BORN2BEROOT

Preliminary tests

For this project, you have to clone their Git repository on their station.- Ensure that the "signature.txt" file is present
Check that the signature contained in "signature.txt" is identical to that of the ".vdi" file of the virtual machine.

How a virtual machine works:
Las máquinas virtuales son una tecnología que permite crear múltiples entornos simulados o recursos dedicados desde un solo sistema de hardware físico. Podrás automatizar, gestionar y modernizar todas tus cargas de trabajo de virtualización.

Their choice of operating system:

Debian por su facilidad de uso y porque todo su software en open source y tiene una gran comunidad detrás.

The purpose of virtual machines:

Las máquinas virtuales se pueden implementar para adaptarse a diferentes niveles de necesidades de potencia de procesamiento, para ejecutar software que requiere un diferente sistema operativo o para probar aplicaciones en un entorno seguro y aislado.

If the evaluated student chose Debian: the difference between aptitude and apt:

Aptitude es un administrador de paquetes de alto nivel, mientras que APT es un administrador de paquetes de nivel inferior que puede ser utilizado por otros administradores de paquetes de nivel superior.

Si bien apt-get no tiene una interfaz de usuario,Aptitude tiene una interfaz de usuario interactiva y de solo texto.

what APPArmor is.

APPArmor es un modulo de seguridad del kernel de Linux que permite al administrador del sistema restringir las capacidades de un programa por perfiles de programa.

Sudo aa-status

a script must display information all every 10 minutes.

Si está el script en cron esperar a que se ejecute sin más.

Simple setup

Ensure that the machine does not have a graphical environment at launch.

…
A password will be requested before attempting to connect to this machine.

…
Connect with a user with the help of the student.This user must not be root.

Loguearse con un usuario creado

Pay attention to the password chosen, it must follow the rules imposed in the subject.

Ver después con la creación de contraseña del nuevo usuario

Check that the UFW service is started with the help of the evaluator.

Sudo ufw status

Check that the SSH service is started with the help of the evaluator.

Sudo service ssh status

Check that the chosen operating system is Debian or CentOS with the help of the evaluator.

uname -a

The subject requests that a user with the login of the student being evaluated is present on the virtual machine.

Getent passwd |grep “usuario”

Getent passwd “usuario”

Check that it has been added and that it belongs to the "sudo" and "user42" groups.

Getent group o getent group user42 y getent group sudo

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.

sudo adduser “usuario”

Assign it a password of your choice, respecting the subject rules. (*reglas creadas en el paso de abajo***)**

…

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.

Sudo nano /etc/login.defs caducidad de la contraseña(PASS_MAX_DAYS,etc)

Sudo nano /etc/pam.d/common-password (long pass, retry,mxrepeat, etc)

Ask the student to create a group named "evaluating" and assign it to this user.

sudo addgroup evaluating

sudo adduser “usuario” evaluating

Finally, check that this user belongs to the "evaluating" group.

Sudo getent group evaluating

Ask the student to explain the advantages of this password policyHostname and partitions Remember:

Check that the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).

hostnamectl

- Modify this hostname by replacing the login with yours, then restart the machine.

Sudo nano /etc/hostname ó

Sudo hostnamectl set-hostname “nuevo nombre” y sudo nano /etc/hosts

systemctl reboot

- You can now restore the machine to the original hostname.

Sudo nano /etc/hostname ó

Sudo hostnamectl set-hostname “nuevo nombre” y sudo nano /etc/hosts

systemctl reboot

- Ask the student being evaluated how to view the partitions for this virtual machine.
- Compare the output with the example given in the subject.

lsblk

Please note: if the student evaluated makes the bonuses, it will be necessary to refer to the bonus example. The student being evaluated shouldgive you a brief explanation of how LVM works and what it is all

Explicación del sistema de particionado(LVM logical volumen manager).

Los volúmenes lógicos agrupan particiones físicas de disco, y estos a su vez se engloban en un grupo lógico. De esta forma, /home se compone de hda3, hda4 y hdb3, y a su vez, /usr engloba a hda1, hda2, hdb1 y hdb2.(solo un ejemplo).

SUDO

Check that the "sudo" program is properly installed on the virtual machine.

apt -qq list sudo

The student being evaluated should now show assigning your new user to the "sudo" group.

