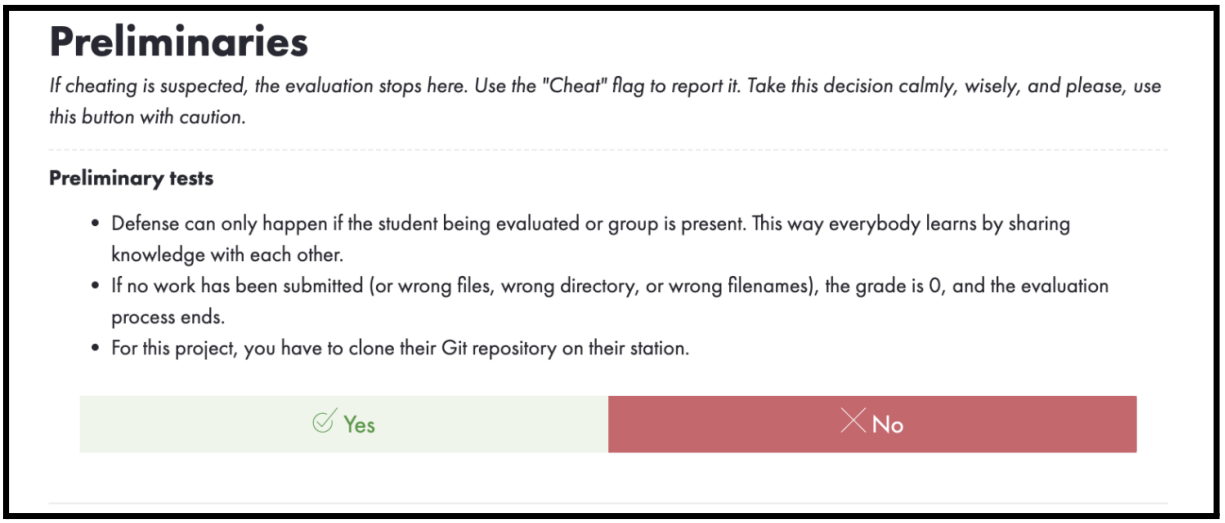
EVALUACIÓN BORN-2-B-ROOT



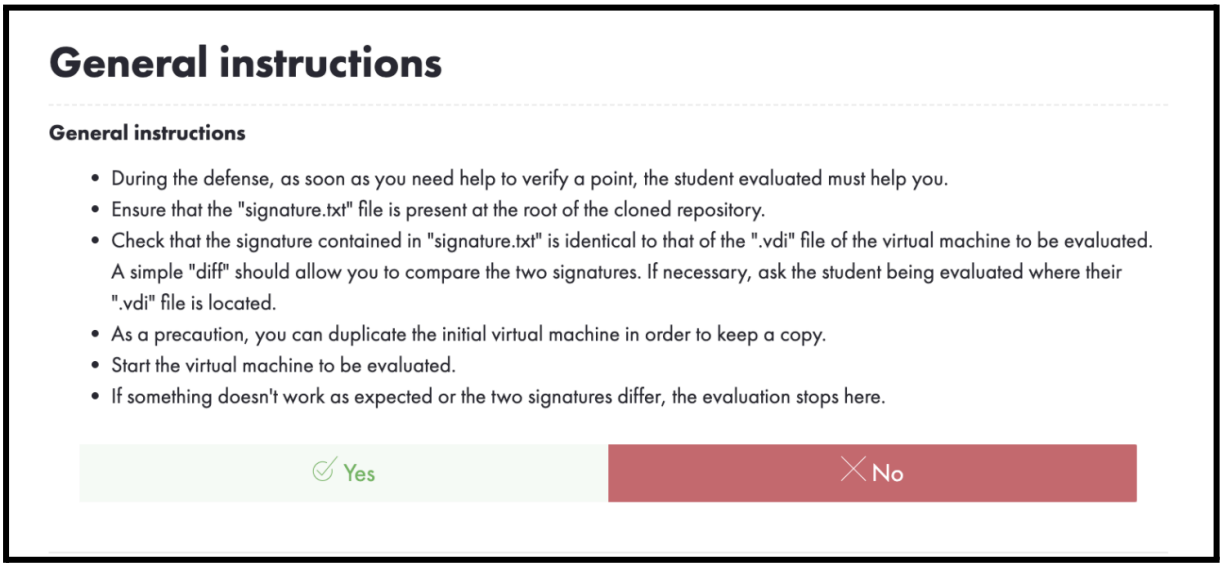
Preliminaries

If cheating is suspected, the evaluation stops here. Use the "Cheat" flag to report it. Take this decision calmly, wisely, and please, use this button with caution.

Preliminary tests

- Defense can only happen if the student being evaluated or group is present. This way everybody learns by sharing knowledge with each other.
- If no work has been submitted (or wrong files, wrong directory, or wrong filenames), the grade is 0, and the evaluation process ends.
- For this project, you have to clone their Git repository on their station.

