Tasks for Lab Assignment 2: Hardening file systems, quotas

1. Establish quotas in their home directories for all the users in the system. These quotas are to remain active after a system reboot
   - no user can use more than 20 Mbytes for more than 10 days. Under no circunstances can any of them use more than 23 Mbytes
   - user018 and user019 together can never have more than 50 files. They can exceed 40 files for as long as 10 days.
     - **NOTE:** debian quota utilities assume that if an ext4 filesystem is being used for quotas it has already been formatted with quotas. We should create the quota files with the options `-c` and `-m`
2. using *acls*, allow user001 and user002 to read and modify `/boot/grub/grub.cfg`. Allow members of the group *password* to modify `/etc/shadow`

Tasks for Lab Assigment 2: Hardening file systems, crypting

3. add a second disk to machine FSO-2025 an partition it using GPT
4. create two partitions with all the remaining space on the first disk
5. create 4 partitions on the second disk (/dev/sdb1, /dev/sdb2, /dev/sdb3 and /dev/sdb4)
6. create a crypted file system on /dev/sdb1 *plain mode*. Mount it onto `/crypt1`.
7. create a crypted file system on /dev/sdb2 *LUKS mode*. Mount it onto `/crypt2`.
   - add three more passphrases to it

Tasks for Lab Assigment 3: Hardening file systems, crypting

8. create a crypted volume comprising the available (just created) partitions in `/dev/sda`, `/dev/sdb3` and `/dev/sdb4`. Use the recommended method to create the physical volumes on the crypted devices. Mount it and copy files onto it
   - `/dev/sda4` should be plain type, the others should be LUKS type
   - use the same passphrase for all the physical volumes. Change the *passphrases*.
9. reboot and access the crypted device. Check that the files are in it
10. Using *encfs*, create a crypted directory `$HOME/.crypted` that can be accessed under `$HOME/CLEAR`.
    - copy files to `$HOME/CLEAR` and check de contents of `$HOME/.crypted`
    - unmount `$HOME/CLEAR` (with `fusermount -u`). Change the `passphrase` and check that the files can be accessed with the new `passphrase`

Lab Assignment 2: Work submission

- After performing the corresponding tasks of the lab assigment, a pdf document, describing what has been done (including screenshots showing the behaviour of the virtual machine, changes made to configuraton files, output from commands...) should be sent to
  - `antonio.yanez@udc.es`. (students at udc)
  - `yolanda@det.uvigo.es`. (students at uvigo)
- The subject of the mail should be *FSO: practica-2*
- The attachement should be named with the lab assignment number and the surname and name of the student, in the form P2-Surname-Name.pdf, avoiding non-ascii characteres (á, é, ñ ...)

Lab Assignment 2: Work submission

- example
  - For this lab assigment, the work submitted by student *Donald Trump Núñez* should come as an attached file named `P2-TrumpNunez-Donald.pdf` to a mail with the subject *FSO: practica-2*
  - Should Donald Trump Núñez team up with Vladimir Putin Vázquez to make the lab assignments, ONLY ONE OF THEM should mail the file. The first page of the pdf should contain BOTH names, and the file could be named either `P2-TrumpNunez-Donald.pdf` or `P2-PutinVazquez-Vladimir.pdf`
- The work must be submitted within 15 minutes of the end of the lab assignment class