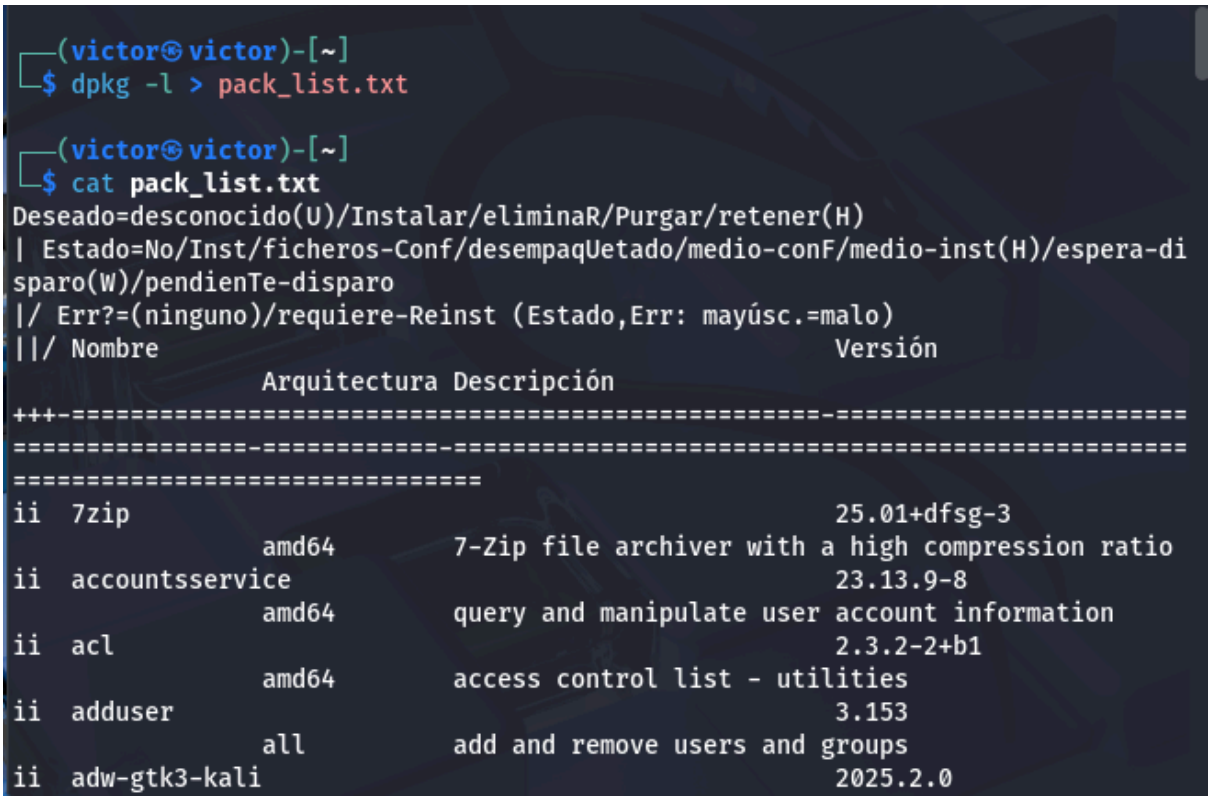
Extraer información de un sistema

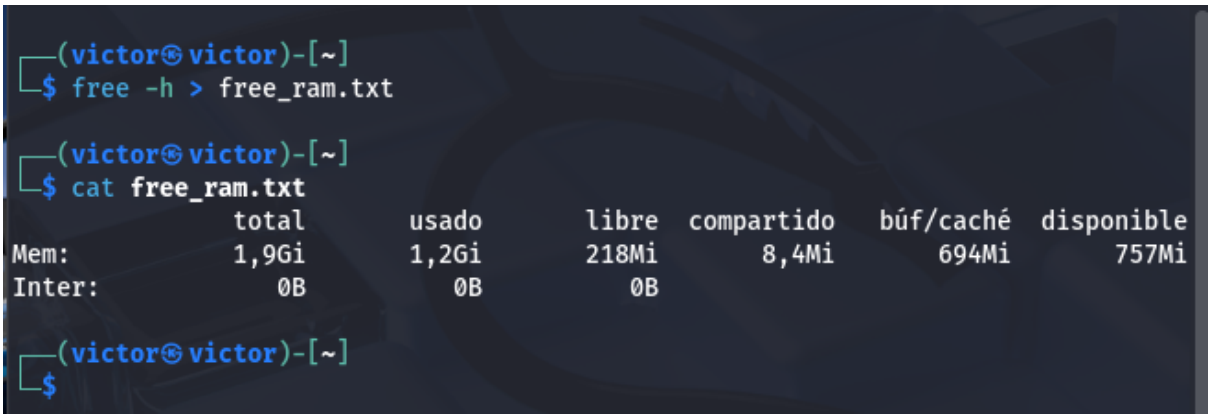
1. Verificar tiempo de actividad del sistema con uptime.