Yes | No



General instructions

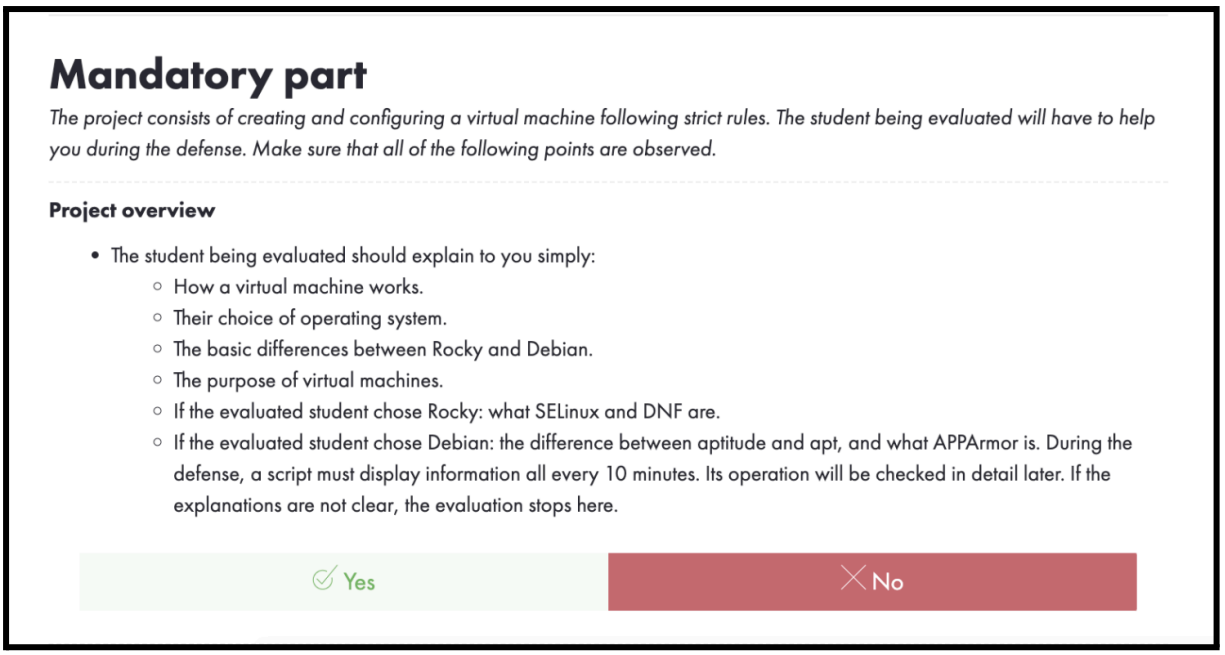
General instructions

- During the defense, as soon as you need help to verify a point, the student evaluated must help you.
- Ensure that the "signature.txt" file is present at the root of the cloned repository.
- Check that the signature contained in "signature.txt" is identical to that of the ".vdi" file of the virtual machine to be evaluated. A simple "diff" should allow you to compare the two signatures. If necessary, ask the student being evaluated where their ".vdi" file is located.
- As a precaution, you can duplicate the initial virtual machine in order to keep a copy.
- Start the virtual machine to be evaluated.
- If something doesn't work as expected or the two signatures differ, the evaluation stops here.

Yes | No

INSTRUCCIONES GENERALES

En primer lugar, hay que comprobar que el archivo entregado en el repositorio **'signature.txt'** contenga la **firma de la máquina virtual** que se puede obtener en la misma accediendo al archivo .vdi de la máquina virtual. Para comprobar que estén correctas se puede hacer un diff para comparar ambas. La **ubicación del archivo .vdi** se encuentra en **-> sgoinfre/Born2beRoot y hacer shasum Born2beroot.vdi**



Mandatory part

The project consists of creating and configuring a virtual machine following strict rules. The student being evaluated will have to help you during the defense. Make sure that all of the following points are observed.

Project overview

- The student being evaluated should explain to you simply:
  - How a virtual machine works.
  - Their choice of operating system.
  - The basic differences between Rocky and Debian.
  - The purpose of virtual machines.
  - If the evaluated student chose Rocky: what SELinux and DNF are.
  - If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

Yes | No

RESUMEN DEL PROYECTO

Que es una máquina virtual

Una máquina virtual es un software que simula un sistema de computación y que puede ejecutar programas como si fuese una computadora real, permitiendo crear múltiples entornos simulados desde un solo sistema de hardware físico.

Qué opción has escogido para el sistema operativo

En el subject hay un apartado en el que te indica y elegir entre la última versión de Debian y de Rocky. Como en el propio documento dice, se recomienda escoger Debian si no tienes experiencia en administración de sistemas ya que configurar Rocky es bastante complejo.

