Born2beroot notes

This cheatsheet aims to provide the important commands for the Born2beroot project. It is not a substitute for a formal tutorial. Each section corresponds to a keyword. They are not necessarily in a relevant order.

1 Monitoring

- For the architecture of the operating system and its kernel version, use the command `uname`.

`uname`	prints certain system information
`-s`	print the kernel name
`-r`	print the kernel release
`-v`	print the kernel version
`-m`	print the machine hardware name
`-o`	print the operating system

- The `/proc/cpuinfo` file lists all virtual processors and information about them. Each virtual processor has a physical id corresponding to which physical processor each belongs to.

`grep 'physical id'`	gets all physical ids
`sort`	sorts them
`uniq`	erases duplicates
`wc -l`	counts the number of lines

- The same file can easily give the number of virtual processors.

`grep 'processor'`	gets all virtual processors
`wc -l`	counts the number of lines

- The command `free` can be used to print the RAM available.

`free`	displays amount of free and used memory
`-m`	displays the amount of memory in MiB
`-k`	displays the amount of memory in KiB

`awk` can then be used with the pattern `/^Mem:/` to get both the total (`$2`) and used memory (`$3`).

- The command `df` can get storage information.

`df`	report file system disk space usage
`-BM`	scale sizes by MB
`-BG`	scale sizes by GB
`--total`	produce a grand total

`awk` can then be used with the pattern `/^total/` to get the total (`$2`), used (`$3`) and utilization rate (`$5`).

- The command `top` can get information about the processor usage.

`top`	display Linux processes
`-b`	starts top in Batch mode
`-n1`	sets to 1 the maximum number of iterations top should produce before ending

`awk` can then be used with the pattern `/^%Cpu/` to get the user (`$2`) and system (`$4`) utilization rates.

- The command `who` can get the last boot information.

`who`	print information about users who are currently logged in
`-b`	time of last system boot

`awk` can then be used to get the last boot date (`$3`) and time (`$4`).

- `lsblk` can be used to check if LVM is used.

`lsblk`	list block devices
`-o TYPE`	prints only TYPE column

Use `wc -l` to count the number of `lvm` blocks and then an `if` condition to print either yes or no.

- `ss` can be used to get socket information.

`ss`	dump socket statistics
`-H`	no header
`-t`	display TCP sockets
`grep ESTAB`	gets only established ones
`wc -l`	counts them

- Simply use `users` and `wc -w`.
- The IP address can be obtained with `hostname` and `ip` can be used to get the MAC address.

`hostname`	show info about the hostname
`-I`	show all IP addresses of the host
`ip`	show rounting and network devices
`link`	network device
`show`	shows the addresses

- `journalctl` can be used to get the `sudo` commands.

`journalctl`	query the systemd journal
`_COMM=sudo`	get only the sudo entries
`grep COMMAND`	get only the command entries
`wc -l`	counts them

2 sudo

To get in sudo mode, type `su -`. Then install `sudo` with `apt`.
`sudo visudo` to modify `sudo` rules.

3 UFW

Common commands:

`ufw status`	check UFW status
`ufw enable`	enable UFW
`ufw disable`	disable UFW
`ufw allow <port>`	allow port
`ufw deny <port>`	deny port
`ufw delete allow <port>`	delete allow rule
`ufw delete deny <port>`	delete deny rule

4 SSH

SSH config is found in `/etc/ssh/sshd_config`.
Use `ssh <username>@localhost -p 4242` to connect.

5 System control

Common commands (to be used with a service afterwards):

`systemctl status`	checks service status
`systemct enable`	enable service
`systemct disable`	disable service
`systemctl start`	starts service
`systemctl restart`	restarts service

6 Password policy

Password aging controls are found in `/etc/login.defs`. Use `chage` to change rules for existing users.

`chage <user>`	change age parameters
`-M 30`	changes maximum days to 30 days
`-m 2`	changes miminum days to 2 days
`-W 7`	changes warning delay to 7 days

Other requirements are addressed with `libpam-pwquality`. They can be edited in the `/etc/security/pwquality.conf` file or in the `/etc/pam.d/common-password`.

7 Users, groups and hostname

`adduser`	adds a new user
`deluser`	deletes a user
`users`	logged in users
`groupadd`	creates a new group
`groupdel`	deletes a group
`getent group <group>`	get members of group
`usermod -aG <g> <u>`	adds user to group
`usermod -G <g> <u>`	removes user
`ufw delete deny <port>`	delete deny rule
`hostnamectl set-hostname`	change hostname
`hostnamectl status`	info about hostname

8 Crontab

Access task file with `crontab -u root -e`.

9 Fail2ban

`fail2ban-client status <jail>`	status for jail
`fail2ban-client unban <ip>`	unbans IP
`fail2ban-client set <j> banip <i>`	bans an IP