Lab Assignment 3: Hardening applications

1. Open the web browser and start to download the following url

   https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/debian-12.9.0-amd64-DVD-1.iso

   - with the top command check how much CPU the web browser is using
   - use the cpulimit program to reduce the CPU this web browser is using to one fifth (1/5) of whatever it is using
   - check how much CPU it is using now
   - (close the web browser and end the cpulimit program)

Lab Assignment 3: Hardening applications

2 create a container of type *debian*, and start it
  - put password to the root user in the container
  - add three users (with their home directories and password, and whose names do not match any of the users in the host machine)
  - install the web server (apt-get install apache2) and the ssh server (apt-get install ssh, if it is not already installed) in the container
  - change the network address in the container to use a static network address, in the same network it was before
  - change the ssh server port in the container to 222 (file /etc/sshd/sshd_config)
  - stop the container
  - Add to the container configuration file (/var/lib/lxc/container-name/config)
    ```
    lxc.start.auto = 1
    lxc.start.delay = 3
    ```
  - reboot the machine

Lab Assignment 3: Hardening applications

3 Create a *cgroup*

- Open a terminal and add the shell in that terminal to the cgroup
- From that very shell open firefox and atril
- Check the contents of the file *cgroup.procs* and *memory.current*
- Put an '1' in *cgroups.freeze*. What happens? What are the contents of the *memory.current* file?
- Put an '0' in *cgroups.freeze*
- Put the values 30000 100000 en el ficheros *cpu.max del cgroup*. what is happening??

Lab Assignment 3: Hardening applications

4. Make a copy of the *ls* program, call it /usr/bin/listar
   and create an empty apparmor profile for it
   - it the profile allow it to read any part of the filesystem,
     except for the /etc directory and its descendants
   - Put the profile in *enforce* mode
   - Can it list files/directories whose path name starts with
     /etc?
   - What happnes when doing long (-l) listings of other
     files/directories?

Lab Assignment 3: 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
  - david.otero.freijeiro@udc.es. (students at udc)
  - yolanda@det.uvigo.es. (students at uvigo)
- The subject of the mail should be *FSO: practica-3*
- The attachement should be named with the lab assignment number and the surname and name of the student, in the form P3-Surname-Name.pdf, avoiding non-ascii characteres (á, é, ñ . . .)

Lab Assignment 3: Work submission

- example
  - For this lab assigment, the work submitted by student *Donald Trump Núñez* should come as an attached file named P3-TrumpNunez-Donald.pdf to a mail with the subject *FSO: practica-3*
  - 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 P3-TrumpNunez-Donald.pdf or P3-PutinVazquez-Vladimir.pdf
- The work must be submitted within 15 minutes of the end of the lab assignment class