Cuales son las diferencias básicas entre debian y rocky

Rocky y Debian son dos distribuciones de Linux con enfoques diferentes. Debian es una distribución universal y antigua, conocida por su estabilidad y desarrollo comunitario, con ciclos de lanzamiento flexibles que incluyen versiones estables, inestables y de pruebas. Utiliza APT y paquetes .deb, y es versátil, adecuada para servidores, escritorios y dispositivos embebidos, con una amplia comunidad de apoyo. Por otro lado, Rocky Linux está basado en Red Hat Enterprise Linux (RHEL) y se centra en entornos empresariales, siguiendo un ciclo de lanzamientos alineado con RHEL y priorizando la estabilidad. Utiliza DNF (o YUM) y paquetes .rpm, y está principalmente diseñado para servidores. Aunque Rocky Linux tiene una comunidad en crecimiento respaldada por la Fundación Rocky, Debian cuenta con una comunidad más amplia y recursos variados.

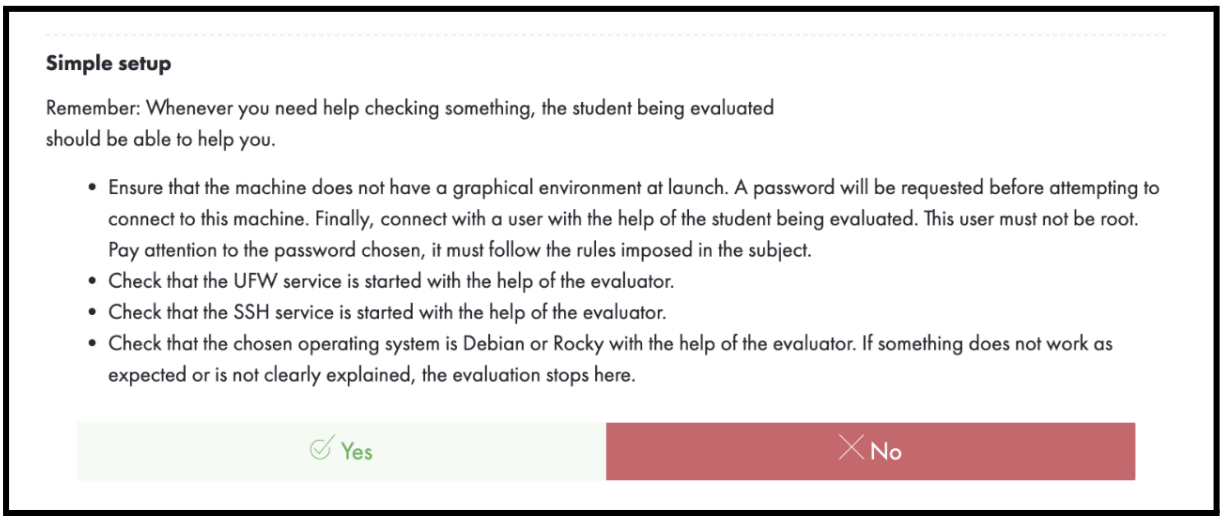
Cuales son los propósitos de la máquinas virtuales

Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de hardware y del sistema operativo, que oculte los detalles de la plataforma en la que se encuentra y que permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.

Elección Debian -> Cual es la diferencia entre apt y aptitude y que es APPArmor

La diferencia entre aptitude y apt es que la primera es una versión mejorada de la segunda, siendo apt un administrador de paquetes de nivel inferior mientras que aptitude es de alto nivel. Por otra parte, aptitude ofrece una mejor funcionalidad en comparación con apt-get. Ambos son capaces de proporcionar los medios necesarios para la gestión de paquetes pero si se busca un enfoque con más características debería de usarse aptitude.

Por otro lado APPArmor es un módulo de seguridad de kernel Linux que permite al administrador del sistema restringir las capacidades de un programa.



