Contents

(cc) BY-SA

(cc) BY-SA

1 Basics

Exercise 1: ls

`ls` stands for "list".

a) List all files (including hidden files) in your current directory.

```
ls -a
```

b) List all files in your `/bin` directory.

```
ls /bin
```

c) List all files in your `/bin` directory whose names consist of only two letters.

```
ls /bin/??
```

d) Find the size of your bash executable (depending on your system, it's `/usr/bin/bash` or `/bin/bash`).

```
ls -la /usr/bin/bash
```

or

```
ls -la /bin/bash
```

Exercise 2: mv

`mv` stands for move.

a) Make a file `hello` using `touch hello`. Now rename this file to `world`.

```
touch hello
mv hello world
```

b) Move this file into a directory. (e.g. your `Downloads` directory).

```
mv world ~/Downloads
```

(cc) BY-SA

Exercise 3: cd

`cd` stands for "change directory".

a) From your home directory, change to `./Documents`. Then change back to the `home` directory.

```
cd Documents
cd ..
```

b) Change into the `/root` directory.

```
cd /root
```

c) Change back to your home directory without writing out the full path.

```
cd ~
```

or just

```
cd
```

Exercise 4: cat

a) Look at the output of whatever file you desire.

```
cat file
```

b) Move the contents of one file into another, overwriting it.

```
cat file1 > file2
```

Exercise 5: mkdir and rmdir

`mkdir` stands for "make directory", `rmdir` for "remove directory".

a) Make a directory called `hello` in your home directory, and then remove it.

```
mkdir hello
rmdir hello
```

b) Can you remove your home directory with rmdir?

Answer: No, you can only remove empty directories with `rmdir`

Exercise 6: rm

`rm` stands for "remove". It directly removes files, it doesn't put them in the trash.

a) Create a file `world`, then delete it.

```
touch world
rm world
```

(cc) BY-SA

b) Create a directory called `foo`, then create 3 files with names of your choice instead inside this directory. Remove them all at once.

```
mkdir foo
cd foo
touch file1
touch file2
touch file3
rm *
```

Exercise 7: cp

`cp` stands for `copy`.

a) Create a `Backup` directory and copy your `.bashrc` (bash configuration file) there. Check if it worked with `ls`.

```
mkdir Backup
cp .bashrc Backup
ls Backup
```

b) Copy a directory into `Backup/` (e.g. your `Downloads` directory). What is the difference to copying a file?

Answer: `-r` flag (recursive) has to be used.

```
cp -r Downloads Backup
```

c) Remove the `Backup/` directory you just created. Again, the `-r` flag is needed to recursively delete everything in the directory.

```
rm -r Backup
```

Exercise 8: clear

a)

```
clear
```

(cc) BY-SA

2 Files

Exercise 1

a) Execute:

```
mkdir ~/TempDir
cd ~/TempDir
```

b) Execute:

```
nano capture.txt
```

Press `^O`, then Enter to save in nano and `^X` to quit (where `^` stands for the Control key).

c) Execute:

```
wc capture.txt
```

d) Execute:

```
cp capture.txt capture-copy.txt
diff capture.txt capture-copy.txt
```

e) Execute:

```
nano capture.txt
diff capture.txt capture-copy.txt
```

f) Execute:

```
ls -l
chown root:users capture.txt
```

- You should have received an error message due to lack of permissions.
- *Hint:* use `sudo`.

```
sudo chown root:users capture.txt
ls -l
```

g) Execute:

```
chmod -w capture-copy.txt
nano capture-copy.txt
```

(cc) BY-SA

- This gives an error message because now the file can't be written to when attempting to save in nano.
- Extra exercise: Would it be possible to overcome the write restriction using `sudo`?