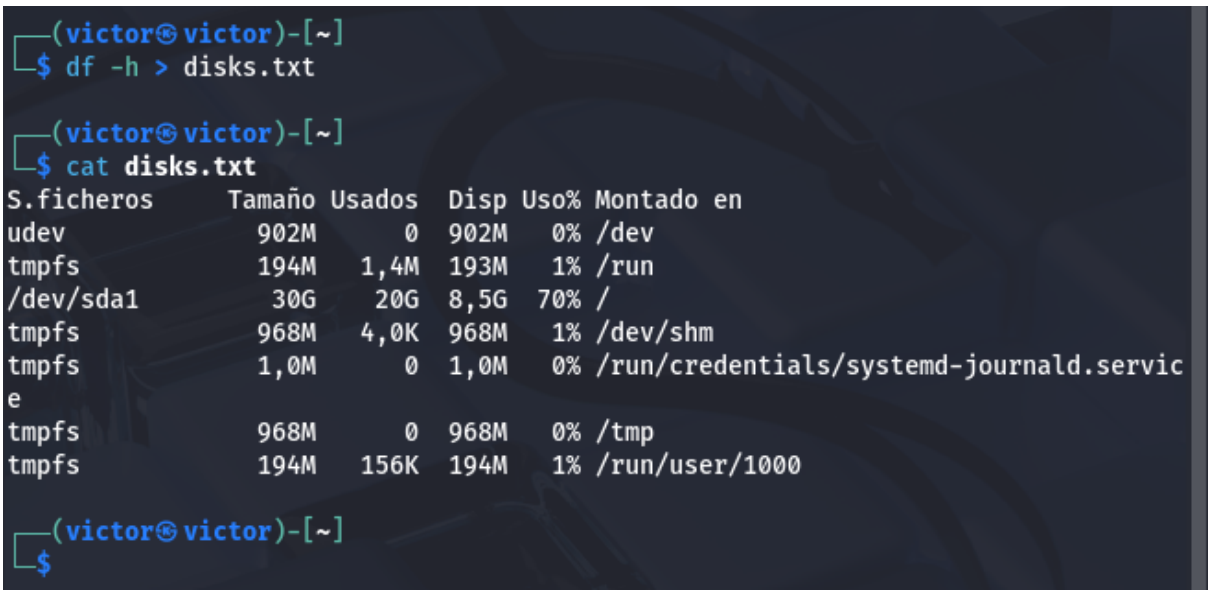
2. Listar paquetes instalados con dpkg -l.