SET UP DEL PROYECTO

Comprobar que no haya interfaz gráfica en uso

ls /usr/bin/*session

Comprobar que el servicio UFW está activo

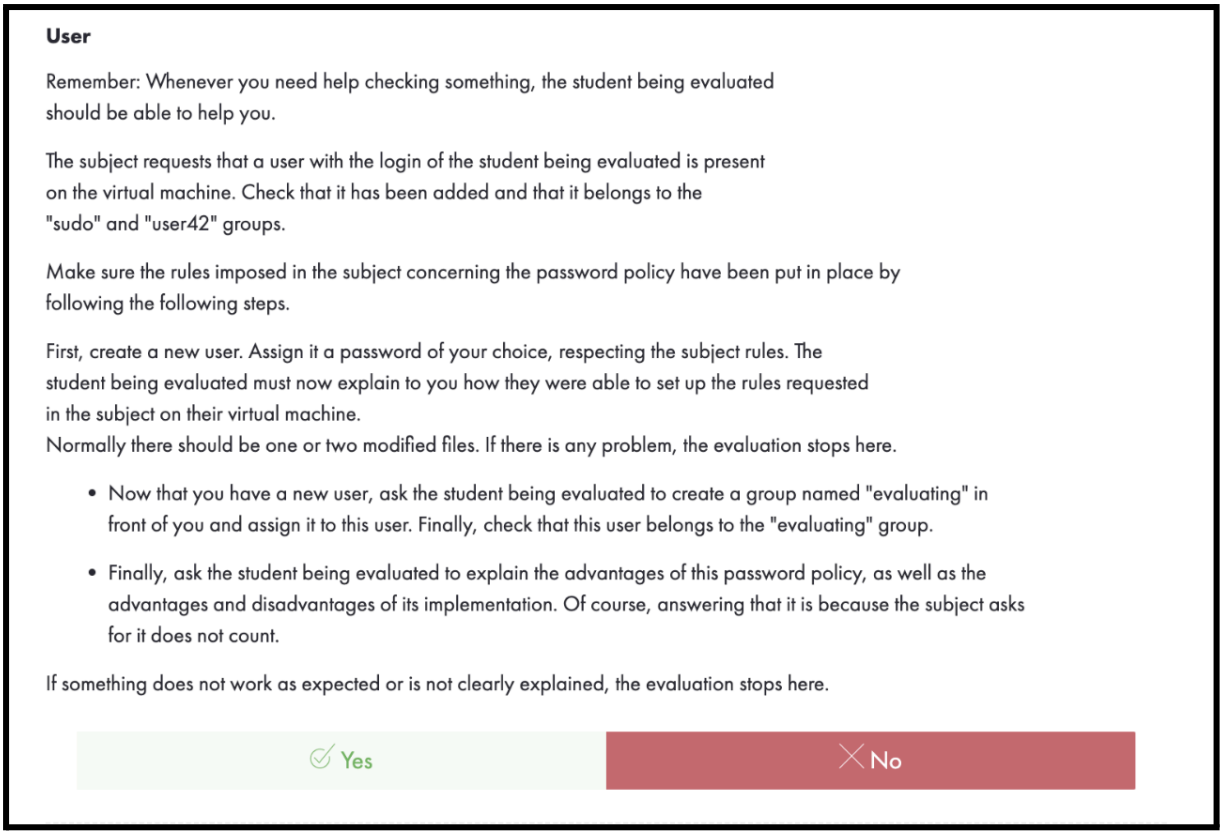
sudo ufw status

Comprobar que el servicio SSH está en uso

sudo service ssh status

Comprobar que utilizas el sistema operativo Debian / CentOS

uname -v / uname - - kernel-version



User

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to the "sudo" and "user42" groups.

Make sure the rules imposed in the subject concerning the password policy have been put in place by following the following steps.

First, create a new user. Assign it a password of your choice, respecting the subject rules. The student being evaluated must now explain to you how they were able to set up the rules requested in the subject on their virtual machine.
Normally there should be one or two modified files. If there is any problem, the evaluation stops here.

- Now that you have a new user, ask the student being evaluated to create a group named "evaluating" in front of you and assign it to this user. Finally, check that this user belongs to the "evaluating" group.
- Finally, ask the student being evaluated to explain the advantages of this password policy, as well as the advantages and disadvantages of its implementation. Of course, answering that it is because the subject asks for it does not count.

If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes No

USUARIOS

Comprobar que el usuario está dentro de los grupos “sudo” y “user42”

getent group sudo

getent group user42

Crear un nuevo usuario y mostrar que sigue la política de contraseñas que se ha creado

sudo adduser name_user

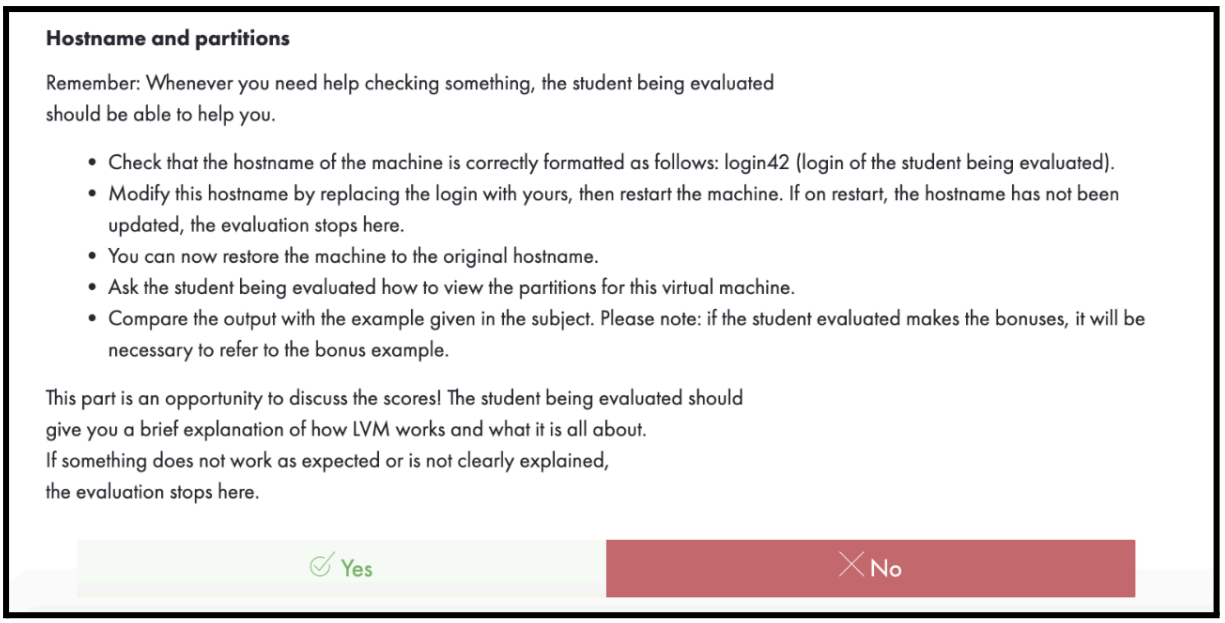
introducir contraseña que siga la política

