

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»  
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ  
Кафедра компьютерной инженерии и моделирования

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №12**  
**«Утилиты мониторинга производительности в среде GNU/Linux»**

Практическая работа  
по дисциплине «Системное программное обеспечение»  
студента 3 курса группы ИВТ-б-о-222(1)  
Гоголева Виктора Григорьевича

09.03.01 «Направление подготовки»

Симферополь, 2025

## 1. Войти в систему под рутом

```
(kali㉿kali)-[~]  
$ sudo su  
[sudo] password for kali:  
(root㉿kali)-[/home/kali]  
#
```

## 2. Ознакомится с документацией

```
File Actions Edit View Help  
FREE(1) User Commands  
NAME  
free - Display amount of free and used memory in the system  
SYNOPSIS  
free [options]  
DESCRIPTION  
free displays the total amount of free and used physical and swap memory in the system, as well as the buffers and caches used by the kernel. The information is gathered by parsing /proc/meminfo. The display includes the following fields:  
total Total installed memory (MemTotal and SwapTotal in /proc/meminfo)  
used Used or unavailable memory (calculated as total - available)  
free Unused memory (MemFree and SwapFree in /proc/meminfo)  
shared Memory used (mostly) by tmpfs (Shmem in /proc/meminfo)  
buffers Memory used by kernel buffers (Buffers in /proc/meminfo)  
cache Memory used by the page cache and slabs (Cached and SReclaimable in /proc/meminfo)  
buff/cache Sum of buffers and cache  
available Estimation of how much memory is available for starting new applications, without swapping. Unlike the data provided by the cache or free fields, this field takes into account page cache and all reclaimable memory slabs will be reclaimed due to items being in use (MemAvailable in /proc/meminfo, available on kernels 3.14, emulated on kernels 2.6.27+, otherwise the same as free)  
OPTIONS  
-b, --bytes Display the amount of memory in bytes.  
-k, --kibi Display the amount of memory in Kibibytes. This is the default.  
-m, --mibi Display the amount of memory in mebibytes.  
-g, --gibi Display the amount of memory in gibibytes.  
--tebi Display the amount of memory in tebibytes.  
--pebi Display the amount of memory in pebibytes.  
--kilo Display the amount of memory in kilobytes. Implies --si.  
--mega Display the amount of memory in megabytes. Implies --si.  
--giga Display the amount of memory in gigabytes. Implies --si.  
Manual page free(1) line 1 (press h for help or q to quit)
```

Рисунок – документация команды free

```
File Actions Edit View Help
VMSTAT(8) System Administration

NAME
    vmstat - Report virtual memory statistics

SYNOPSIS
    vmstat [options] [delay [count]]

DESCRIPTION
    vmstat reports information about processes, memory, paging, block IO, traps, disks and cpu activity.

    The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case.

OPTIONS
    delay The delay between updates in seconds. If no delay is specified, only one report is printed with the average values since boot.

    count Number of updates. In absence of count, when delay is defined, default is infinite.

    -a, --active
        Display active and inactive memory, given a 2.5.41 kernel or better.

    -f, --forks
        The -f switch displays the number of forks since boot. This includes the fork, vfork, and clone system calls, and is equivalent to the total number of tasks created. Each process is counted once, depending on thread usage. This display does not repeat.

    -m, --slabs
        Displays slabinfo.

    -n, --one-header
        Display the header only once rather than periodically.

    -s, --stats
        Displays a table of various event counters and memory statistics. This display does not repeat.

    -d, --disk
        Report disk statistics (2.5.70 or above required).

    -D, --disk-sum
        Report some summary statistics about disk activity.

    -p, --partition device
        Detailed statistics about partition (2.5.70 or above required).

    -S, --unit character
        Switches outputs between 1000 (k), 1024 (K), 1000000 (m), or 1048576 (M) bytes. Note this does not change the swap (si/so) or block (bi/bo) fields.

    -t, --timestamp
        Append timestamp to each line

    -w, --wide
        Wide output mode (useful for systems with higher amount of memory, where the default output mode suffers from unwanted column breakage). The output is wider than 80 characters per line.

    -y, --no-first
        Omits first report with statistics since system boot.

Manual page vmstat(8) line 1 (press h for help or q to quit)
```