3. Consultar cantidad de memoria RAM con free -h.



4. Verificar el uso del espacio en los sistemas de ficheros con df -h.



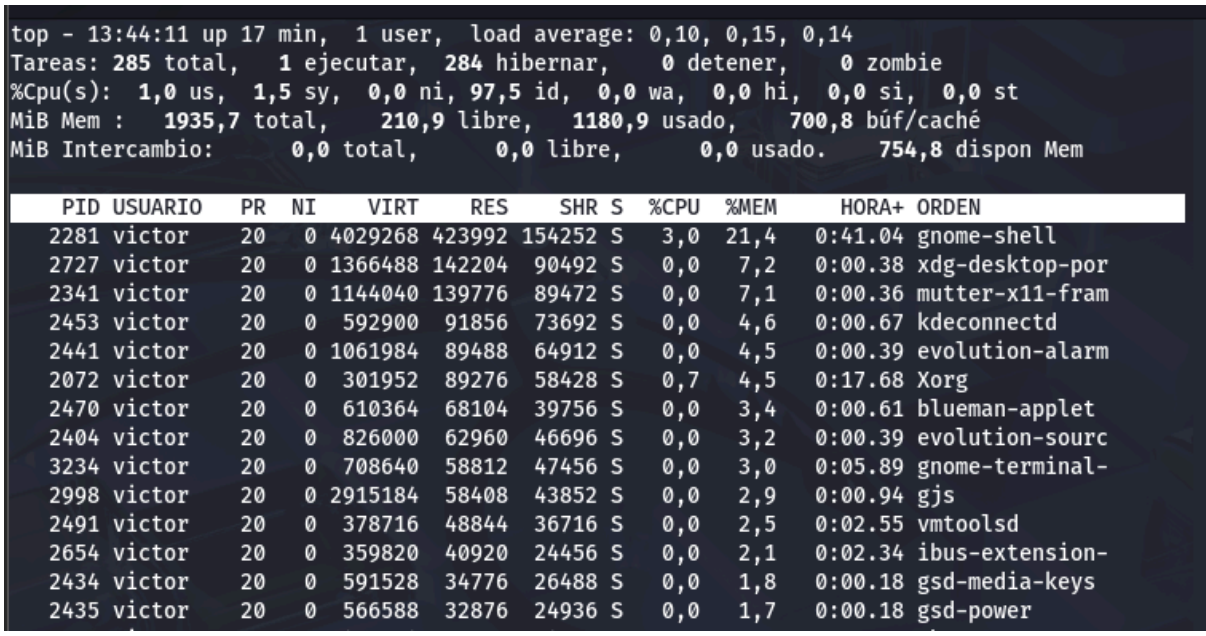
5. Obtener información detallada sobre el uso de la CPU durante 5 segundos con sar -u 1 5.

```
┌──(victor㉿victor)-[~]
└─$ sar -u 1 5 > cpu.txt

┌──(victor㉿victor)-[~]
└─$ cat cpu.txt
Linux 6.12.38+kali-amd64 (victor)       08/10/25        _x86_64_        (2 CPU)

13:38:34        CPU     %user     %nice   %system   %iowait    %steal     %idle
13:38:35        all      1,50      0,00      2,00      0,00      0,00     96,50
13:38:36        all      0,51      0,00      1,01      0,00      0,00     98,48
13:38:37        all      1,52      0,00      1,52      0,00      0,00     96,95
13:38:38        all      0,51      0,00      1,01      0,00      0,00     98,48
13:38:39        all      0,00      0,00      2,53      0,00      0,00     97,47
Media:          all      0,81      0,00      1,61      0,00      0,00     97,58

┌──(victor㉿victor)-[~]
└─$
```

6. Ver procesos en ejecución con top.
    a. Listar por uso de CPU con P.

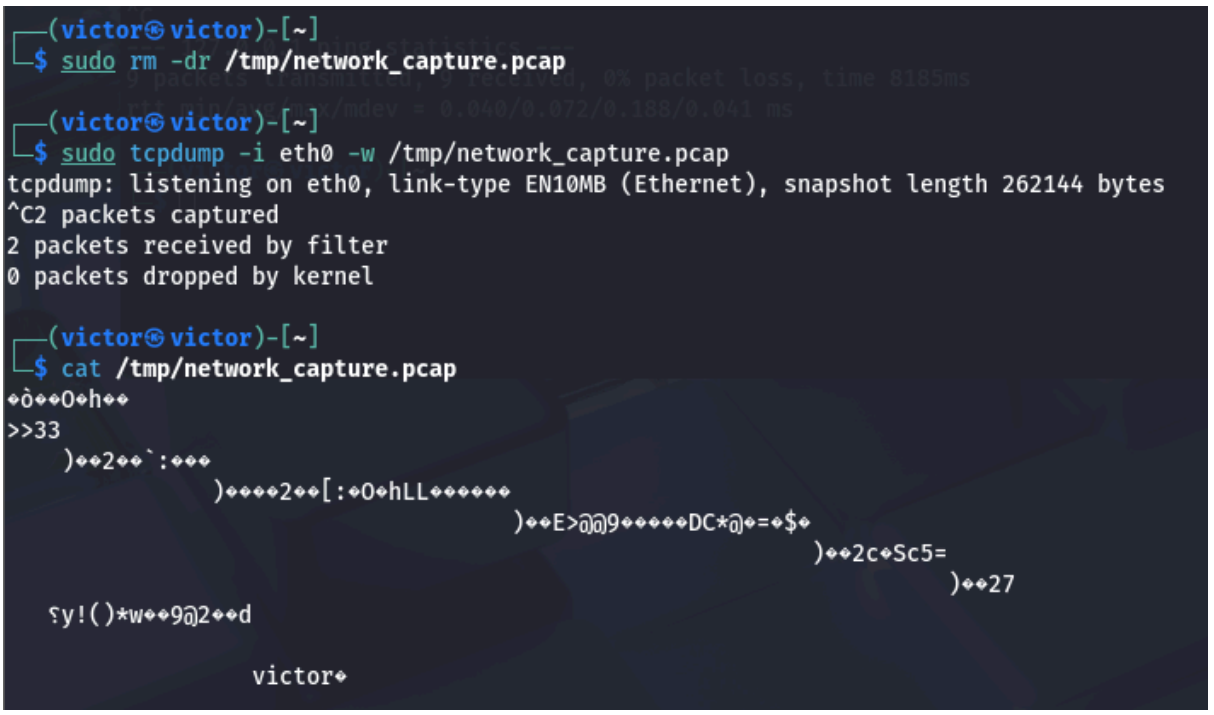
```
top - 13:43:36 up 17 min,  1 user,  load average: 0,18, 0,17, 0,14
Tareas: 287 total,   1 ejecutar,  286 hibernar,    0 detener,    0 zombie
%Cpu(s):  1,5 us,  1,9 sy,  0,0 ni, 96,6 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :   1935,7 total,    217,3 libre,   1174,6 usado,    700,7 búf/caché
MiB Intercambio:      0,0 total,      0,0 libre,      0,0 usado.    761,1 dispon Mem

    PID USUARIO    PR  NI    VIRT    RES    SHR S  %CPU  %MEM     HORA+ ORDEN
   2281 victor     20   0 4029268 423848 154252 S   2,7  21,4   0:40.26 gnome-shell
   2072 victor     20   0  301952  89276  58428 S   1,0   4,5   0:17.55 Xorg
   3234 victor     20   0  708640  58812  47456 S   0,7   3,0   0:05.86 gnome-terminal-
      9 root       20   0       0      0      0 I   0,3   0,0   0:00.80 kworker/0:0-mpt_pol+
     18 root       20   0       0      0      0 I   0,3   0,0   0:00.38 rcu_preempt
    403 root       20   0       0      0      0 I   0,3   0,0   0:00.11 kworker/u513:28-eve+
    997 root       20   0  114088   9944   8536 S   0,3   0,5   0:02.34 vmtoolsd
   1109 root       20   0  337320  19880  16808 S   0,3   1,0   0:00.21 NetworkManager
   2491 victor     20   0  377924  47948  36716 S   0,3   2,4   0:02.45 vmtoolsd
   2998 victor     20   0 2915184  58664  43852 S   0,3   3,0   0:00.92 gjs
   8976 victor     20   0   10688   5856   3680 R   0,3   0,3   0:00.03 top
   8995 root       20   0  313920   8972   7948 S   0,3   0,5   0:00.01 nm-dispatcher
```