Crear un grupo nuevo llamado “evaluating” y añadir el nuevo usuario al grupo creado

sudo addgroup evaluating

sudo adduser name_user evaluating

getent group evaluating (Comprobar que se ha creado y añadadido correctamente)



HOSTNAME Y PARTICIONES

Comprobar que el hostname de la máquina es correcto (login + 42)

hostname

Modificar el hostname para reemplazar el login por el del evaluador

sudo vim /etc/hostname -> cambiamos allí el login propio por el del evaluador

Reiniciamos la máquina virtual

sudo reboot

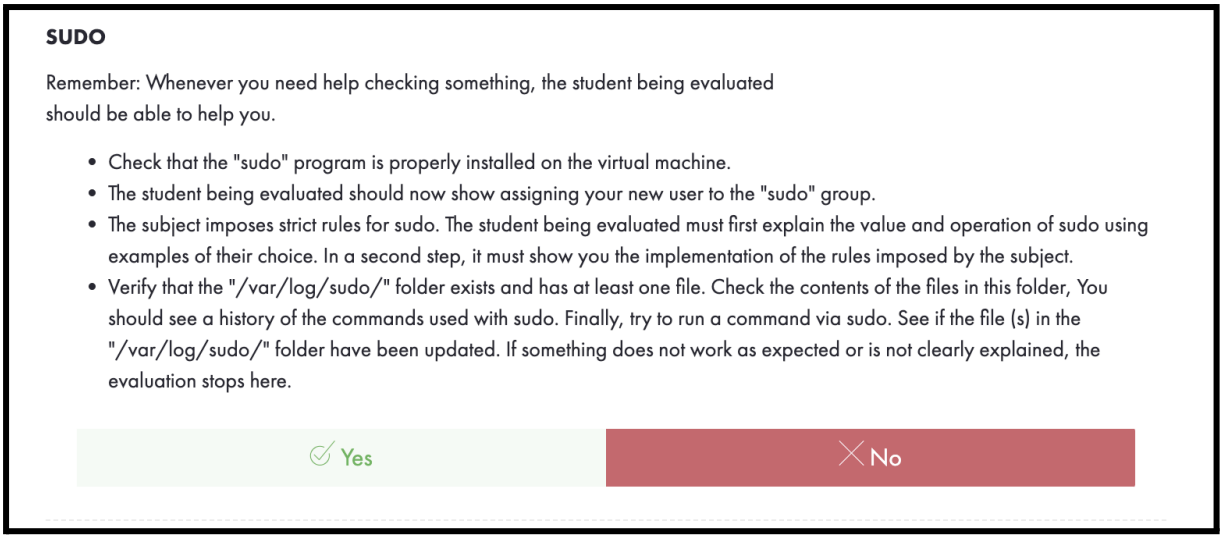
Volvemos a cambiar el hostname al original

sudo vim /etc/hostname -> volvemos al login propio

Comprobación de las particiones son como el subject

lsblk

LVM es un software que ayuda a gestionar discos y particiones en un sistema. Permite crear "volúmenes" de almacenamiento que se pueden ajustar y mover según lo necesites. Así, puedes organizar y manejar tu espacio en disco de manera más flexible.whcd