### Рисунок — документация команды vmstat

```

TOP(1)
User Commands

NAME
    top - display Linux processes

SYNOPSIS
    top [options]

DESCRIPTION
    The top program provides a dynamic real-time view of a running system. It can display system summary information as well as a list of processes or their summary information shown and the types, order and size of information displayed for processes are all user configurable and that configuration can be made.

    The program provides a limited interactive interface for process manipulation as well as a much more extensive interface for personal configuration -- (c) 1993 by Bill Dertouzos. Throughout this document, you are free to name the program anything you wish. That new name, possibly an alias, will then be reflected on top's display.

OVERVIEW
    Documentation
    The remaining Table of Contents

    OVERVIEW
    Operation
    Linux Memory Types
    1. COMMAND-LINE Options
    2. SUMMARY Display
        a. UPTIME and LOAD Averages
        b. TASK and CPU States
        c. MEMORY Usage
    3. FIELDS / Columns Display
        a. DESCRIPTIONS of Fields
        b. MANAGING Fields
    4. INTERACTIVE Commands
        a. GLOBAL Commands
        b. SUMMARY AREA Commands
        c. TASK AREA Commands
            1. Appearance
            2. Content
            3. Size
            4. Sorting
        d. COLOR Mapping
    5. ALTERNATE-DISPLAY Provisions
        a. WINDOWS Overview
        b. COMMANDS for Windows
        c. SCROLLING a Window
        d. SEARCHING in a Window
        e. FILTERING in a Window
    6. FILES
        a. PERSONAL Configuration File
        b. ADDING INSPECT Entries
        c. SYSTEM Configuration File
        d. SYSTEM Restrictions File
    7. ENVIRONMENT VARIABLE(S)
    8. STUPID TRICKS Sampler
        a. Kernel Magic
        b. Bouncing Windows

Manual page top(1) line 1 (press h for help or q to quit)

```

### Рисунок – документация команды top

```
HTOP(1) User Commands

NAME
  htop, pcp-htop - interactive process viewer

SYNOPSIS
  htop [-dCFhpustvH]
  pcp htop [-dCFhpustvH] [--host/~h host]

DESCRIPTION
  htop is a cross-platform ncurses-based process viewer.

  It is similar to top, but allows you to scroll vertically and horizontally, and interact using a pointing device (mouse). You can observe processes in a list view, as well as view them in a tree format, select multiple processes and act on them all at once.

  Tasks related to processes (killing, renicing) can be done without entering their PIDs.

  pcp-htop is a version of htop built using the Performance Co-Pilot (PCP) Metrics API (see PCPIntro(1), PMAPI(3)), allowing to extend htop to cover a wide range of system metrics for further details.

COMMAND-LINE OPTIONS
  Mandatory arguments to long options are mandatory for short options too.

  -d --delay=DELAY
      Delay between updates, in tenths of a second. If the delay value is less than 1, it is increased to 1, i.e. 1/10 second. If the delay value is greater than 10, it is decreased to 10.

  -C --no-color --no-colour
      Start htop in monochrome mode

  -F --filter=FILTER
      Filter processes by terms matching the commands. The terms are matched case-insensitive and as fixed strings (not regexes). You can separate multiple filter terms with spaces.

  -h --help
      Display a help message and exit

  -p --pid=PID,PID...
      Show only the given PIDs

  -s --sort-key COLUMN
      Sort by this column (use --sort-key help for a column list). This will force a list view unless you specify -t at the same time.

  -u --user=USERNAME|UID
      Show only the processes of a given user

  -U --no-unicode
      Do not use unicode but ASCII characters for graph meters

  -M --no-mouse
      Disable support of mouse control

  --readonly
      Disable all system and process changing features

  -V --version
      Display the version number and exit

Manual page htop(1) line 1 (press h for help or q to quit)
```

Рисунок - документация команды htop

```
File Actions Edit View Help
PS(1)
NAME
  ps - report a snapshot of the current processes.
SYNOPSIS
  ps [options]
DESCRIPTION
  ps displays information about a selection of the active processes. If you want a repetitive update of the selection and the displayed information, use top instead.

  This version of ps accepts several kinds of options:

  1  UNIX options, which may be grouped and must be preceded by a dash.
  2  BSD options, which may be grouped and must not be used with a dash.
  3  GNU long options, which are preceded by two dashes.

  Options of different types may be freely mixed, but conflicts can appear. There are some synonymous options, which are functionally identical, due to the many standards.

  Note that ps -aux is distinct from ps aux. The POSIX and UNIX standards require that ps -aux print all processes owned by a user named x, as well as printing all processes owned by the user named x does not exist, this ps may interpret the command as ps aux instead and print a warning. This behavior is intended to aid in transitioning old scripts to the new syntax.

  By default, ps selects all processes with the same effective user ID (euid=EUID) as the current user and associated with the same terminal as the invoker. It displays the process (tname=TTY), the cumulated CPU time in [DD-]hh:mm:ss format (time=TIME), and the executable name (ucmd=CMD). Output is unsorted by default.

  The use of BSD-style options will add process state (stat=STAT) to the default display and show the command args (args=COMMAND) instead of the executable name. You can also use the -o option to change the process selection to include processes on other terminals (TTys) that are owned by you; alternately, this may be used to filter processes to exclude processes owned by other users or not on a terminal. These effects are not considered when options are described as being "identical".

  Except as described below, process selection options are additive. The default selection is discarded, and then the selected processes are added to the set of processes that meet any of the given selection criteria.
EXAMPLES
  To see every process on the system using standard syntax:
    ps -e
    ps -ef
    ps -eF
    ps -ely

  To see every process on the system using BSD syntax:
    ps ax
    ps axu

  To print a process tree:
    ps -o jH
    ps axjf

  To get info about threads:
    ps -elf
    ps axms

  To get security info:
    ps -o selinux
Manual page ps(1) line 1 (press h for help or q to quit)
```

