BORN2BEROOT

********Adding and removing users/groups**********
****

-To add a new user : `$ sudo adduser [username]`
-To remove a user : `$ sudo deluser [username] [group name(optional)]`
-To delete the home dir : `$ sudo deluser --remove-home username`
-To add a new group : `$ sudo groupadd [group name]`
-To add a user to a group : `$ sudo usermod -aG [group name] [username]`
-To check who is in each group : `$ getent group [group name]`
-To give privileges to a user : `$ sudo visudo` > [USERNAME] ALL=(ALL:ALL) ALL
-To give privileges to a whole group : `$ sudo visudo` > [%GROUP NAME] ALL=(ALL:ALL)ALL
-To check which groups the user is in : `$ groups [username]`

**********************SSH/UFW*********************
****

-To install ssh server : `$ sudo apt install openssh-server`
-To check ssh status : `$ sudo systemctl status ssh`
-To restart ssh service : `$ sudo ssh restart`
-To change the default port : `$ sudo vi /etc/ssh/sshd_config`
-To check if the port has changed : `$ sudo grep Port /etc/ssh/sshd_config(requires sr*)`
-To connect through ssh : `$ ssh [username]@[server_ip] -p [port]`

-To install UFW : `$ sudo apt install ufw`
-To enable UFW : `$ sudo ufw enable`
-To check UFW status : `$ sudo ufw status numbered`(option [numbered] to list with numbers)
-To configure the rules : `$ sudo ufw allow ssh`(can as well use it as `$ sudo ufw allow 22`)
-To delete a rule : `$ sudo ufw delete [rule]`(the use of numbered option comes handy here)
NB: in case of using VBox you need to add forward rules for virtualbox.

***************PASSWORDS AND SECURITY*************
****

-To install libpam-pwquality : `$ sudo apt install libpam-pwquality`
-To change rules : `$ sudo vim /etc/pam.d/common-password` > then add a length rule/condition
'password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt minlen=10'
-In the same file at `/etc/pam.d/common-password` this line should be changed too
'password requisite pam_pwquality.so retry=3 lcredit=-1 ucredit=-1 dcredit=-1 maxrepeat=3 usercheck=0 difok=7 enforce_for_root'
This should add rules for the min length of the passwd and the structure of it.
-To change password expiration date `$ sudo vi /etc/login.defs` to access and edit the file these rules should be added:

```
'PASS_MAX_DAYS 30
PASS_MIN_DAYS 2
PASS_WARN_AGE 7'
```

-To check which password rules are applied on a user : `$ chage -l [username]`
-To limit password tries to 3 times and add bad password message : `$ sudo vi /etc/sudoers` then add the following rules: *'Defaults   passwd_tries=3*

Defaults   badpass_message=["custom message!"]
Defaults   requiretty

-To add a file to record logs : $ sudo su > $ mkdir */var/log/sudo* > $ sudo *vi /etc/sudoers* and then add the following rules : '*Defaults   logfile="/var/log/sudo/sudo.log"*
Defaults   log_input, log_output'

**********************HOSTNAME********************

****

-To check current hostname : $ hostnamectl

-To change the hostname : $ hostnamectl set-hostname [new_hostname]

-To change hostname in files : $ sudo vi */etc/hosts* > change this '*127.0.0.1   localhost*
127.0.0.1   [username]'

************************SCRIPT********************

****

-To make the script show netstats : $ sudo apt install -y net-tools > $ sudo vi */bin/monitoring.sh* > $ sudo chmod +x */bin/monitoring.sh* then go to the sudoers file to allow it to run without asking for permission : $ sudo visudo and add this line '*[username] (ALL)=(ALL) NOPASSWD: /bin/monitoring.sh* then we add a timer to the script with the crontab command : $ sudo crontab -u [username] -e then add the line '**/[time] * * * * /bin/monitoring.sh'*