SUDO

Comprobar que sudo está instalado

which sudo // => dpkg -s sudo

Asignar el nuevo usuario al grupo sudo

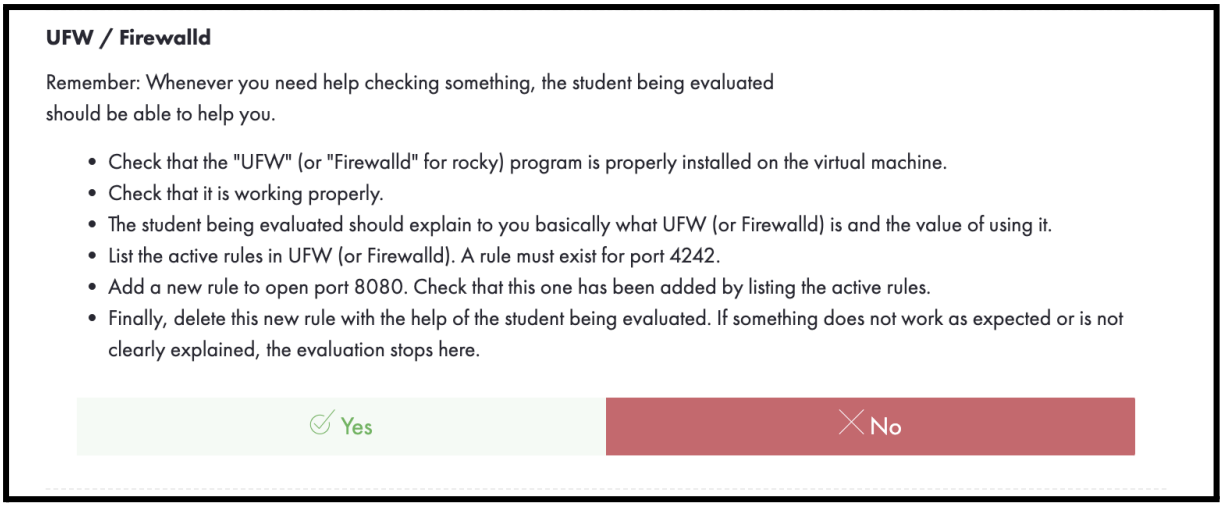
sudo adduser name_user sudo

Mostrar las reglas dadas par sudo

vim /etc/sudoers.d/sudo_config

Mostrar /var/log/sudo y ver que contiene al menos un fichero, además ver ese fichero