Рисунок – документация команды ps

```
root@kali: /home/kali
File Actions Edit View Help
DSTAT(1)
NAME
  dstat - versatile tool for generating system resource statistics
SYNOPSIS
  dstat [-afv] [options..] [delay [count]]
DESCRIPTION
  Dstat is a versatile replacement for vmstat, iostat and ifstat. Dstat overcomes some of the limitations and adds some extra features.
  Dstat allows you to view all of your system resources instantly, you can eg. compare disk usage in combination with interrupts from your IDE control
  throughput (in the same interval).
  Dstat also cleverly gives you the most detailed information in columns and clearly indicates in what magnitude and unit the output is displayed. Les
  Dstat is unique in letting you aggregate block device throughput for a certain diskset or network bandwidth for a group of interfaces, ie. you can s
  filesystem or storage system.
  Dstat allows its data to be directly written to a CSV file to be imported and used by OpenOffice, Gnumeric or Excel to create graphs.
  Note
  Users of Sleuthkit might find Sleuthkit's dstat being renamed to datastat to avoid a name conflict. See Debian bug #283709 for more information.
OPTIONS
  -c, --cpu
    enable cpu stats (system, user, idle, wait), for more CPU related stats also see --cpu-adv and --cpu-use
  -C 0,3,total
    include cpu0, cpu3 and total (when using -c/--cpu); use all to show all CPUs
  -d, --disk
    enable disk stats (read, write), for more disk related stats look into the other --disk plugins
  -D total,hda
    include total and hda (when using -d/--disk)
  -g, --page
    enable page stats (page in, page out)
  -i, --int
    enable interrupt stats
  -I 5,10
    include interrupt 5 and 10 (when using -i/--int)
  -l, --load
    enable load average stats (1 min, 5 mins, 15mins)
  -m, --mem
    enable memory stats (used, buffers, cache, free); for more memory related stats also try --mem-adv and --swap
  -n, --net
    enable network stats (receive, send)
Manual page dstat(1) line 1 (press h for help or q to quit)
```

## Документация команды dstat

```
File Actions Edit View Help
IOSTAT(1) Linux User's Manual

NAME
    iostat - Report Central Processing Unit (CPU) statistics and input/output statistics for devices and partitions.

SYNOPSIS
    iostat [ -c ] [ -d ] [ -h ] [ -k | -m ] [ -N ] [ -s ] [ -t ] [ -V ] [ -x ] [ -y ] [ -z ] [ --compact ] [ --dec={ 0 | 1 | 2 } ] [ { -f | +f } direct
    group_name ] [ --human ] [ --pretty ] [ -p [ device[, ...] | ALL ] ] [ device [ ... ] | ALL ] [ interval [ count ] ]

DESCRIPTION
    The iostat command is used for monitoring system input/output device loading by observing the time the devices are active in relation to their average t
    change system configuration to better balance the input/output load between physical disks.

    The first report generated by the iostat command provides statistics concerning the time since the system was booted, unless the -y option is used (in t
    the time since the previous report. All statistics are reported each time the iostat command is run. The report consists of a CPU header row followed by
    calculated system-wide as averages among all processors. A device header row is displayed followed by a line of statistics for each device that is confi

    The interval parameter specifies the amount of time in seconds between each report. The count parameter can be specified in conjunction with the inte
    determines the number of reports generated at interval seconds apart. If the interval parameter is specified without the count parameter, the iostat com

REPORTS
    The iostat command generates two types of reports, the CPU Utilization report and the Device Utilization report.

CPU Utilization Report
    The first report generated by the iostat command is the CPU Utilization Report. For multiprocessor systems, the CPU values are global averages an

    %user Show the percentage of CPU utilization that occurred while executing at the user level (application).

    %nice Show the percentage of CPU utilization that occurred while executing at the user level with nice priority.

    %system Show the percentage of CPU utilization that occurred while executing at the system level (kernel).

    %iowait Show the percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.

    %steal Show the percentage of time spent in involuntary wait by the virtual CPU or CPUs while the hypervisor was servicing another virtual proces

    %idle Show the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.

Device Utilization Report
    The second report generated by the iostat command is the Device Utilization Report. The device report provides statistics on a per physical devi
    tics are to be displayed may be entered on the command line. If no device nor partition is entered, then statistics are displayed for every dev
    tics for it. If the ALL keyword is given on the command line, then statistics are displayed for every device defined by the system, including th
    by default, unless the environment variable POSIXLY_CORRECT is set, in which case 512-byte blocks are used. The report may show the following fi

    Device: This column gives the device (or partition) name as listed in the /dev directory.

    tps Indicate the number of transfers per second that were issued to the device. A transfer is an I/O request to the device. Multiple logi
    transfer is of indeterminate size.

    Blk_read/s (kB_read/s, MB_read/s)
        Indicate the amount of data read from the device expressed in a number of blocks (kilobytes, megabytes) per second. Blocks are equivalent

Manual page iostat(1) line 1 (press h for help or q to quit)
```