Sudo adduser “usuario” sudo

The subject imposes strict rules for sudo. The student being evaluated must first explain the value and operation of sudo using examples of their choice.

Sudo nano /etc/sudoers.d/sudoconfig(tiene que estar creado con las reglas dentro)

In a second step, it must show you the implementation of the rules imposed by the subject.

sudo nano /etc/pam.d/common-password

(ahí están longitud mínima,cantidad de intentos,letras repetidas,etc)

- Verify that the "/var/log/sudo/" folder exists and has at least one file. Check the contents of the files in this folder, You should see a history of the commands used with sudo.

Navegar por las carpetas /var/log/sudo/00/00/* y entrar en los archivos log

Finally, try to run a command via sudo. See if the file (s) in the "/var/log/sudo/" folder have been updated.

Hacer la prueba con cualquier comando con sudo delante(crear carpeta, apt get,etc)

UFW

Check that the "UFW" program is properly installed on the virtual machine.

Sudo apt -qq -list ufw

dpkg -l | grep ufw

- Check that it is working properly.

Sudo ufw status

- The student being evaluated should explain to you basically what UFW is and the value of using it.

Ufw es un cortafuegos que por defecto deniega cualquier conexión a los puertos del pc a excepción de las reglas que se van añadiendo aquí.

- List the active rules in UFW. A rule must exist for port 4242.

Sudo ufw status

- Add a new rule to open port 8080. Check that this one has been added by listing the active rules.

Sudo ufw allow 80

Sudo ufw status

- Finally, delete this new rule with the help of the student being evaluated.

Sudo ufw deny 80

Sudo ufw status

SSH

Check that the SSH service is properly installed on the virtual machine.Check that it is working properly.

Sudo apt -qq list ssh (versión reducida del comando de abajo)

dpkg -l | grep ssh (ver los componentes instalados)

Sudo service ssh status (ver si esta funcionando)

- The student being evaluated must be able to explain to you basically what SSH is and the value of using it.

SSH o (secure socket Shell) es un protocolo de red que permite a los usuarios, normalmente administradores del sistema una forma segura de acceder a una computadora remota en una red insegura.

Verify that the SSH service only uses port 4242.

Sudo nano /etc/ssh/sshd_config

The student being evaluated should help you use SSH in order to log in with the newly created user. To do this, you can use a key or a simple password.

Crear un usuario nuevo y acceder al sistema mediante ssh al sistema.

Sudo adduser “usuario”

Ssh usuario@ipdelsistema -p 4242

make sure that you cannot use SSH with the "root" user as stated in the subject.

Probar a loguearse mediante ssh con root.

Script monitoring

The student being evaluated should explain to you simply: How their script works by showing you the code.

Explicar script monitoring.sh haciendo nano sobre el.

Eje: sudo nano /var/local/monitoring.sh(buscar la ruta en crontab)

What "cron" is.

Cron es un administrador de tareas de Linux que permite ejecutar comandos en un momento determinado.

How the student being evaluated set up their script so that it runs every 10 minutes from when the server starts.

Sudo crontab -u root -e

*/10 * * * * sh /var/local/monitoring.sh

Para ver las tareas del cron:

Sudo crontab -u root -l

Once the correct functioning of the script has been verified, the student being evaluated should ensure that this script runs every minute.

Sudo crontab -u root -e

*/1 * * * * sh /var/local/monitoring.sh

You can run whatever you want to make sure the script runs with dynamic values correctly.

Finally, the student being evaluated should make the script stop running when the server has started up, but without modifying the script itself. To check this point, you will have to restart the server one last time.

Sudo /etc/init.d/cron stop para detener el demonio cron

Sudo /etc/init.d/cron start para iniciar el demonio cron

At startup, it will be necessary to check that the script still exists in the same place, that its rights have remained unchanged, and that it has not been modified.

Verificar que la tarea sigue existiendo en cron

Sudo crontab -u root -**l**

Bonus

E*valuate 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.*

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.

Lsblk lista de particiones
Setting up WordPress, only with the services required by the subject, is worth 2 points.

Linux Lighttpd MariaDB PHP (LLMP) Stack:

sudo apt install lighttpd

dpkg -l | grep lighttpd

sudo ufw allow 80

sudo apt install mariadb-server

dpkg -l | grep mariadb-server

sudo mysql_secure_installation

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.