cd /var/log/sudo -> cat -e sudo_config



COMPROBACIÓN UFW

Comprobar que ufw está configurado

dpkg -s ufw

Comprobar que funciona correctamente ufw

sudo service ufw status

Lista las reglas activas en UFW

sudo ufw status numbered

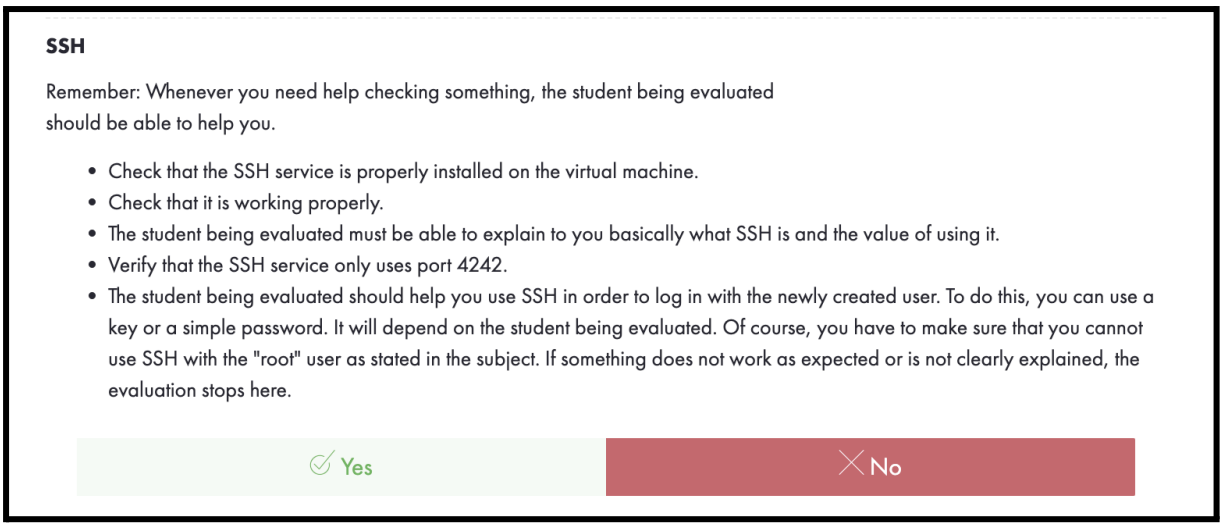
Crear nuevo puerto

sudo ufw allow 1080

sudo ufw status numbered

Eliminar regla 8080

sudo ufw delete 1080



SSH

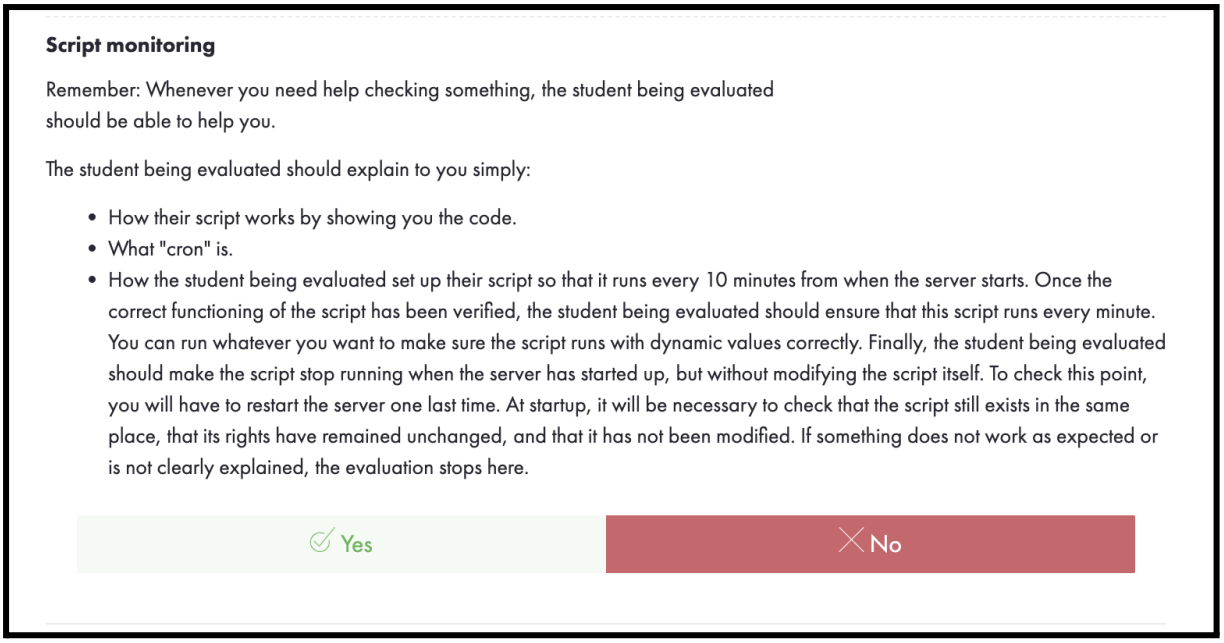
Comprobar que el ssh está instalado y activo

which ssh

sudo service ssh status

Iniciar sesión desde terminal con el nuevo usuario

ssh newuser@localhost -p [used port in host]



MONITOREO DEL SCRIPT

Para esta parte, enseñar el script de **"monitoring.sh"** y explicar lo que hace cada comando:

Monitoring.sh

1. arch=$(uname -a)
    - Descripción: Obtiene la arquitectura y la información general del sistema operativo (como el kernel, la versión, la arquitectura del sistema).
2. cpuf=$(grep "physical id" /proc/cpuinfo | wc -l)
    - Descripción: Cuenta el número de "physical id" en el archivo /proc/cpuinfo, lo que indica cuántos núcleos físicos tiene el procesador.
3. cpuv=$(grep "processor" /proc/cpuinfo | wc -l)
    - Descripción: Cuenta el número de "processor" en /proc/cpuinfo, lo que indica cuántos núcleos virtuales (hilos) tiene el procesador, incluyendo los núcleos lógicos si el procesador soporta Hyper-Threading.
4. Memoria RAM:
    - ram_total=$(free --mega | awk '$1 == "Mem:" {print $2}'): Obtiene la cantidad total de RAM (en MB).
    - ram_use=$(free --mega | awk '$1 == "Mem:" {print $3}'): Obtiene la cantidad de RAM usada (en MB).
    - ram_percent=$(free --mega | awk '$1 == "Mem:" {printf("%.2f"), $3/$2*100}'): Calcula el porcentaje de uso de la RAM.
5. Disco:

- disk_total=$(df -m | grep "/dev/" | grep -v "/boot" | awk '{disk_t += $2} END {printf ("%.1fGb\n"), disk_t/1024}'): Obtiene el tamaño total del disco (en GB), excluyendo las particiones relacionadas con /boot.
- disk_use=$(df -m | grep "/dev/" | grep -v "/boot" | awk '{disk_u += $3} END {print disk_u}'): Obtiene el uso total del disco (en MB), excluyendo /boot.
- disk_percent=$(df -m | grep "/dev/" | grep -v "/boot" | awk '{disk_u += $3} {disk_t+= $2} END {printf("%d"), disk_u/disk_t*100}'): Calcula el porcentaje de uso del disco.

6. Carga de la CPU:
   - cpul=$(vmstat 1 2 | tail -1 | awk '{printf $15}'): Obtiene el valor de "idle" (porcentaje de tiempo en el que la CPU está inactiva).
   - cpu_op=$(expr 100 - $cpul): Calcula el porcentaje de uso de la CPU restando el valor de "idle" de 100.
   - cpu_fin=$(printf "%.1f" $cpu_op): Formatea el valor de uso de la CPU a un solo decimal.
7. Último reinicio:
   - lb=$(who -b | awk '$1 == "system" {print $3 " " $4}'): Muestra la fecha y hora del último reinicio del sistema.
8. Uso de LVM:
   - lvmu=$(if [$(lsblk | grep "lvm" | wc -l) -gt 0]; then echo yes; else echo no; fi): Verifica si el sistema está utilizando LVM (Logical Volume Manager). Si hay alguna partición con LVM, devuelve yes; si no, devuelve no.
9. Conexiones TCP activas:
   - tcpc=$(ss -ta | grep ESTAB | wc -l): Cuenta las conexiones TCP establecidas actualmente.
10. Número de usuarios logueados:
    - ulog=$(users | wc -w): Cuenta cuántos usuarios están logueados en el sistema.
11. Red:
    - ip=$(hostname -I): Muestra la dirección IP de la máquina.
    - mac=$(ip link | grep "link/ether" | awk '{print $2}'): Muestra la dirección MAC de la interfaz de red.
12. Número de comandos ejecutados con sudo:
    - cmnd=$(journalctl _COMM=sudo | grep COMMAND | wc -l): Cuenta cuántos comandos se han ejecutado usando sudo en el sistema.