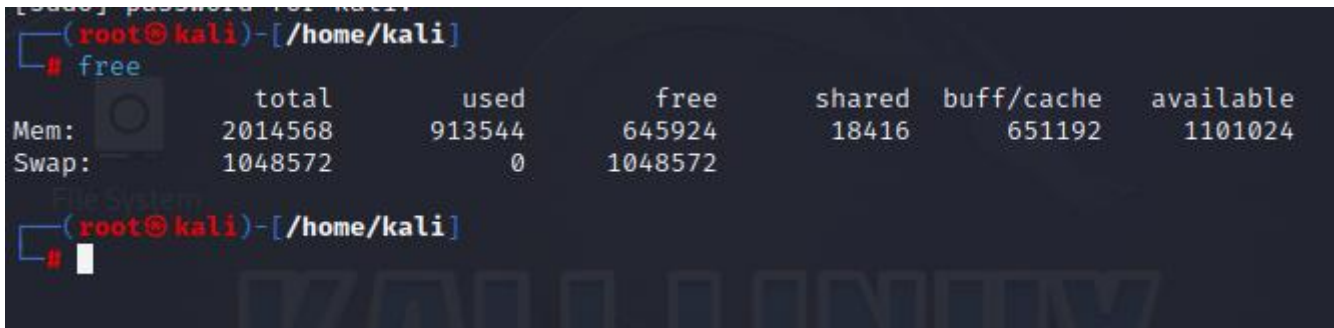
Рисунок – документация команды iostat



### 3. Запустить поочерёдно каждую утилиту

#### Free

Команда `free` в Linux используется для отображения информации о использовании оперативной памяти (RAM) на системе. Она выводит статистику по памяти в байтах и представляет ее в виде таблицы с несколькими столбцами.



```
(root@kali)-[/home/kali]
# free
Mem:              total        used        free      shared  buff/cache   available
Swap:            1048572           0      1048572           0        651192     1101024

(root@kali)-[/home/kali]
#
```

- `total` (всего): общий объем оперативной памяти в системе
- `used` (используется): количество памяти, занятой процессами, кэшем и буферами.
- `free` (свободно): количество неиспользуемой памяти, доступной для новых процессов
- `shared` (разделяемая): размер памяти, используемой разделяемыми библиотеками.
- `buff/cache` (буфер/кэш): объем памяти, используемый ядром операционной системы для буферов и кэша данных
- `available` (доступно): оценка объема памяти, доступного для новых процессов без подкачки на диск



## Vmstat

Команда `vmstat` в Linux используется для отображения статистики использования виртуальной памяти, процессора, ввода-вывода (I/O) и других системных ресурсов. Она предоставляет информацию о производительности системы в реальном времени.

```
(root@kali)-[/home/kali]
# vmstat
procs -----memory----- --swap--  --io--  -system-  --cpu--
r  b    swpd  free  buff  cache  si  so    bi    bo    in    cs  us  sy  id  wa  st
1  0        0 645924 163240 488040  0  0    35     3   387   227  0  1 99  0  0
```

### 1. Procs - информация о процессах:

- `r` - количество процессов, ожидающих выполнения (в состоянии "runnable").
- `b` - количество процессов, заблокированных, ожидающих ввода-вывода (I/O).

### 2. Memory - информация о использовании памяти:

- `swpd` - количество использованного подкачки (swap space) в килобайтах.
- `free` - количество свободной физической памяти в килобайтах.
- `buff` - количество памяти, используемой в буферах ядра в килобайтах.
- `cache` - количество памяти, используемой в кэше файловой системы в килобайтах.

### 3. Swap - информация о использовании подкачки:

- `si` - количество данных, считываемых из подкачки в секунду (swap in) в килобайтах

- so - количество данных, записываемых в подкачку в секунду (swap out) в килобайтах

4. IO - информация о вводе-выводе:

- bi - количество блоков, считываемых с блочных устройств в секунду (блок = 512 байт).
- bo - количество блоков, записываемых на блочные устройства в секунду.

5. System - информация о системных операциях:

- in - количество прерываний от устройств в секунду, обрабатываемых ядром
- cs - количество контекстных переключений (включая переключения между процессами) в секунду.