h) Execute:

```
echo "Hello World!"
```

i) Execute:

```
touch -t 201701310001.30 capture.txt
ls -l
```

j) Execute:

```
ln capture.txt ~/Desktop/capture-link
```

k) Execute:

```
file * ~/Downloads/* ~/Pictures/* ~/Music/*
file * ~/Downloads/* ~/Pictures/* ~/Music/* > file-types.log
```

l) Execute:

```
less file-types.log
```

m) Execute:

```
which ls
whereis ls
```

n) Execute:

```
cd ~/TempDir
```

Make sure you're in the correct directory, then execute:

```
rm *
```

- *Note 1:* If a warning appears asking to confirm removal of write protected files, confirm with `y`.
- *Note 2:* Even file a who's owner was changed to root is also deleted! Ownership doesn't protect the files.

```
cd ~
rmdir TempDir
```

(cc) BY-SA

3 Jobs

Exercise 1

a) Ubuntu: `sudo apt install htop`, OpenSUSE: `sudo zypper in htop`

b) `cd jobs/`

c) `./infiniteLoop.sh`

d) (press Ctrl+C, Mac users make sure to press the "control" key)

e) `./infiniteLoop.sh &`

f) `fg`

g) For this it's best to press `Ctrl+Z` to suspend the job and then type `bg` which will move it to the background. CTRL+C is now insufficient to kill it.

Note: running this script as a background job is pretty ugly because it still spams the console. In order to stop this you would need to redirect the output to somewhere else. However redirection is not the topic we are covering in the exercise and the output helps you to see if the program is still running or not.

h) The PID can be found it using htop, top works similar but is not recommended. In htop you can see the name of the running processes totally on the right and on the left you can see the PID of that process. Remember the PID.

i) One way is to use `kill -9 PID`.

j) Execute:

```
./infiniteloop.sh &
./infiniteloop.sh &
./infiniteloop.sh &
jobs
kill %2
kill %1
kill %3
```

Note: The percentage symbol can also be used with fg and bg to move specific jobs into the foreground or background.

(cc) BY-SA

Exercise 2

In order to find the PID we will use the `ps` command. Just type `ps -e` this will list every process in your system. Again find the infiniteLoop.sh and remember it's PID. Since we used `kill -9` last time we will do something else this time. A very nice way to kill a process is using pkill. The nice thing about pkill is that you do not need the PID. Simply type in `pkill -SIGKILL infinite`.

Another thing you could use is xkill. However xkill will kill the entire terminal not just the one process.

(cc) BY-SA

4 Remote

Exercise 1

a) `ssh hacker@pterodactyl.vsos.ethz.ch`
b) `mkdir $yourName` (you do not need to type the $ simply use your nethz name)
c) Hit `Ctrl+D`.
d) `scp supercoolNumericalSimulation.c hacker@pterodactyl.vsos.ethz.ch:$yourname/`
e) Run the ssh command again, navigate to your directory, and compile with: `gcc supercoolNumericalSimulation.c` this gives you a file called a.out
f) Running: `./a.out`. In case you get an error saying the file is not executable make it executable with `chmod -x a.out`. Now you should see an output file.
g) `Ctrl+D`, navigate to your remoteExercise directory, `scp hacker@pterodactyl.vsos.ethz.ch:$yourName/result.txt .`

Exercise 2

a) `tmux` (if it's not yet installed, do `sudo apt install tmux` on Ubuntu or `sudo zypper in tmux` on OpenSUSE)
b) `Ctrl+B`, `"` (this is the quotes symbol, typically `SHIFT+2`)
c) `Ctrl+B`, `%` (percent sign, typically `SHITFT+5`) to split and `Ctrl+B`, `Arrow-Key` to navigate.
d) `tmux a` to attach to tmux (note that there is no `-` before the `a`).
e) (no solution)
f) Typically, `Alt+F4` or click the close button on the windows of the terminals. To attach, do again `tmux a`.
g) Repeatedly type `exit` or press `Ctrl+D`.
h) `ssh hacker@pterodactyl.vsos.ethz.ch`
i) Simply type `w`.
j) `tmux a` to attach (if it says "no sessions", type `tmux`).
k) `Ctrl+B`, `d`
l) `exit` or `Ctrl+D`