Comando `wall`:

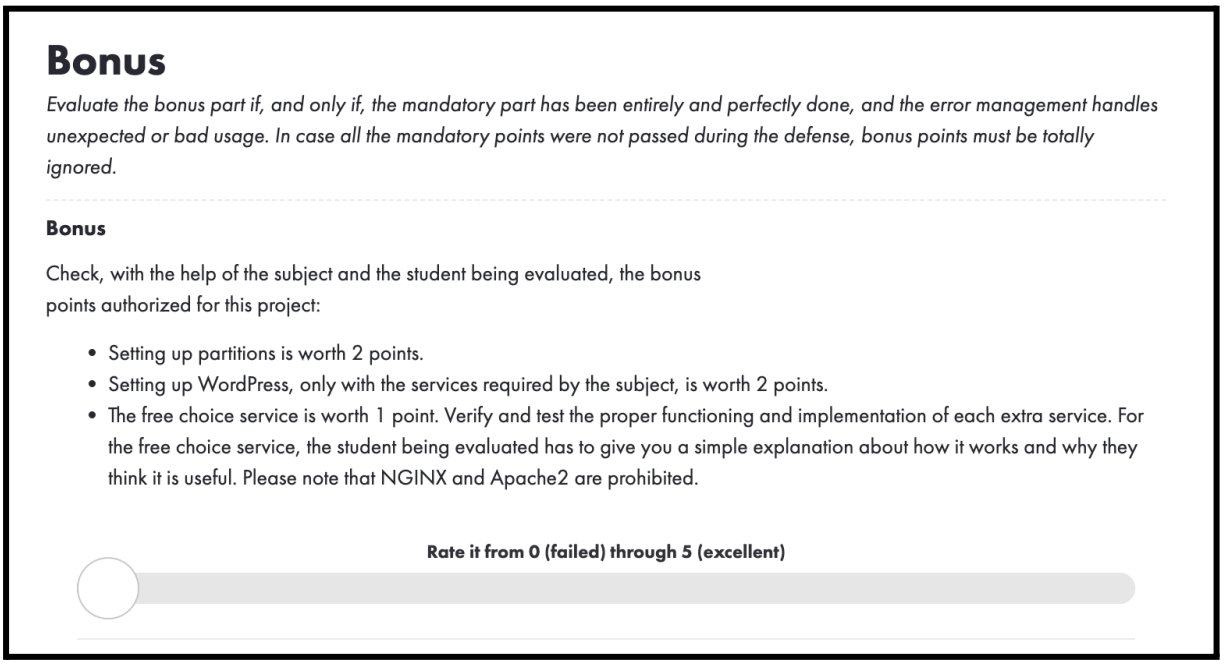
Al final, el script usa el comando `wall` para mostrar toda esta información en los monitores conectados a la máquina:

Cómo funciona crontab

Crontab es una herramienta del sistema que permite asignar tareas con un tiempo determinado, por ejemplo en este caso se pide hacer que se ejecute el script **monitoring.sh** cada 10 min.

Para cambiar esto acceder a **sudo crontab -u root -e.**

BONUS



Bonus

Evaluate the bonus part if, and only if, the mandatory part has been entirely and perfectly done, and the error management handles unexpected or bad usage. In case all the mandatory points were not passed during the defense, bonus points must be totally ignored.

Bonus

Check, with the help of the subject and the student being evaluated, the bonus points authorized for this project:

- Setting up partitions is worth 2 points.
- Setting up WordPress, only with the services required by the subject, is worth 2 points.
- The free choice service is worth 1 point. Verify and test the proper functioning and implementation of each extra service. For the free choice service, the student being evaluated has to give you a simple explanation about how it works and why they think it is useful. Please note that NGINX and Apache2 are prohibited.

Rate it from 0 (failed) through 5 (excellent)

Enseñar las particiones

lsblk

Enseñar wordpress

http://localhost:8086/ en el navegador

Enseñar lighttpd

sudo systemctl status lighttpd

Enseñar mariadb

mariadb // SHOW DATABASES;

Enseñar PHP

vim /var/www/html/wp-config.php

Servicio extra escogido: LiteSpeed

LiteSpeed es un servidor web rápido y eficiente. Mejora el rendimiento, ahorra recursos y es compatible con Apache. Ideal para sitios de alto tráfico, con caché integrado y soporte para PHP. Además he tirado por esta opción ya que tiene versión gratuita. Para acceder a esta https://localhost:7080/ en el navegador.