6. CPU - информация о загрузке процессора:

- us - процент времени процессора, затраченного на выполнение пользовательских процессов (user).
- sy - процент времени процессора, затраченного на выполнение системных задач ядра (system).
- id - процент времени процессора, простаивающего (idle).
- wa - процент времени процессора, затраченного на ожидание ввода-вывода (I/O wait).
- st - процент времени процессора, затраченного на выполнение виртуализованных задач (steal, если вы используете виртуализацию).

## Тор

Команда `top` в Linux используется для отображения системной информации о процессах, запущенных в системе, и их использования ресурсов, таких как ЦПУ, память и т.д. Она обновляет данные в реальном времени, что позволяет отслеживать текущую нагрузку на систему.

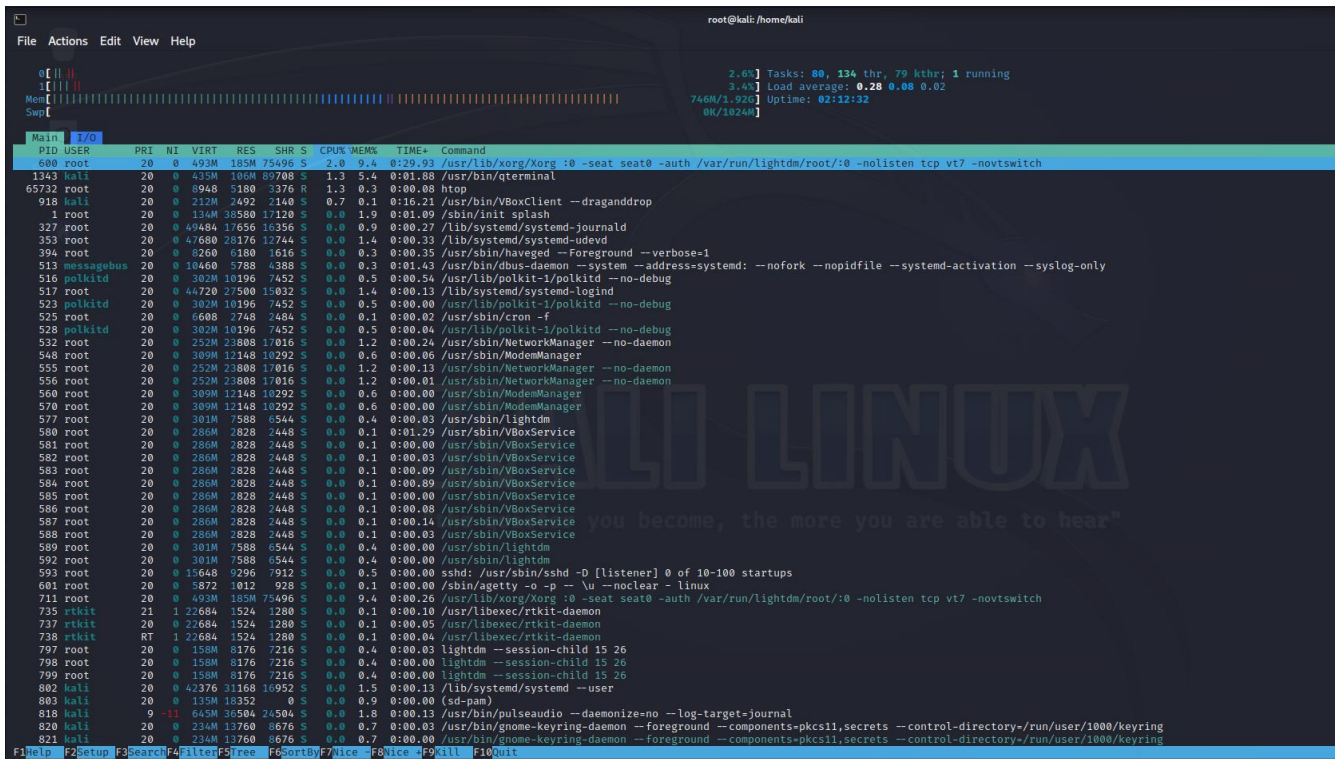
```
root@kali: /home/kali
File Actions Edit View Help
top - 06:13:26 up 2:11, 2 users, load average: 0.01, 0.02, 0.00
Tasks: 159 total, 1 running, 158 sleeping, 0 stopped, 0 zombie
%Cpu(s): 5.4 us, 1.9 sy, 0.0 ni, 92.6 id, 0.2 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1967.4 total, 582.0 free, 937.5 used, 646.1 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used, 1029.9 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
 1020 kali       20   0 582684 115068 50264 S   6.0   5.7   0:02.02 xfdesktop
   600 root        20   0 494532 183364 75244 S   4.0   9.1   0:29.29 Xorg
 1343 kali       20   0 446120 109472 89708 S   1.3   5.4   0:01.48 qterminal
   827 kali       20   0   9588   5532  4428 S   0.3   0.3   0:02.64 dbus-daemon
   910 kali       20   0 217444   2488  2136 S   0.3   0.1   0:06.08 VBoxClient
   977 kali       20   0 945564 107644 79272 S   0.3   5.3   0:16.95 xfwm4
  1003 kali       20   0 231552  30212 19848 S   0.3   1.5   0:00.92 xfsettingsd
  1011 kali       20   0 475920  50664 34624 S   0.3   2.5   0:01.20 xfce4-panel
  1026 kali       20   0 352524  38304 22240 S   0.3   1.9   0:18.50 panel-13-cpugra
  1028 kali       20   0 293004  30696 20824 S   0.3   1.5   0:15.63 panel-15-genmon
  1031 kali       20   0 391788  45972 32832 S   0.3   2.3   0:00.52 panel-18-power-
  1056 kali       20   0 390324  44460 31476 S   0.3   2.2   0:00.69 xfce4-notifyd
  1114 kali       20   0 192564  26768 17208 S   0.3   1.3   0:00.22 xfce4-power-man
 65271 root        20   0 11748   5336  3196 R   0.3   0.3   0:00.02 top
    1 root        20   0 137856  38580 17120 S   0.0   1.9   0:01.09 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
    8 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kblockd
   10 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
   11 root        20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
   12 root        20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
   13 root        20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
   14 root        20   0      0      0      0 S   0.0   0.0   0:00.39 ksoftirqd/0
   15 root        20   0      0      0      0 I   0.0   0.0   0:02.41 rcu_preempt
   16 root        rt   0      0      0      0 S   0.0   0.0   0:00.04 migration/0
   18 root        20   0      0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   19 root        20   0      0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
   20 root        rt   0      0      0      0 S   0.0   0.0   0:00.16 migration/1
   21 root        20   0      0      0      0 S   0.0   0.0   0:00.46 ksoftirqd/1
   23 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_highpri
   26 root        20   0      0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
   27 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
   28 root        20   0      0      0      0 S   0.0   0.0   0:00.00 kauditd
   29 root        20   0      0      0      0 S   0.0   0.0   0:00.00 khungtaskd
   30 root        20   0      0      0      0 S   0.0   0.0   0:00.00 oom_reaper
   32 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 writeback
   33 root        20   0      0      0      0 S   0.0   0.0   0:00.29 kcompactd0
   34 root        25   5      0      0      0 S   0.0   0.0   0:00.00 ksmd
   36 root        39  19      0      0      0 S   0.0   0.0   0:00.20 khugepaged
   37 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 kintegrityd
   38 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 kblockd
   39 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 blkcg_punt_bio
   40 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 tpm_dev_wq
   41 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 edac-poller
   42 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 devfreq_wq
```