b. Listar por uso de RAM con M.



```
top - 13:44:11 up 17 min,  1 user,  load average: 0,10, 0,15, 0,14
Tareas: 285 total,   1 ejecutar,  284 hibernar,    0 detener,    0 zombie
%Cpu(s):  1,0 us,  1,5 sy,  0,0 ni, 97,5 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :   1935,7 total,    210,9 libre,   1180,9 usado,    700,8 búf/caché
MiB Intercambio:      0,0 total,      0,0 libre,      0,0 usado.    754,8 dispon Mem

    PID USUARIO    PR  NI    VIRT    RES    SHR S  %CPU  %MEM     HORA+ ORDEN
   2281 victor    20   0 4029268 423992 154252 S   3,0  21,4   0:41.04 gnome-shell
   2727 victor    20   0 1366488 142204  90492 S   0,0   7,2   0:00.38 xdg-desktop-por
   2341 victor    20   0 1144040 139776  89472 S   0,0   7,1   0:00.36 mutter-x11-fram
   2453 victor    20   0  592900  91856  73692 S   0,0   4,6   0:00.67 kdeconnectd
   2441 victor    20   0 1061984  89488  64912 S   0,0   4,5   0:00.39 evolution-alarm
   2072 victor    20   0  301952  89276  58428 S   0,7   4,5   0:17.68 Xorg
   2470 victor    20   0  610364  68104  39756 S   0,0   3,4   0:00.61 blueman-applet
   2404 victor    20   0  826000  62960  46696 S   0,0   3,2   0:00.39 evolution-sourc
   3234 victor    20   0  708640  58812  47456 S   0,0   3,0   0:05.89 gnome-terminal-
   2998 victor    20   0 2915184  58408  43852 S   0,0   2,9   0:00.94 gjs
   2491 victor    20   0  378716  48844  36716 S   0,0   2,5   0:02.55 vmtoolsd
   2654 victor    20   0  359820  40920  24456 S   0,0   2,1   0:02.34 ibus-extension-
   2434 victor    20   0  591528  34776  26488 S   0,0   1,8   0:00.18 gsd-media-keys
   2435 victor    20   0  566588  32876  24936 S   0,0   1,7   0:00.18 gsd-power
```