(cc) BY-SA

5 Searching

Exercise 1: `grep`

a) Take a look at the file

```
cd HackingSessionExercises/
cat grep_exercise.md
```

b) Find the word “contains”.

```
grep "contains" grep_exercise.md
```

c) Come up with a pattern such that the output are the three lines `Dog`, `Dig` and `Dug`.

```
grep -E "D(o|i|u)g" grep_exercise.md
```

d) Look for all lines beginning with `##`.

```
grep -E "^##" grep_exercise.md
```

e) Print all lines beginning with `##`, but exclude the ones that starts with `###`.

```
grep -E "^##[^#]" grep_exercise.md
```

or you can just use:

```
grep -E "^## " grep_exercise.md
```

f) Search for the lines `Cat`, `Rat`, `Sat` and so on, up until `Bat`, but without the line `Latin`.

```
grep -Eo "^.at" grep_exercise.md
```

g) Produce the same lines as in e), but this time with the line `Latin` included.

```
grep -E "^.at.*" grep_exercise.md
```

h) Try for the lines `Brat` up until `Bat`, but without the line `Latin`.

```
grep -Eo "^..?at" grep_exercise.md
```

i) Adjust your command so that it lists the lines `Brat` up until `Bat`, this time with `Latin`.

```
grep -E "^..?at.*" grep_exercise.md
```

j) Check for the three list elements (these are the lines beginning with `*`).

(cc) BY-SA

```
grep "^\*.*" grep_exercise.md
```

k) Investigate for the entire block of Java code (the one at the end of the file).

```
grep -oz "\`\`\`.*\`\`\`" grep_exercise.md
```

or with single quotes:

```
grep -oz '```.*```' grep_exercise.md
```

l) Within that code, output the class that contains the method `out`.

```
grep -Eoz "class[^}]*void out.*}" grep_exercise.md
```

or, with slight cheating:

```
grep -Eoz "class Out.*}" grep_exercise.md
```

m) Pry for all animals that consist of exactly two words.

```
grep -Eo "\+ [A-Z]\w* \w+" grep_exercise.md
```

If you don't want the plus signs, we need to use the pearl regex engine with `-P` and use a technique called "lookbehind". This is rather advanced. If you're more interested, you can look for "lookbehind regex" online.

```
grep -Po "(?<=\+ )[A-Z]\w* \w+" grep_exercise.md
```

n) Probe for all animals that begin with `Danger`.

```
grep -Eo "Danger\w* ?(\w+[- ]?)*" grep_exercise.md
```

o) Finally, if you're still motivated: All animals that contain the word `Danger` *or* `danger`.

```
grep -Eo "([A-Z]\w*|D)anger\w* ?([A-Z]\w*[- ]?)*" grep_exercise.md
```

Exercise 2

a) Navigate to your home directory.

```
cd
```

b) Using `find`, search for all files that were created less than 5 days ago.

```
find -atime 5
```

c) Using `find`, search for all the files that you have write access for.

```
find -writable
```

d) Search for all files that start with the letter `d`.

```
find -name "d*"
```

e) Search for all files smaller than 1MB, but larger than 10KB.

```
find -size +10k -size -1M
```

(cc) BY-SA

f) Find all files in the directory `Desktop` (or some different directory).

```
find Desktop/
```

g) Search for all files starting with the letter `d` and execute `cat` on them.

```
find -name "d*" -exec cat {} \;
```

Exercise 3

Combining the knowledge of `grep` and `find`, we can search for some incredibly specific stuff! Look at the `exec` flag in the manual for `find`.

a) Navigate to your etc directory (`/etc`, on most distributions).

```
cd /etc
```

b) Within that directory, search for all lines of text containing the word "root".

```
find -exec grep "root" {} \;
```

or

```
grep -R "root"
```

c) If you received a lot of error messages in exercise b), try to limit your search to files which you have read permissions for.

```
find -readable -type f -exec grep "root" {} \;
```

d) Search for all files containing an IPv4 address.

```
find -exec grep "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}[^.]" {} \;
```

or

```
grep -PRl "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}[^.]"
```

e) Output all comments (lines starting with a `#`) of all files with a name ending in `.conf`.

```
find -name "*.conf" -exec grep "^#" {} \;
```