- PID (Process ID): идентификатор процесса
- USER (User): имя пользователя, от имени которого выполняется процесс
- PR (Priority): приоритет процесса.
- NI (Nice value): значение приоритета в виде "доброты" процесса
- VIRT (Virtual memory): общий объем виртуальной памяти, используемый процессом.
- RES (Resident memory): объем физической памяти, используемый процессом в настоящий момент.
- SHR (Shared memory): объем общей памяти, используемой процессом
- S (Status): текущий статус процесса (запущен, спит и т.д.).
- %CPU (CPU usage): процент использования ЦПУ процессом.
- %MEM (Memory usage): процент использования памяти процессом
- TIME+ (CPU time): общее количество процессорного времени, использованного процессом
- COMMAND (Command name): имя команды или программы, запущенной процессом.

## Нtop

Команда htop в Linux представляет собой интерактивный процесс-менеджер, который позволяет отслеживать системные ресурсы и управлять процессами в реальном времени. Она обеспечивает более детальное и удобное отображение информации о процессах, чем стандартная команда top .



- PID (Process ID) - уникальный идентификатор процесса.
- USER - имя пользователя, от имени которого выполняется процесс.
- PR (Priority) - приоритет процесса.
- NI (Nice value) - значение приоритета, заданное пользователем
- VIRT (Virtual memory) - объем виртуальной памяти, используемой процессом.

- RES (Resident memory) - объем оперативной памяти, используемой процессом.
- SHR (Shared memory) - объем общей памяти, используемой процессом.
- S (Status) - текущий статус процесса (running, sleeping, stopped, etc.).
- %CPU (CPU usage) - процент использования процессорного времени.
- %MEM (Memory usage) - процент использования оперативной памяти.
- . TIME+ (CPU time) - общее процессорное время, затраченное процессом.
- COMMAND (Command name) - имя выполняемой команды или программы.

