

Running applications and system processes can be inspected, killed, ... (aka TaskManager in Windows)

- **ps axuf | less**: inspect currently running processes (one-time)
- **top, htop**: online inspection of processes
 - Frequency of update
 - Search
 - Sort by memory usage instead of CPU
 - Can kill or change priority of a process
- **kill, killall, xkill**: kill process or application
- **nice, renice**: change application priority (0 by default, only root can increase it)
 - Priorities: -20 ... 19
 - **nice -12 large-job**: run large-job with priority 12
 - **nice --12 large-job**: run large-job with priority -12
 - **renice 17 -p 1134**: change priority of process with id 1134 to 17
- **cpulimit**: limit cpu usage of a process
- **ulimit, unlimit**: limit resources for a process (resp. in active shell): e.g. memory, number of opened files, ...
 - User can't override defaults in **/etc/security/limits.conf**
 - **ulimit -a**: see current limits
 - **unlimit**: set limits to the system defaults (not further limits for user)
 - **ulimit -Sv**: limit memory usage in kilobytes

- **xrestop**: GUI processes
- **xkill**: GUI kill
- **wmctrl**: Change GUI window position, size, etc.
- **xev**: Monitor / debug key press (special keys)
- **xprop**: Properties of GUI window
- **xdotool**: Properties of GUI window, including emulation of keyboard/mouse

- **iotop**: Disk usage per process
- **jnettop**: Network usage

Administration

In general: search for solutions of problems e.g. at stackoverflow.com, but be careful advices include modification of system files (configs are OK; reshuffling binaries, libraries etc. NOT)

- `shutdown`, `poweroff`, `halt`, `reboot`,
- `hibernate`, `hibernate-ram`, `hibernate-disk`, `s2disk`, `s2ram`
- `systemctl` command:
 - `list-units`: list running system services
 - `stop`, `start`, `restart`: handle given service, only works till restart
 - `disable`, `enable`: enable/disable service completely (even after restart)

System configuration:

- in `/etc` directory
- most common default options in `/etc/default` directory

Logging of system events: in `/var/log` directory

- `syslog`, `daemon.log`, `messages`, `kern.log`, `debug`: system messages
- `auth.log`: info about logging of users (including virtual ones)
- `Xorg.0.log`: log of the GUI system
- Log files are usually backedup per month and started freshly again (`/etc/logrotate.conf`, `/etc/logrotate.d`)

Handled by the Linux Kernel (includes HW drivers)

- Info about HW in pseudofiles: `/dev/*`, `/sys/*`, `/proc`
- Commands to list HW:
 - `lspci`: HW connected to the PCI bus
 - `lshw`: detailed info about all HW
 - `lsusb`: USB devices
 - `lsblk`: Block devices (disks)
 - `lsscsi`: SCSI devices (CD/DVD)
- Adding removing driver (= kernel module):
 - `lsmod`: list loaded kernel modules
 - `modinfo`: detailed info about kernel module
 - `modprobe`: add, or remove (`-r`) from kernel
 - `insmod`, `rmmod`: simple add / remove module from kernel
 - PS: Not all drivers are as separated modules, but can be builtin in the kernel = ζ the only way to disable them is via kernel option in GRUB boot loader
- Configuring kernel modules:
 - `/etc/modules`: force load of kernel modules not picked up automatically (special HW, very new HW, ...)
 - `/etc/modprobe.d`: add options to drivers, blacklist drivers

Nowadays most systems use *NetworkManager* (NM) application to handle the net connection

- `/sbin/ifconfig`: Show info about network devices and connection (IP address, MAC address)
- NM allows complex configuration, including scripts
- NM recently generates random WiFi MAC address for security on public sites: might need to be disabled in corporate networks through `/etc/NetworkManager` settings

Useful commands:

- `ping`: Check remote host is online
- `traceroute`: Show full communication path to remote host
- `ssh`: connect to remote host via Secure Shell
- `ftp`, `sftp`, `scp`, `nfs`: copy files from/to remote host (see later lectures)
- `netstat`: info about connections, opened ports etc. (`netstat -natulp | less`)

The linux system mostly rely on CUPS printing system:

- `/etc/cups`: configuration of the print client and server
- `localhost:631` in web-browser: WEB-based configuration of CUPS

However, recently some GUI applications can ignore CUPS settings and search for available printers by themselves...

CRON system:

- `/etc/crontab`: basic file to run tasks per hour/day/week/month
- `/etc/cron.hourly`
- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/etc/cron.monthly`
- `/etc/cron.d`: more complicated rules

```
# /etc/cron.d/renew_prak0x: crontab entries for reweal of the prak0x user home directories
# Execute only during the period of the exercises (01.Oct - 20.Jan)
# TODO ?: Add entry in between day in case of 2 excercises per single day

SHELL=/bin/bash

# m h dom mon dow user  command
32 01 * OCT,NOV,DEC,JAN SUN root /home/prak_template/bin/reboot.cron.sh
# NO!!! (studenti by po rebootu nenasli sva data !)
#@reboot root /home/prak_template/bin/renew_prak0x.cron.sh
12 03 * OCT,NOV,DEC * root /home/prak_template/bin/renew_prak0x.cron.sh
12 03 1-20 JAN * root /home/prak_template/bin/renew_prak0x.cron.sh
```

APT system to download and install packages from repositories

- **apt-get**, **aptitude**: commands to run the tasks (install, remove, update package list)
- **/etc/apt**: configuration of the packaging system
- Temporary files (package list, downloaded installation files) in **/var/lib/apt/lists** and **/var/cache/apt** files
- Dependencies are flagged as auto-installed (**/var/lib/apt/extended_states**)
- Simulate action (complicated upgrades): **apt-get -s**

DPKG is used to handle already installed packages:

- **-i**: install local package
- **-r/-P**: remove/purge installed package (purge = remove also config files)
- Allows to install even conflicting packages (**--force-depends**, **--force-conflicts**): use with care !
- Packages can ask for configuration options during installation process, reinvoke these questions by **dpkg-reconfigure** command
- Packages can provide "alternatives" for similar tasks: **update-alternatives** command to handle these selections

Linux on net is also target of attacks, especially through the ssh connection

- **sshguard**: service that stops ssh login after several failed attempts
- **rkhunter**: complex check of the most important system utilities
- **chkrootkit**: simple check of most known "viruses" in the system utilities
- **logcheck**: scans log files and reports suspicious activities

Many of these commands are set to run regularly and send reports by e-mail to the system admin (see `/etc/aliases` file)