(cc) BY-SA

6 System management

Exercise 1: Power on/off

a) Try to put your computer into suspend, and wake it back up.

```
systemctl suspend
```

```
shutdown 10
shutdown -c
```

b) Reboot your computer from the command line.

```
reboot
```

Exercise 2: Space left on disk

a) Find out what size (in MB) the exercise directory has.

```
du -sh HackingSessionExercises
```

b) Find out how much space is used by your root directory `/`.

```
df -h /
```

Exercise 3: User management

a) Add a new user called `ExerciseUser`.

```
sudo useradd exercise_user
```

b) Add a new group called `exercise_group`.

```
sudo groupadd exercise_group
```

c) Add your new user to the new group.

```
sudo gpasswd -a exercise_user exercise_group
```

d) Remove the user and the group again.

```
sudo userdel exercise_user
sudo groupdel exercise_group
```

(cc) BY-SA

7 Block devices and file systems

Exercise 1: Partition a disk

a) Create two partitions: One with 1MB size, one with the rest of the available space. Both should be of type `Linux filesystem`. Two options:

(1) `cfdisk`

- Run `cfdisk TestDisk`.
- Select `gpt`/`dos` label (both will work), in an actual system you will probably want `gpt`.
- Select `New` with the arrow keys, hit enter.
- Edit the size to 1M, hit enter.
- Select `Free space` with the arrow keys.
- Same thing again: New, use the default size (all space left), hit enter.
- Select `Write` with the arrow keys.
- Type `Quit`.

(2) `gdisk`

- Run `gdisk TestDisk`.
- Enter `n` for new partition.
- Select number 1.
- Set first sector to default (just hit enter).
- Set second sector to +1M.
- Use the default partition type.
- Do the same thing for the second partition again, but use the defaults for both sectors, and use partition number 2.
- Enter `w` to write your changes.

Exercise 2: Create a file system

a) Create a FAT file system on `partition1`.

```
mkfs.vfat partition1
```

b) Create a ext4 file system on `partition2`.

```
mkfs.ext4 partition2
```

- You can check if this worked by looking at the output of `file partition1` and `file partition2` .

(cc) BY-SA

Exercise 3: Using dd

a) Write `image.iso` to `TestDisk` using `dd`.

```
dd if=image.iso of=TestDisk
```

(cc) BY-SA

8 Software management

Exercise 1: Package manager

This section is specific to your distribution. In the following we will present solutions for Ubuntu and OpenSUSE based distributions. If you're in trouble running another distro, please contact a helper.

Under Ubuntu based systems

a) `sudo apt update`
b) `sudo apt upgrade`, then press ENTER when asked `[Y/n]`. Note the capital Y: it means that if you simply press ENTER (without typing anything) this option will be chosen.
c) `sudo apt autoremove`, press ENTER when asked as above. This will uninstall old kernels from your system and free space.
d) `apt search youtube-dl`
e) `sudo apt install youtube-dl`
f) `youtube-dl` should display something like "Usage: ..."
g) `man youtube-dl`, quit with `q`
h) `sudo apt autoremove youtube-dl`
i) `df` shows your current disk usage (use `df -h` for human-readable numbers). On the right hand side, you can see "Mounted on". Look for `/`, which stands for your system partition. The used and free space can be seen in the other columns. To clean the package cache: `sudo apt clean`