## Ps

Команда `ps` в Linux используется для вывода информации о текущих процессах в системе

```
(root@kali)-[/home/kali]
# ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	1.9	138056	38584	?	Ss	04:01	0:01	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	04:01	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	04:01	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	04:01	0:00	[rcu_par_gp]
root	5	0.0	0.0	0	0	?	I<	04:01	0:00	[slub_flushwq]
root	6	0.0	0.0	0	0	?	I<	04:01	0:00	[netns]
root	8	0.0	0.0	0	0	?	I<	04:01	0:00	[kworker/0:0H-kblockd]
root	10	0.0	0.0	0	0	?	I<	04:01	0:00	[mm_percpu_wq]
root	11	0.0	0.0	0	0	?	I	04:01	0:00	[rcu_tasks_kthread]
root	12	0.0	0.0	0	0	?	I	04:01	0:00	[rcu_tasks_rude_kthread]
root	13	0.0	0.0	0	0	?	I	04:01	0:00	[rcu_tasks_trace_kthread]
root	14	0.0	0.0	0	0	?	S	04:01	0:00	[ksoftirqd/0]
root	15	0.0	0.0	0	0	?	I	04:01	0:03	[rcu_preempt]
root	16	0.0	0.0	0	0	?	S	04:01	0:00	[migration/0]
root	18	0.0	0.0	0	0	?	S	04:01	0:00	[cpuhp/0]
root	19	0.0	0.0	0	0	?	S	04:01	0:00	[cpuhp/1]
root	20	0.0	0.0	0	0	?	S	04:01	0:00	[migration/1]
root	21	0.0	0.0	0	0	?	S	04:01	0:00	[ksoftirqd/1]
root	23	0.0	0.0	0	0	?	I<	04:01	0:00	[kworker/1:0H-events_highpri]
root	26	0.0	0.0	0	0	?	S	04:01	0:00	[kdevtmpfs]
root	27	0.0	0.0	0	0	?	I<	04:01	0:00	[inet_frag_wq]
root	28	0.0	0.0	0	0	?	S	04:01	0:00	[kauditd]
root	29	0.0	0.0	0	0	?	S	04:01	0:00	[khungtaskd]
root	30	0.0	0.0	0	0	?	S	04:01	0:00	[oom_reaper]
root	32	0.0	0.0	0	0	?	I<	04:01	0:00	[writeback]
root	33	0.0	0.0	0	0	?	S	04:01	0:00	[kcompactd0]
root	34	0.0	0.0	0	0	?	SN	04:01	0:00	[ksmd]
root	36	0.0	0.0	0	0	?	SN	04:01	0:00	[khugepaged]
root	37	0.0	0.0	0	0	?	I<	04:01	0:00	[kintegrityd]
root	38	0.0	0.0	0	0	?	I<	04:01	0:00	[kblockd]
root	39	0.0	0.0	0	0	?	I<	04:01	0:00	[blkcg_punt_bio]
root	40	0.0	0.0	0	0	?	I<	04:01	0:00	[tpm_dev_wq]
root	41	0.0	0.0	0	0	?	I<	04:01	0:00	[edac-poller]
root	42	0.0	0.0	0	0	?	I<	04:01	0:00	[devfreq_wq]
root	44	0.0	0.0	0	0	?	S	04:01	0:00	[kswapd0]
root	50	0.0	0.0	0	0	?	I<	04:01	0:00	[kthrotld]
root	52	0.0	0.0	0	0	?	I<	04:01	0:00	[acpi_thermal_pm]
root	53	0.0	0.0	0	0	?	S	04:01	0:00	[xenbus_probe]
root	54	0.0	0.0	0	0	?	I<	04:01	0:00	[mld]
root	55	0.0	0.0	0	0	?	I<	04:01	0:00	[kworker/1:1H-kblockd]
root	56	0.0	0.0	0	0	?	I<	04:01	0:00	[ipv6_addrconf]
root	61	0.0	0.0	0	0	?	I<	04:01	0:00	[kstrp]

USER: Имя пользователя, владеющего процессом.

PID: Идентификатор процесса (Process ID).

. %CPU: Процент процессорного времени, используемого процессом.

%MEM: Процент используемой процессом оперативной памяти

VSZ: Виртуальный размер процесса в килобайтах.



RSS: Размер резидентной набора страниц процесса в килобайтах

TTY: Терминал, связанный с процессом (если есть).

STAT: Состояние процесса (например, S - спящий, R - работает, Z - зомби и т.д.).

START: Время запуска процесса или дата для длительно работающих процессов.

TIME: Общее процессорное время, затраченное процессом.

COMMAND: Имя выполняемой команды или программы.

Флаги:

-A: показывает процессы всех пользователей, а не только текущего пользователя

-U: выводит дополнительную информацию о процессах, включая информацию о владельце процесса (пользователь), использование CPU и памяти, время запуска процесса и команду, которой был запущен процесс.

-X: выводит также процессы, не связанные с терминалом. Это позволяет отображать процессы, запущенные в фоновом режиме или системные процессы.

## Dstat

Команда dstat в Linux представляет собой утилиту мониторинга системы, которая отображает различную информацию о производительности системы в реальном времени. Она собирает и отображает данные о процессоре, памяти, дисковом пространстве, сети и других системных ресурсах.