7. Capturar trafico de red con tcdump y guardarlo en un archivo .pcap.



```
┌──(victor㉿victor)-[~]
└─$ sudo rm -dr /tmp/network_capture.pcap

┌──(victor㉿victor)-[~]
└─$ sudo tcpdump -i eth0 -w /tmp/network_capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C2 packets captured
2 packets received by filter
0 packets dropped by kernel

┌──(victor㉿victor)-[~]
└─$ cat /tmp/network_capture.pcap
◆ò◆◆O◆h◆◆
>>33
    )◆◆2◆◆`:◆◆◆
              )◆◆◆◆2◆◆[:◆O◆hLL◆◆◆◆◆◆
                                  )◆◆E>@@9◆◆◆◆◆DC*@◆=◆$◆
                                                        )◆◆2c◆Sc5=
                                                                  )◆◆27
   ʂy!()*w◆◆9@2◆◆d

                victor◆
```

8. Obtener información detallada sobre el uso de la CPU durante 5 segundos con sar -r.

```
┌──(victor㉿victor)-[~]
└─$ sar -r > swap.txt

┌──(victor㉿victor)-[~]
└─$ cat swap.txt
Linux 6.12.38+kali-amd64 (victor)       08/10/25        _x86_64_        (2 CPU)

┌──(victor㉿victor)-[~]
└─$
```

9. Obtener información detallada sobre el uso de la CPU durante 5 segundos con sar -n ALL 1 5.

```
┌──(victor㉿victor)-[~]
└─$ sar -n ALL 1 5 > net_activity.txt

┌──(victor㉿victor)-[~]
└─$ cat net_activity.txt
Linux 6.12.38+kali-amd64 (victor)       08/10/25        _x86_64_        (2 CPU)

13:56:52        IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
  %ifutil
13:56:53           lo      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00
13:56:53         eth0      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00
13:56:53         eth1      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00

13:56:52        IFACE   rxerr/s   txerr/s    coll/s  rxdrop/s  txdrop/s  txcarr/s  rxfram/s
 rxfifo/s  txfifo/s
13:56:53           lo      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00      0,00
13:56:53         eth0      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00      0,00
13:56:53         eth1      0,00      0,00      0,00      0,00      0,00      0,00      0,00
     0,00      0,00
```

Archivo conjunto:

```
┌──(victor㉿victor)-[~]
└─$ {cat uptime.txt && cat free_ram.txt && cat swap.txt && cat disks.txt && cat pack_list.txt} > sistema_info.txt

┌──(victor㉿victor)-[~]
└─$ cat sistema_info.txt
 13:58:47 up 32 min,  1 user,  load average: 0,00, 0,02, 0,05
               total        usado       libre  compartido  búf/caché  disponible
Mem:           1,9Gi       1,2Gi       218Mi       8,4Mi       694Mi       757Mi
Inter:           0B          0B          0B
Linux 6.12.38+kali-amd64 (victor)       08/10/25        _x86_64_        (2 CPU)
S.ficheros     Tamaño Usados  Disp Uso% Montado en
udev             902M      0  902M   0% /dev
tmpfs            194M   1,4M  193M   1% /run
/dev/sda1         30G    20G  8,5G  70% /
tmpfs            968M   4,0K  968M   1% /dev/shm
tmpfs            1,0M      0  1,0M   0% /run/credentials/systemd-journald.service
tmpfs            968M      0  968M   0% /tmp
tmpfs            194M   156K  194M   1% /run/user/1000
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  7zip                                        25.01+dfsg-3                             amd64        7-Zip file archiver with a high compression ratio
ii  accountsservice                             23.13.9-8                                amd64        query and manipulate user account information
ii  acl                                         2.3.2-2+b1                               amd64        access control list - utilities
ii  adduser                                     3.153                                    all          add and remove users and groups
```

Preguntas.

- ¿Cuánto tiempo lleva encendido el sistema?
  En el momento de la captura, 3 minutos.

- ¿Cuánta memoria RAM y espacio de intercambio está siendo utilizado actualmente?
  1,2 GB usados de RAM y swap sin usar.

- ¿Cuáles son las 3 aplicaciones que están usando más recursos en tu sistema?
  En el momento de la captura, la shell de gnome, Xorg, y la terminal visual de gnome en cuanto a CPU, y la shell de gnome, el entorno de escritorio, y mutter-x11-fram a nivel de RAM

- ¿Qué porcentaje de uso tiene la partición principal del sistema de ficheros?
  70%

- ¿Qué detalles interesantes encontraste en tu disco principal?
  El tamaño de cada partición o dispositivo, la ubicación de montaje, su porcentaje de uso, espacio disponible, y espacio usado.

- ¿Cuántos paquetes están instalados en tu sistema?
  3835 paquetes instalados

- Describe un paquete capturado por tcpdump y qué información es posible deducir de él.
  No es posible en esta captura, ya que los paquetes están cifrados.