Under OpenSUSE

a) `sudo zypper ref` (or `sudo zypper refresh`)
b) `sudo zypper up` (or `sudo zypper update`), then press ENTER when asked `[y/n/?] (y)`. Note the y in parentheses: it means that if you simply press ENTER (without typing anything) this option will be chosen.
c) (skip this under OpenSUSE)
d) `zypper se youtube-dl` (or `zypper search youtube-dl`)
e) `sudo zypper in youtube-dl` (or `sudo zypper install youtube-dl`)
f) `youtube-dl` should display something like "Usage: ..."
g) `man youtube-dl`, (if asked, press ENTER), finally quit with `q`
h) `sudo zypper rm youtube-dl` (or `sudo zypper remove youtube-dl`)
i) `df` shows your current disk usage (use `df -h` for human-readable numbers). On the right hand side, you can see "Mounted on". Look for `/`, which stands for your system partition. The used and free space can be seen in the other columns. To clean the package cache: `sudo zypper clean`

(cc) BY-SA

Exercise 2: Ubuntu only: Installing software from PPA

a) The page we're looking for is https://launchpad.net/~stebbins/+archive/ubuntu/handbrake-releases

b) `sudo add-apt-repository ppa:stebbins/handbrake-releases`

c) `sudo apt update`

d) `sudo apt install handbrake-gtk`

e) (no solution)

f) `sudo apt autoremove handbrake-gtk`

g) Open up your favourite text editor (e.g. `nano /etc/apt/sources.list`), remove the two lines described below and save:

```
deb http://ppa.launchpad.net/stebbins/handbrake-releases/ubuntu
    YOUR_UBUNTU_VERSION_HERE main
deb-src http://ppa.launchpad.net/stebbins/handbrake-releases/
    ubuntu YOUR_UBUNTU_VERSION_HERE main
```

h) `sudo apt update`

i) `sudo apt install handbrake-gtk` or `apt search handbrake`

Exercise 3: Installing a package manually

a) (no solution)
b) (individual)
c) `cd Downloads; ls`
d) Depends on your distro, at `<TAB>` press the tabulator key for autocompletion:

- Ubuntu: `sudo apt install teamviewer<TAB>`, will complete with . . . deb
- OpenSUSE: `sudo zypper in teamviewer<TAB>`, will complete with . . . rpm

e) (no solution)
f) Depends on your distro:

- Ubuntu: `sudo apt autoremove teamviewer`
- OpenSUSE: `sudo zypper rm teamviewer`

Exercise 4: Compile from source using git

a) (no solution)

b) The desired URL is https://github.com/AltraMayor/f3.git

c) Execute:

```
cd Downloads
git clone https://github.com/AltraMayor/f3.git
```

d) Execute:

```
cd f3
```

(cc) BY-SA

(On Ubuntu, according to the section "Install Dependencies" in the README): `sudo apt-get install libudev1 libudev-dev libparted0-dev`

`make`

`sudo make install` (Without sudo, the command fails due to missing permissions, you are supposed to figure that out on your own)

e) `f3read` should complain "f3read: The disk path was not specified".

f) We will first look around, then delete the files:

```
ls /usr/local/bin/f3*

/usr/local/bin/f3read
/usr/local/bin/f3write

ls /usr/local/share/man/man1/f3*

/usr/local/share/man/man1/f3read.1
/usr/local/share/man/man1/f3write.1

rm /usr/local/bin/f3*
rm /usr/local/share/man/man1/f3*
```

Exercise 5: Installing from a self-containing install script

a) (no solution)

b) `cd Downloads`

c) `chmod a+x postgresql<TAB>` where TAB is autocompletion by pressing the Tabulator key on your keyboard.

d) `./postresql<TAB>`

e) `sudo ./postresql<TAB>`

f) (no solution)

g) `/opt/PostgreSQL/YOUR.VERSION/bin/postgres` should complain that it does not know where to find the server configuration file.

h) `sudo ln /opt/PostgreSQL/YOUR.VERSION/bin/postgres /usr/bin/`

i) `postgres` should now print the error message about the missing config file.

j) Execute:

```
cd /opt/PostgreSQL/YOUR.VERSION
sudo ./uninstall-postgresql
```

Press "Yes"

k) `cd` (Leave the `/opt/PostgreSQL` directory since you are going to delete it)

```
sudo rm -rf /opt/PostgreSQL
```

l) `sudo userdel postgres`

(cc) BY-SA