```
(root@kali)-[/home/kali]
# dstat -cdlmnpst
```

--total-cpu-usage--					-dsk/total-		--load-avg--			--memory-usage--				-net/total-		--procs--			--swap--		--system--	
usr	sys	idl	wai	stl	read	writ	1m	5m	15m	used	free	buff	cach	recv	send	run	blk	new	used	free	int	csw
0	1	99	0	0	66k	15k	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.3	0	1024M	759	459
0	1	99	0	0	0	0	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	748	483
0	1	99	0	0	0	0	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	712	499
1	1	98	0	0	0	0	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	736	474
0	1	99	0	0	0	0	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	705	476
1	1	99	0	0	0	0	0.07	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	717	481
1	1	99	0	0	0	0	0.06	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	754	493
2	3	95	0	0	0	0	0.06	0.03	0	797M	299M	166M	621M	0	0	0	0	8.0	0	1024M	951	1001 ^c

- **cpu** : Процент использования CPU. Это отображает общую загрузку процессора в процентах.
- **dsk** : Загрузка диска. Этот столбец показывает количество операций чтения/записи на диске в секунду.
- **net** : Загрузка сети. Он отображает количество байтов, переданных и полученных через сетевые интерфейсы в секунду.
- **load** : Загрузка системы. Это отображает среднюю нагрузку системы за последние 1, 5 и 15 минут
- **mem** : Использование памяти. Он показывает количество использованной и свободной памяти, а также память, используемую для кэширования данных
- **swar** : Использование области подкачки. Этот столбец показывает использование области подкачки (swar) в системе.

- `procs` : Информация о процессах. Он показывает количество процессов, запущенных в системе, а также статистику по процессам в режиме реального времени.
- `sys` : Системные вызовы. Этот столбец отображает количество системных вызовов в секунду
- `int` : Прерывания. Он показывает количество прерываний в системе.
- `csu` : Переключения контекста. Этот столбец показывает количество переключений контекста в секунду.
- `disk` : Загрузка диска (расширенная информация). Он отображает загрузку диска по отдельным разделам и устройствам.
- `lock` : Загрузка блокировок. Этот столбец показывает использование блокировок в системе

Флаги:

- `c` : Загрузка процессора (CPU)
- `d` : Загрузка диска (disk).
- `l` : Загрузка системы (load).
- `m` : Использование памяти (memory).
- `n` : Загрузка сети (network).
- `p` : Информация о процессах (processes).
- `s` : Использование области подкачки (swap).
- `y` : Системные вызовы (system).

## Iostat

Команда `iostat` в Linux используется для отображения статистики производительности ввода/вывода (I/O) системы. Она предоставляет информацию о использовании дисков, дисковых контроллерах, и средств коммуникации ввода-вывода, таких как сетевые интерфейсы.

```
(root@kali)-[/home/kali]
# iostat
Linux 6.1.0-kali9-amd64 (kali) 06/05/2023      _x86_64_      (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.46    0.00    0.63    0.06    0.00   98.86

Device            tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda                4.42         81.99         18.87          0.00     686567     158017         0
```

- `avg-cpu` : Заголовок столбца, который указывает, что следующие столбцы содержат средние значения использования ЦП в процентах для определенных интервалов времени.
- `%user` : Процент времени ЦП, затраченного на обработку пользовательских процессов
- `%nice` : Процент времени ЦП, затраченного на обработку приоритетных процессов.
- `%system` : Процент времени ЦП, затраченного на обработку системных процессов ядра.
- `%iowait` : Процент времени, когда ЦП ожидает завершения операций ввода-вывода.

- %steal : Процент времени, когда виртуальный процессор ожидает физического процессора из-за вмешательства других виртуальных процессоров.
- %idle : Процент времени, когда ЦП не занят выполнением задач и ожидает новых задач
- Device : Заголовок столбца, который указывает, что следующие столбцы содержат информацию о конкретных устройствах хранения данных.
- tps : Количество транзакций ввода-вывода в секунду (transactions per second), т.е. количество операций чтения и записи, выполняемых на устройстве в секунду.
- kB\_read/s : Количество килобайт, считываемых с устройства в секунду.
- kB\_wrtn/s : Количество килобайт, записываемых на устройство в секунду.
- kB\_dscd/s : Количество килобайт, отменяемых на устройстве в секунду.
- kB\_read : Общее количество килобайт, считанных с устройства с момента его запуска.
- kB\_wrtn : Общее количество килобайт, записанных на устройство с момента его запуска
- kB\_dscd : Общее количество килобайт, отменяемых на устройстве с момента его запуска.